This electronic version (PDF) was scanned by the International Telecommunication Union (ITU) Library & Archives Service from an original paper document in the ITU Library & Archives collections.

La présente version électronique (PDF) a été numérisée par le Service de la bibliothèque et des archives de l'Union internationale des télécommunications (UIT) à partir d'un document papier original des collections de ce service.

Esta versión electrónica (PDF) ha sido escaneada por el Servicio de Biblioteca y Archivos de la Unión Internacional de Telecomunicaciones (UIT) a partir de un documento impreso original de las colecciones del Servicio de Biblioteca y Archivos de la UIT.

هذه النسخة الإلكترونية (PDF) للاتصالات الدولي الاتحاد في والمحفوظات المكتبة قسم أجراه الضوئي بالمسح تصوير نتاج (ITU) والمحفوظات المكتبة قسم في المتوفرة الوثائق ضمن أصلية ورقية وثيقة من نقلاً.

此电子版（PDF版本）由国际电信联盟（ITU）图书馆和档案室利用存于该处的纸质文件扫描提供。

Настоящий электронный вариант (PDF) был подготовлен в библиотечно-архивной службе Международного союза электросвязи путем сканирования исходного документа в бумажной форме из библиотечно-архивной службы МСЭ.

© International Telecommunication Union

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

LIBRO AZUL

TOMO VIII – FASCÍCULO VIII.7

REDES DE COMUNICACIÓN DE DATOS
SISTEMAS DE TRATAMIENTO DE MENSAJES

RECOMENDACIONES X.400 A X.420

IX ASAMBLEA PLENARIA
MELBOURNE, 14-25 DE NOVIEMBRE DE 1988

Ginebra 1989

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

LIBRO AZUL

TOMO VIII – FASCÍCULO VIII.7

REDES DE COMUNICACIÓN DE DATOS
SISTEMAS DE TRATAMIENTO DE MENSAJES

RECOMENDACIONES X.400 A X.420

IX ASAMBLEA PLENARIA
MELBOURNE, 14-25 DE NOVIEMBRE DE 1988

ARCHIVES U.I.T. GENÈVE

Ginebra 1989

ISBN 92-61-03723-2

© UIT

Impreso en Suiza

CONTENIDO DEL LIBRO DEL CCITT EN VIGOR DESPUÉS DE LA NOVENA ASAMBLEA PLENARIA (1988)

LIBRO AZUL

Tomo I

FASCÍCULO I.1 – Actas e Informes de la Asamblea Plenaria.

Lista de las Comisiones de Estudio y de las Cuestiones en estudio.

FASCÍCULO I.2 – Ruegos y Resoluciones.

Recomendaciones sobre la organización de los trabajos del CCITT (serie A).

FASCÍCULO I.3 – Términos y definiciones. Abreviaturas y acrónimos. Recomendaciones sobre los medios de expresión (serie B) y las estadísticas generales de las telecomunicaciones (serie C).

FASCÍCULO I.4 – Índice del Libro Azul.

Tomo II

FASCÍCULO II.1 – Principios generales de tarificación – Tasación y contabilidad en los servicios internacionales de telecomunicación. Recomendaciones de la serie D (Comisión de Estudio III).

FASCÍCULO II.2 – Red telefónica y RDSI – Explotación, numeración, encaminamiento y servicio móvil. Recomendaciones E.100 a E.333 (Comisión de Estudio II).

FASCÍCULO II.3 – Red telefónica y RDSI – Calidad de servicio, gestión de la red e ingeniería de tráfico. Recomendaciones E.401 a E.880 (Comisión de Estudio II).

FASCÍCULO II.4 – Servicios de telegrafía y móvil – Explotación y calidad de servicio. Recomendaciones F.1 a F.140 (Comisión de Estudio I).

FASCÍCULO II.5 – Servicios de telemática, transmisión de datos y teleconferencia – Explotación y calidad de servicio. Recomendaciones F.160 a F.353, F.600, F.601 y F.710 a F.730 (Comisión de Estudio I).

FASCÍCULO II.6 – Servicios de tratamiento de mensajes y guía – Explotación y definición del servicio. Recomendaciones F.400 a F.422 y F.500 (Comisión de Estudio I).

Tomo III

FASCÍCULO III.1 – Características generales de las conexiones y circuitos telefónicos internacionales. Recomendaciones G.101 a G.181 (Comisiones de Estudio XII y XV).

FASCÍCULO III.2 – Sistemas internacionales analógicos de portadoras. Recomendaciones G.211 a G.544 (Comisión de Estudio XV).

FASCÍCULO III.3 – Medios de transmisión – Características. Recomendaciones G.601 a G.654 (Comisión de Estudio XV).

FASCÍCULO III.4 – Aspectos generales de los sistemas de transmisión digital; equipos terminales. Recomendaciones G.700 a G.772 (Comisiones de Estudio XV y XVIII).

FASCÍCULO III.5 – Redes digitales, secciones digitales y sistemas de línea digitales. Recomendaciones G.801 a G.956 (Comisiones de Estudio XV y XVIII).

FASCÍCULO III.6 – Transmisión en línea de señales no telefónicas. Transmisión de señales radiofónicas y de televisión. Recomendaciones de las series H y J (Comisión de Estudio XV).

FASCÍCULO III.7 – Red digital de servicios integrados (RDSI). Estructura general y capacidades de servicio. Recomendaciones I.110 a I.257 (Comisión de Estudio XVIII).

FASCÍCULO III.8 – Red digital de servicios integrados (RDSI). Aspectos y funciones globales de la red, interfaces usuario-red de la RDSI. Recomendaciones I.310 a I.470 (Comisión de Estudio XVIII).

FASCÍCULO III.9 – Red digital de servicios integrados (RDSI). Interfaces entre redes y principios de mantenimiento. Recomendaciones I.500 a I.605 (Comisión de Estudio XVIII).

Tomo IV

FASCÍCULO IV.1 – Principios generales de mantenimiento: mantenimiento de los sistemas de transmisión y de los circuitos telefónicos internacionales. Recomendaciones M.10 a M.782 (Comisión de Estudio IV).

FASCÍCULO IV.2 – Mantenimiento de circuitos internacionales de telegrafía y de telefotografía y de circuitos internacionales arrendados. Mantenimiento de la red telefónica pública internacional. Mantenimiento de sistemas marítimos por satélite y de transmisión de datos. Recomendaciones M.800 a M.1375 (Comisión de Estudio IV).

FASCÍCULO IV.3 – Mantenimiento de circuitos internacionales para transmisiones radiofónicas y de televisión. Recomendaciones de la serie N (Comisión de Estudio IV).

FASCÍCULO IV.4 – Especificaciones de los aparatos de medida. Recomendaciones de la serie O (Comisión de Estudio IV).

Tomo V – Calidad de transmisión telefónica. Recomendaciones de la serie P (Comisión de Estudio XII).

Tomo VI

FASCÍCULO VI.1 – Recomendaciones generales sobre la conmutación y la señalización telefónicas. Funciones y flujos de información para los servicios de la RDSI. Suplementos. Recomendaciones Q.1 a Q.118 *bis* (Comisión de Estudio XI).

FASCÍCULO VI.2 – Especificaciones de los sistemas de señalización N.^{os} 4 y 5. Recomendaciones Q.120 a Q.180 (Comisión de Estudio XI).

FASCÍCULO VI.3 – Especificaciones del sistema de señalización N.º 6. Recomendaciones Q.251 a Q.300 (Comisión de Estudio XI).

FASCÍCULO VI.4 – Especificaciones de los sistemas de señalización R1 y R2. Recomendaciones Q.310 a Q.490 (Comisión de Estudio XI).

FASCÍCULO VI.5 – Centrales digitales locales, de tránsito, combinadas e internacionales en redes digitales integradas y en redes mixtas analógico-digitales. Suplementos. Recomendaciones Q.500 a Q.554 (Comisión de Estudio XI).

FASCÍCULO VI.6 – Interfuncionamiento de los sistemas de señalización. Recomendaciones Q.601 a Q.699 (Comisión de Estudio XI).

FASCÍCULO VI.7 – Especificaciones del sistema de señalización N.º 7. Recomendaciones Q.700 a Q.716 (Comisión de Estudio XI).

FASCÍCULO VI.8 – Especificaciones del sistema de señalización N.º 7. Recomendaciones Q.721 a Q.766 (Comisión de Estudio XI).

FASCÍCULO VI.9 – Especificaciones del sistema de señalización N.º 7. Recomendaciones Q.771 a Q.795 (Comisión de Estudio XI).

FASCÍCULO VI.10 – Sistema de señalización digital de abonado N.º 1 (SDA 1), capa enlace de datos. Recomendaciones Q.920 a Q.921 (Comisión de Estudio XI).

FASCÍCULO VI.11 – Sistema de señalización digital de abonado N.º 1 (SDA 1), capa red, gestión usuario-red. Recomendaciones Q.930 a Q.940 (Comisión de Estudio XI).

FASCÍCULO VI.12 – Red móvil terrestre pública, interfuncionamiento con RDSI y RTPC. Recomendaciones Q.1000 a Q.1032 (Comisión de Estudio XI).

FASCÍCULO VI.13 – Red móvil terrestre pública. Parte aplicación móvil e interfaces. Recomendaciones Q.1051 a Q.1063 (Comisión de Estudio XI).

FASCÍCULO VI.14 – Interfuncionamiento con sistemas móviles por satélite. Recomendaciones Q.1100 a Q.1152 (Comisión de Estudio XI).

Tomo VII

FASCÍCULO VII.1 – Transmisión telegráfica. Recomendaciones de la serie R. Equipos terminales para los servicios de telegrafía. Recomendaciones de la serie S (Comisión de Estudio IX).

FASCÍCULO VII.2 – Conmutación telegráfica. Recomendaciones de la serie U (Comisión de Estudio IX).

FASCÍCULO VII.3 – Equipo terminal y protocolos para los servicios de telemática. Recomendaciones T.0 a T.63 (Comisión de Estudio XVIII).

FASCÍCULO VII.4 – Procedimientos de prueba de conformidad para las Recomendaciones teletex. Recomendación T.64 (Comisión de Estudio VIII).

FASCÍCULO VII.5 – Equipo terminal y protocolos para servicios de telemática. Recomendaciones T.65 a T.101 y T.150 a T.390 (Comisión de Estudio VIII).

FASCÍCULO VII.6 – Equipo terminal y protocolos para servicios de telemática. Recomendaciones T.400 a T.418 (Comisión de Estudio VIII).

FASCÍCULO VII.7 – Equipo terminal y protocolos para servicios de telemática. Recomendaciones T.431 a T.564 (Comisión de Estudio VIII).

Tomo VIII

FASCÍCULO VIII.1 – Comunicación de datos por la red telefónica. Recomendaciones de la serie V (Comisión de Estudio XVII).

FASCÍCULO VIII.2 – Redes de comunicación de datos: servicios y facilidades, interfaces. Recomendaciones X.1 a X.32 (Comisión de Estudio VII).

FASCÍCULO VIII.3 – Redes de comunicación de datos: transmisión, señalización y conmutación, aspectos de red, mantenimiento, disposiciones administrativas. Recomendaciones X.40 a X.181 (Comisión de Estudio VII).

FASCÍCULO VIII.4 – Redes de comunicación de datos: Interconexión de sistemas abiertos (ISA) – Modelo y notación, definición del servicio. Recomendaciones X.200 a X.219 (Comisión de Estudio VII).

FASCÍCULO VIII.5 – Redes de comunicación de datos: Interconexión de sistemas abiertos (ISA) – Especificación de protocolos, pruebas de conformidad. Recomendaciones X.220 a X.290 (Comisión de Estudio VII).

FASCÍCULO VIII.6 – Redes de comunicación de datos: Interfuncionamiento entre redes, sistemas móviles de transmisión de datos, gestión interredes. Recomendaciones X.300 a X.370 (Comisión de Estudio VII).

FASCÍCULO VIII.7 – Redes de comunicación de datos: Sistemas de tratamiento de mensajes. Recomendaciones X.400 a X.420 (Comisión de Estudio VII).

FASCÍCULO VIII.8 – Redes de comunicación de datos: La guía. Recomendaciones X.500 a X.521 (Comisión de Estudio VII).

Tomo IX – Protección contra las perturbaciones. Recomendaciones de la serie K (Comisión de Estudio V) – Construcción, instalación y protección de los cables y otros elementos de planta exterior. Recomendaciones de la serie L (Comisión de Estudio VI).

Tomo X

FASCÍCULO X.1 – Lenguaje de especificación y descripción funcionales (LED). Criterios para la utilización de técnicas de descripción formal (TDF). Recomendación Z.100 y anexos A, B, C y E, Recomendación Z.110 (Comisión de Estudio X).

FASCÍCULO X.2 – Anexo D a la Recomendación Z.100: Directrices para el usuario del LED (Comisión de Estudio X).

FASCÍCULO X.3 – Anexo F.1 a la Recomendación Z.100: Definición formal del LED. Introducción (Comisión de Estudio X).

FASCÍCULO X.4 – Anexo F.2 a la Recomendación Z.100: Definición formal del LED. Semántica estática (Comisión de Estudio X).

FASCÍCULO X.5 – Anexo F.3 a la Recomendación Z.100: Definición formal del LED. Semántica dinámica (Comisión de Estudio X).

FASCÍCULO X.6 – Lenguaje de alto nivel del CCITT (CHILL). Recomendación Z.200 (Comisión de Estudio X).

FASCÍCULO X.7 – Lenguaje hombre-máquina (LHM). Recomendaciones Z.301 a Z.341 (Comisión de Estudio X).

ÍNDICE DEL FASCÍCULO VIII.7 DEL LIBRO AZUL

Recomendaciones X.400 a X.420

Redes de comunicación de datos:
Sistemas de tratamiento de mensajes

Rec. N.º		Página
X.400	Sistema de tratamiento de mensajes: visión de conjunto del sistema y del servicio . . .	3
X.402	Sistemas de tratamiento de mensajes: arquitectura global	75
X.403	Sistemas de tratamiento de mensajes: pruebas de conformidad	147
X.407	Sistemas de tratamiento de mensajes: convenios para la definición del servicio abstracto	200
X.408	Sistemas de tratamiento de mensajes: reglas de conversión de tipos de información codificada	228
X.411	Sistemas de tratamiento de mensajes: sistema de transferencia de mensajes: definición del servicio abstracto y procedimientos	272
X.413	Sistemas de tratamiento de mensajes: definición del servicio abstracto de almacenamiento de mensajes	426
X.419	Sistemas de tratamiento de mensajes: especificaciones de protocolo	502
X.420	Sistemas de tratamiento de mensajes: sistema de mensajería interpersonal	543

NOTAS PRELIMINARES

1 Las Cuestiones asignadas a cada Comisión de Estudio para el periodo de estudios 1989-1992 figuran en la Contribución N.º 1 de dicha Comisión.

2 En este fascículo, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una Administración de telecomunicaciones como una empresa privada de explotación de telecomunicaciones reconocida.

3 Los términos anexo y apéndice a las Recomendaciones de la serie X deberán interpretarse como sigue (salvo que se especifique lo contrario):

- el *anexo* a una Recomendación forma parte integrante de la misma;
- el *apéndice* a una Recomendación no forma parte integrante de la misma y tiene solamente por objeto proporcionar explicaciones o informaciones complementarias específicas a dicha Recomendación.

4 Algunas de las Recomendaciones de la serie X contenidas en este fascículo se desarrollaron conjuntamente y en colaboración con la ISO/CEI. En el cuadro que sigue se facilitan las referencias mutuas entre esas Recomendaciones y las normas ISO/CEI correspondientes.

Recomendación del CCITT	Norma ISO/CEI
X.400	ISO 10021-1, Information processing systems – Text communication – Message oriented text interchange system – Part 1: System and service overview [a].
X.402	ISO 10021-2, Information processing systems – Text communication – Message oriented text interchange system – Part 2: Overall architecture [a].
X.407	ISO 10021-3, Information processing systems – Text communication – Message oriented text interchange system – Part 3: Abstract service definition co nventions [a].
X.411	ISO 10021-4, Information processing systems – Text communication – Message oriented text interchange system – Part 4: Message transfer system: Abstract service definition and procedures [a].
X.413	ISO 10021-5, Information processing systems – Text communication – Message oriented text interchange system – Part 5: Message store: Abstract service definition. [a]
X.419	ISO 10021-6, Information processing systems – Text communication – Message oriented text interchange system – Part 6: Protocol specifications [a].
X.420	ISO 10021-7, Information processing systems – Text communication – Message oriented text interchange system – Part 7: Interpersonal messaging system [a].

[a] Actualmente a nivel de proyecto de norma internacional (PNI).

FASCÍCULO VIII.7

Recomendaciones X.400 a X.420

REDES DE COMUNICACIÓN DE DATOS: SISTEMAS DE TRATAMIENTO DE MENSAJES

PAGE INTENTIONALLY LEFT BLANK

PAGE LAISSEE EN BLANC INTENTIONNELLEMENT

Recomendación X.400 [1]

SISTEMA DE TRATAMIENTO DE MENSAJES: VISIÓN DE CONJUNTO DEL SISTEMA Y DEL SERVICIO

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión, controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) la necesidad de transferir y almacenar mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT;

(e) que las Recomendaciones de la serie X.500 definen los sistemas de guía;

(f) que los sistemas de tratamiento de mensajes se definen en la serie de Recomendaciones X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419;

(g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330;

(h) que varias Recomendaciones de la serie F describen los servicios públicos de tratamiento de mensajes: F.400, F.401, F.410 y F.420;

(i) que varias Recomendaciones de la serie F describen la intercomunicación entre los servicios públicos de tratamiento de mensajes y otros servicios: F.421, F.415 y F.422,

recomienda por unanimidad

que la visión de conjunto del sistema y del servicio de tratamiento de mensajes sea la definida en la presente Recomendación.

---

[1] La Recomendación F.400 es idéntica a la Recomendación X.400.

ÍNDICE

PARTE 1 – *Introducción*

0 *Introducción*

1 *Objeto*

2 *Referencias*

3 *Definiciones*

4 *Abreviaturas*

5 *Convenios*

PARTE 2 – *Descripción general de STM*

6 *Finalidad*

7 *Modelo funcional del STM*

- 7.1 Descripción del modelo STM
- 7.2 Estructura de los mensajes
- 7.3 Aplicación del modelo STM
- 7.4 Memoria de mensajes

8 *Servicio de transferencia de mensajes*

- 8.1 Depósito y entrega
- 8.2 Transferencia
- 8.3 Notificaciones
- 8.4 Agente de usuario
- 8.5 Memoria de mensajes
- 8.6 Unidad de acceso
- 8.7 Empleo del STRM en la prestación de servicios públicos

9 *Servicios de mensajería interpersonal (MIP)*

- 9.1 Modelo funcional del servicio de mensajería interpersonal (MIP)
- 9.2 Estructura de los mensajes IP
- 9.3 Notificaciones IP

10 *Intercomunicación con los servicios de entrega física*

- 10.1 Introducción
- 10.2 Configuraciones de organización

11 *Acceso especializado*

- 11.1 Introducción
- 11.2 Acceso teletex
- 11.3 Acceso télex

PARTE 3 – *Capacidades del STM*

12 *Denominación y direccionamiento*

- 12.1 Introducción
- 12.2 Nombre de guía
- 12.3 Nombres O/D
- 12.4 Direcciones O/D

13 *Utilización de la guía por el STM*

13.1 Introducción
13.2 Modelo funcional
13.3 Configuraciones físicas

14 *Listas de distribución en el STM*

14.1 Introducción
14.2 Propiedades de una LD
14.3 Depósito
14.4 Utilización de una guía por la LD
14.5 Expansión de la LD
14.6 Jerarquización
14.7 Control de repetición
14.8 Entrega
14.9 Control del bucle de encaminamiento
14.10 Notificaciones
14.11 Política de tratamiento de LD

15 *Capacidades de seguridad del STM*

15.1 Introducción
15.2 Riesgos que afectan a la seguridad al STM
15.3 Modelo de seguridad
15.4 Características de seguridad del STM
15.5 Gestión de la seguridad

16 *Conversión en el STM*

17 *Utilización del STM en la prestación de servicios públicos*

PARTE 4 – *Elementos de servicio*

18 *Finalidad*

19 *Clasificación*

19.1 Finalidad de la clasificación
19.2 Servicio de transferencia de mensajes básico
19.3 Facilidades facultativas de usuario del servicio TRM
19.4 Intercomunicación de los servicios TM/EF de base
19.5 Facilidades facultativas de usuario para la intercomunicación de los servicios TM/EF
19.6 Memoria de mensajes de base
19.7 Facilidades facultativas de usuario de la MM
19.8 Servicio de mensajería interpersonal básico
19.9 Facilidades facultativas de usuario del servicio MIP

Anexo A – Glosario de términos

Anexo B – Definiciones de los elementos de servicio

Anexo C – Cambios de los elementos de servicio a partir de 1984

Anexo D – Diferencias entre la Recomendación F.400 del CCITT y la norma ISO 10021-1

PARTE 1 – INTRODUCCIÓN

0 Introducción

La presente Recomendación forma parte de una serie de Recomendaciones sobre el tratamiento de mensajes. Esta serie proporciona una especificación completa de los sistemas de tratamiento de mensajes compuestos por cualquier número de sistemas abiertos cooperantes.

Los sistemas y servicios de tratamiento de mensajes permiten a los usuarios intercambiar mensajes empleando medios de almacenamiento y retransmisión. Un mensaje depositado por un usuario, el originador, es transmitido por el sistema de transferencia de mensajes (STRM), componente principal de un sistema más amplio de tratamiento de mensajes (STM), y entregado a continuación a uno o más usuarios destinatarios del mensaje.

El STM se compone de diversas entidades funcionales interconectadas. Los agentes de transferencia de mensajes (STM) cooperan en la ejecución de la función de transferencia de mensajes con almacenamiento y retransmisión. Los dispositivos de almacenamiento de mensajes (AM) constituyen el medio de almacenamiento de los mensajes y permiten el depósito, la extracción y gestión de éstos. Los agentes de usuario (AU) ayudan a los usuarios a obtener acceso al STM. Las unidades de acceso (UA) proporcionan enlaces con otros sistemas y servicios de comunicación de diversa naturaleza (por ejemplo, otros servicios telemáticos, servicios postales).

Esta Recomendación describe globalmente el sistema y el servicio correspondientes a las capacidades de tratamiento de mensajes.

1 Objeto

La presente Recomendación define globalmente el sistema y el servicio de un STM, y proporciona una descripción general de éste.

En otras Recomendaciones, se definen otros aspectos de los sistemas y servicios de tratamiento de mensajes. La distribución de las Recomendaciones que definen el sistema y los servicios de tratamiento de mensajes se muestra en el cuadro 1/X.400. Los servicios públicos construidos sobre un STM, así como el acceso a y desde el STM para servicios públicos se definen en las Recomendaciones de la serie F.400.

Los aspectos técnicos del STM se definen en las Recomendaciones de la serie X.400. La arquitectura global del STM se define en la Recomendación X.402.

CUADRO 1/X.400

Estructura de las Recomendaciones del STM

Nombre de la Recomendación o norma	STM mixto		Soporte mixto		CCITT solamente	
	CCITT	ISO	CCITT	ISO	Sistema	Servicio
STM: Visión de conjunto del sistema y del servicio	X.400	10021-1				F.400
STM: Arquitectura global	X.402	10021-2				
STM: Pruebas de conformidad					X.403	
STM: Convenios para la definición del servicio abstracto	X.407	10021-3				
STM: Reglas de conversión de los tipos de información codificada					X.408	
STM: STRM: Definición del servicio abstracto y procedimientos	X.411	10021-4				
STM: AM: Definición del servicio abstracto de almacenamiento de mensajes	X.413	10021-5				
STM: Especificaciones de protocolo	X.419	10021-6				
STM: Sistema de mensajería interpersonal	X.420	10021-7				
Acceso telemático al SMIP					T.330	
STM: Denominación y direccionamiento para servicios TM públicos						F.401
STM: Servicio público de transferencia de mensajes						F.410
STM: Intercomunicación con servicios públicos de entrega física						F.415
STM: Servicio MIP público						F.420
STM: Intercomunicación servicio MIP/télex						F.421
STM: Intercomunicación servicio MIP/teletex						F.422
ISA: Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT			X.200	7498		
ISA: Especificación de la notación de sintaxis abstracta uno (NSA.1)			X.208	8824		
ISA: Especificación de las reglas básicas de codificación para la notación de sintaxis abstracta uno (NSA.1)			X.209	8825		
ISA: Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT			X.217	8649		
ISA: Transferencia fiable: modelo y definición del servicio			X.218	9066-1		
ISA: Operaciones a distancia: modelo, notación y definición del servicio			X.219	9072-1		
ISA: Especificación del protocolo del control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT			X.227	8650		
ISA: Transferencia fiable: especificación del protocolo			X.228	9066-2		
ISA: Operaciones a distancia: especificación del protocolo			X.229	9072-2		

2 Referencias

En esta Recomendación se citan los siguientes documentos:

Recomendación F.60	Disposiciones relativas a la explotación del servicio télex internacional
Recomendación F.69	Plan de códigos télex de destino
Recomendación F.72	Almacenamiento y retransmisión télex internacional – Principios generales y aspectos operacionales
Recomendación F.160	Disposiciones generales relativas a la explotación de los servicios facsímil públicos internacionales
Recomendación F.200	Servicio teletex
Recomendación F.300	Servicio videotex
Recomendación F.400	Sistema de tratamiento de mensajes: Visión de conjunto del sistema y del servicio (véase también ISO 10021-1)
Recomendación F.401	Servicios de tratamiento de mensajes: Denominación y direccionamiento para los servicios públicos de tratamiento de mensajes
Recomendación F.410	Servicios de tratamiento de mensajes: Servicio público de transferencia de mensajes
Recomendación F.415	Servicios de tratamiento de mensajes: Intercomunicación con los servicios públicos de entrega física
Recomendación F.420	Servicios de tratamiento de mensajes: Servicio público de mensajería interpersonal
Recomendación F.421	Servicios de tratamiento de mensajes: Intercomunicación entre el servicio MIP y el servicio télex
Recomendación F.422	Servicios de tratamiento de mensajes: Intercomunicación entre el servicio MIP y el servicio teletex
Recomendación T.61	Repertorio de caracteres y juegos de caracteres codificados para el servicio teletex internacional
Recomendación T.330	Acceso telemático al servicio de mensajería interpersonal
Recomendación U.80	Almacenamiento y retransmisión télex internacional – Acceso desde el télex
Recomendación U.204	Interfuncionamiento entre el servicio télex y el servicio público de mensajería interpersonal
Recomendación X.200	Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT (véase también ISO 7498)
Recomendación X.208	Especificación de la notación de sintaxis abstracta uno (NSA.1) (véase también ISO 8824)
Recomendación X.209	Especificación de las reglas básicas de codificación para la notación de sintaxis abstracta uno (NSA.1) (véase también ISO 8825)
Recomendación X.217	Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT (véase también ISO 8649)
Recomendación X.218	Transferencia fiable: Modelo y definición del sistema (véase también ISO/CEI 9066-1)
Recomendación X.219	Operaciones a distancia: Modelo, notación y definición del servicio (véase también ISO/CEI 9072-1).
Recomendación X.400	Sistema de tratamiento de mensajes: Visión de conjunto del sistema y del servicio (véase también ISO/CEI 10021-1)
Recomendación X.402	Sistemas de tratamiento de mensajes: Arquitectura global (véase también ISO/CEI 10021-2)
Recomendación X.403	Sistemas de tratamiento de mensajes: Pruebas de conformidad
Recomendación X.407	Sistemas de tratamiento de mensajes: Convenios para la definición del servicio abstracto (véase también ISO/CEI 10021-3)
Recomendación X.408	Sistemas de tratamiento de mensajes: Reglas de conversión de los tipos de información codificada
Recomendación X.411	Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes: definición del servicio abstracto y procedimientos (véase también ISO/CEI 10021-4)

Recomendación X.413 Sistemas de tratamiento de mensajes: Definición del servicio abstracto de almacenamiento de mensajes (véase también ISO/CEI 10021-5)

Recomendación X.419 Sistemas de tratamiento de mensajes: Especificaciones de protocolo (véase también ISO/CEI 10021-6)

Recomendación X.420 Sistemas de tratamiento de mensajes: Sistema de mensajería interpersonal (véase también ISO/CEI 10021-7)

Recomendación X.500 La Guía – Visión de conjunto de conceptos, modelos y servicios (véase también ISO/CEI 9594-1)

Recomendación X.501 La Guía – Modelos (véase también ISO/CEI 9594-2)

Recomendación X.509 La Guía – Marco de autenticación (véase también ISO/CEI 9594-8)

Recomendación X.511 La Guía – Definición del servicio abstracto (véase también ISO/CEI 9594-3)

Recomendación X.518 La Guía – Procedimientos para operación distribuida (véase también ISO/CEI 9594-4)

Recomendación X.519 La Guía – Especificaciones de protocolos (véase también ISO/CEI 9594-5)

Recomendación X.520 La Guía – Tipos de atributo seleccionados (véase también ISO/CEI 9594-6)

Recomendación X.521 La Guía – Clases de objeto seleccionadas (véase también ISO/CEI 9594-7)

3 Definiciones

Esta Recomendación utiliza los términos relacionados a continuación, así como los definidos en el anexo A.

Las definiciones de los elementos de servicio aplicables al STM se encuentran en el anexo B.

3.1 *Interconexión de sistemas abiertos*

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.200:

a) capa de aplicación,
b) proceso de aplicación,
c) interconexión de sistemas abiertos,
d) modelo de referencia ISA.

3.2 *Sistemas de Guía*

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.500:

a) inscripción de guía,
b) agente del sistema de guía,
c) sistema de guía,
d) agente de usuario de guía.

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.501:

e) atributo,
f) grupo,
g) miembro,
h) nombre.

4 Abreviaturas

A	Adicional
DGAD	Dominio de gestión de administración
AU	Unidad de acceso
AC	Acuerdo contractual
LD	Lista de distribución
ASG	Agente de sistema de guía
AUG	Agente de usuario de la guía

E	Esencial
TIC	Tipo de información codificada
E/S	Entrada/salida
IP	Interpersonal
MIP	Mensajería interpersonal
SMIP	Sistema de mensajería interpersonal
DG	Dominio de gestión
TM	Tratamiento de mensajes
STM	Sistema de tratamiento de mensajes
MM	Memoria de mensajes; almacenador de mensajes (AM)
TRM	Transferencia de mensajes
ATM	Agente de transferencia de mensajes
STRM	Sistema de transferencia de mensajes
N/A	No aplicable
O/D	Originador/destinatario
ISA	Interconexión de sistemas abiertos
EF	Entrega física
UAEF	Unidad de acceso de entrega física
SEF	Sistema de entrega física
PM	Por mensaje
PD	Por destinatario
DGPR	Dominio de gestión privado
UATLXP	Unidad de acceso de télex público
ATLM	Agente telemático
UATLX	Unidad de acceso al télex
TTX	Teletex
AU	Agente de usuario

5 Convenios

En esta Recomendación, la expresión «Administración» se utiliza como forma abreviada para indicar una Administración de telecomunicaciones, una empresa privada de explotación reconocida y, en el caso de intercomunicación con el servicio de entrega física, una Administración postal.

Nota – Esta Recomendación es idéntica a la Recomendación F.400. Debido a la armonización deseada con la ISO, se han adoptado convenios de las normas de la ISO para la estructura de este texto. Dichos convenios difieren del estilo del CCITT. Las demás Recomendaciones de la serie X.400 son conformes a los convenios del CCITT.

PARTE 2 – DESCRIPCIÓN GENERAL DEL STM

6 Finalidad

La presente Recomendación forma parte de una serie de Recomendaciones y describe el modelo del sistema de tratamiento de mensajes y los elementos del servicio de tratamiento de mensajes (STM). En ella se pasa revista a las capacidades de un STM que utilizan las Administraciones para proporcionar servicios TM públicos que permiten a los abonados intercambiar mensajes con almacenamiento y retransmisión.

El sistema de tratamiento de mensajes está diseñado de acuerdo con los principios del modelo de referencia de interconexión de sistemas abiertos (modelo de referencia ISA) para aplicaciones del CCITT (Recomendación X.200) y utiliza los servicios de capa de presentación y servicio ofrecidos por otros elementos de servicio de aplicación más generales. Un STM puede construirse utilizando cualquier red que se adapte al objeto de la ISA. El servicio de transferencia de mensajes proporcionado por el STRM es independiente de la aplicación. Un ejemplo de aplicación normalizada es el servicio MIP. Los sistemas de extremo pueden utilizar el servicio de TRM para aplicaciones específicas que se definen en forma bilateral.

Los servicios de tratamiento de mensajes proporcionados por las Administraciones pertenecen al grupo de servicios telemáticos definidos en las Recomendaciones de la serie F.

Otros servicios telemáticos, el télex (Recomendaciones F.60, F.160, F.200, F.300, etc.), los servicios de transmisión de datos (X.1) o los servicios de entrega física (F.415) ganan acceso al servicio MIP y se intercomunican con él o entre sí mediante unidades de acceso.

Los elementos de servicio son las características de servicio suministradas a través de entidades de aplicación. Se considera que estos elementos de servicio son componentes de los servicios suministrados a los usuarios, y son elementos de un servicio básico, o bien *facilidades de usuario facultativas*, clasificadas en *facilidades de usuario facultativas esenciales*, o *facilidades de usuario facultativas adicionales.*

7 Modelo funcional del STM

El modelo funcional del STM sirve de instrumento para formular Recomendaciones sobre el STM y describir los conceptos básicos que pueden ser representados gráficamente. Comprende varios componentes funcionales diferentes que actúan conjuntamente para proporcionar servicios TM. El modelo puede aplicarse a diversas configuraciones físicas y organizaciones diferentes.

7.1 *Descripción del modelo STM*

En la figura 1/X.400 se da una visión de conjunto de las funciones del modelo STM. En este modelo, un usuario es una persona o un proceso de computador. Los usuarios pueden ser usuarios directos (es decir, efectuar el tratamiento de mensajes utilizando el STM directamente) o usuarios indirectos [es decir, efectuar el tratamiento de mensajes a través de otro sistema de comunicación (por ejemplo, un sistema de entrega física), que esté vinculado al STM]. Un usuario es un originador (cuando envía un mensaje), o un destinatario (cuando recibe un mensaje). Los elementos de servicio del tratamiento de mensajes definen el conjunto de tipos de mensajes y las capacidades que permiten a un originador transferir mensajes de estos tipos a uno o más destinatarios.

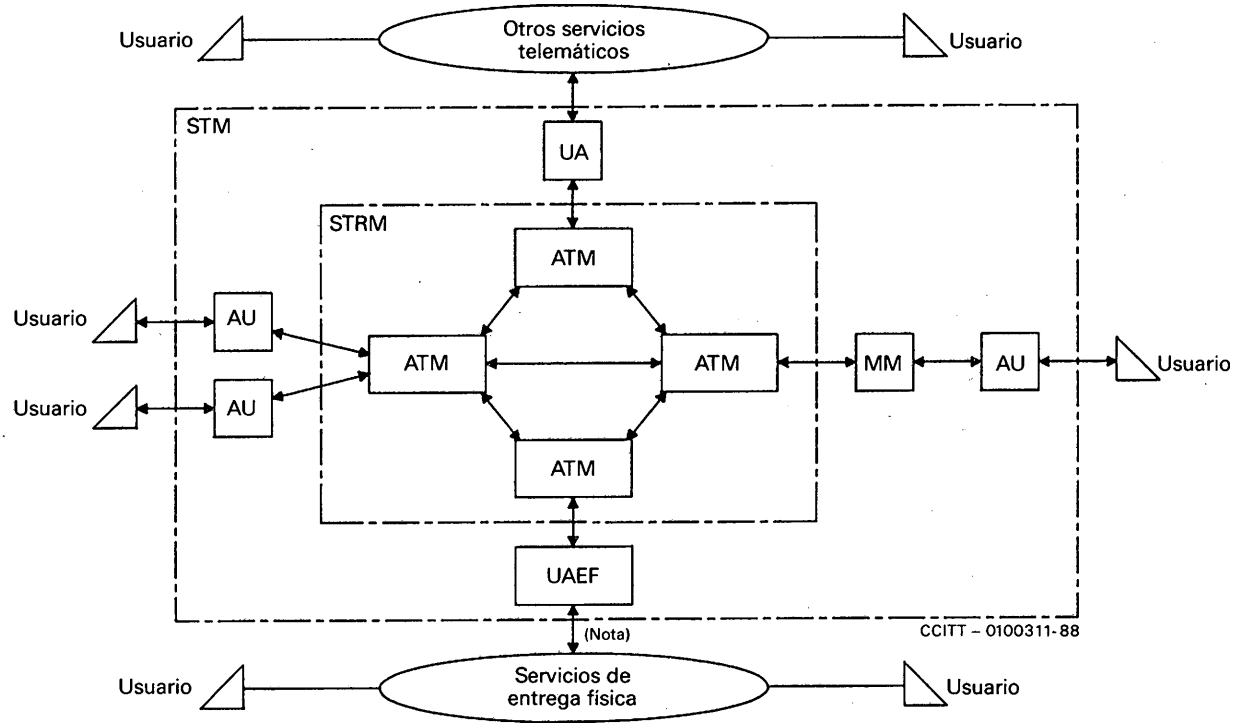
Un originador prepara los mensajes con la ayuda de su agente de usuario. Un agente de usuario (AU) es un proceso de aplicación que interactúa con el sistema de transferencia de mensajes (STRM) o con una memoria de mensajes (MM) para depositar mensajes en nombre de un solo usuario. Los mensajes que el STRM recibe en depósito, los entrega a uno o más AU receptores, unidades de acceso (UA) o MM pudiendo devolver notificaciones al originador. Las funciones realizadas únicamente por el AU y no normalizadas como parte de los elementos de servicio del tratamiento de mensajes se denominan funciones locales. Un AU puede aceptar la entrega de mensajes directamente del STRM o bien puede utilizar la capacidad de la MM para recibir mensajes entregados, para su posterior extracción por el AU.

El STRM comprende varios agentes de transferencia de mensajes (ATM). Operando juntos, en forma de almacenamiento y retransmisión el STRM transfiere mensajes y los entrega a los correspondientes destinatarios.

El acceso de usuarios indirectos del STM se efectúa por medio de los UA. La entrega a usuarios indirectos del STM se efectúa por medio de los UA, al igual que la entrega física, por medio de la unidad de acceso de entrega física (UAEF).

La memoria de mensajes (MM) es una capacidad facultativa de propósito general del STM que actúa como intermediario entre el AU y el ATM. La MM se describe en el modelo funcional del STM que se muestra en la figura 1/X.400. La MM es una entidad funcional cuya finalidad primaria es efectuar el almacenamiento y permitir la extracción de los mensajes entregados. La MM también permite el depósito desde el AU y la alerta al mismo.

La colección de UA, MM, AU y ATM se denomina sistema de tratamiento de mensajes (STM).



Nota – La entrada de mensajes desde los servicios de EF al STM debe ser objeto de ulterior estudio. El flujo indicado de los servicios de EF hacia la UAEF corresponde a las notificaciones.

FIGURA 1/X.400

Modelo funcional del STM

7.2 *Estructura de los mensajes*

En la figura 2/X.400, se muestra la estructura básica de los mensajes transmitidos por el STRM. Un mensaje se compone de un sobre y un contenido. El sobre lleva la información que utiliza el STRM al transferir el mensaje dentro del STRM. El contenido es la información que el AU originador desea entregar a uno o más AU destinatarios. El STRM no modifica ni examina el contenido, salvo para su conversión (véase el § 16).

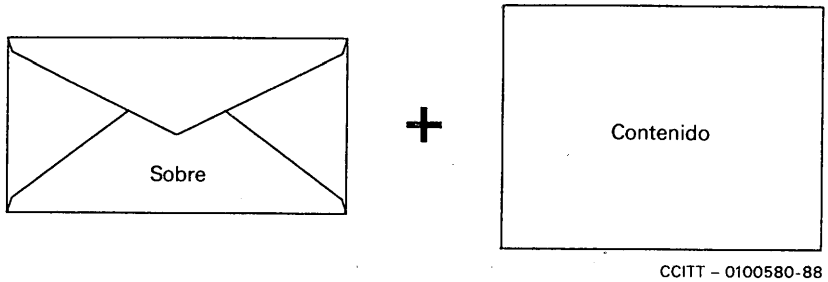


FIGURA 2/X.400

Estructura básica de los mensajes

7.3 *Aplicación del modelo STM*

7.3.1 *Correspondencia física*

Los usuarios acceden a los AU con fines de procesamiento de mensajes, por ejemplo, para crear, presentar o archivar mensajes. Un usuario puede interactuar con su AU a través de un dispositivo o proceso de entrada/salida (por ejemplo, teclado, unidad de visualización, impresora, etc.). Un AU puede realizarse como un (conjunto de) proceso(s) de computador en un terminal inteligente.

Un AU y un ATM pueden estar ubicados en el mismo sistema, o un AU/MM pueden estar realizados en sistemas físicamente separados. En el primer caso, el AU tiene acceso a los elementos de servicio TRM interactuando directamente con el ATM en el mismo sistema. En el segundo caso, el AU debe comunicarse con el ATM a través de protocolos normalizados especificados para el STM. Es posible también que un ATM se realice en un sistema AU o sin MM.

Las figuras 3/X.400 y 4/X.400 se muestran algunas configuraciones físicas posibles. Los diferentes sistemas físicos pueden estar conectados por medio de conexiones directas o de red conmutada.

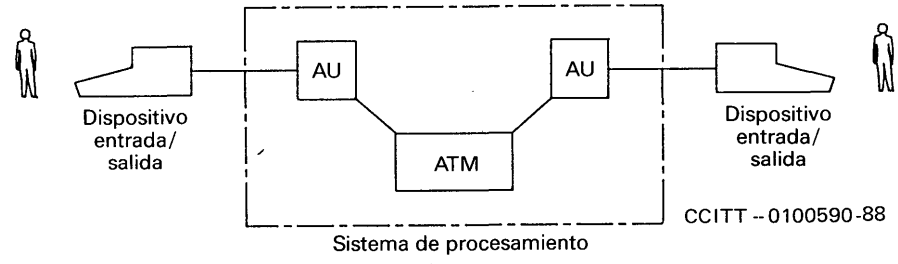


FIGURA 3/X.400

UA y ATM corresidentes

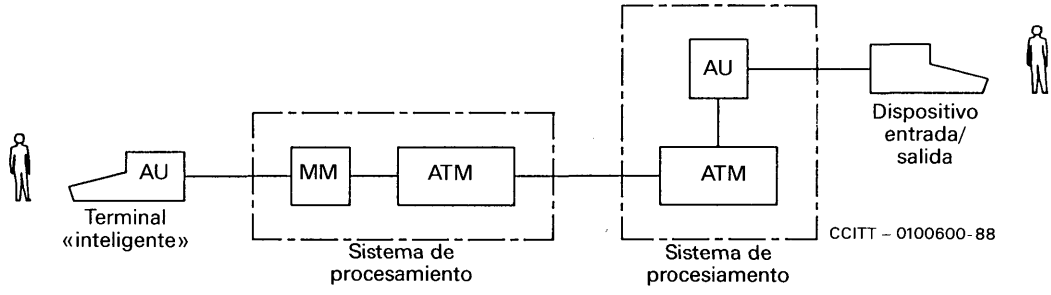


FIGURA 4/X.400

AU autónomo y MM/ATM corresidentes

7.3.2 *Relación de correspondencia orgánica*

Una Administración u organización puede desempeñar diversos papeles al proporcionar servicios de tratamiento de mensajes. En este contexto, una organización puede ser una empresa o una organización no comercial.

La colección de menos un ATM, cero o más AU, cero o más MM y cero o más UA explotados por una Administración u organización constituye un dominio de gestión (DG). Un DG manejado por una Administración se denomina dominio de gestión de Administración (DGAD). Un DG manejado por una organización, que no sea una Administración, se denomina dominio de gestión privado (DGPR). Un DG proporciona servicios de tratamiento de mensajes según la clasificación de elementos de servicios descrita en el § 19. La figura 5/X.400 muestra las relaciones entre los dominios de gestión.

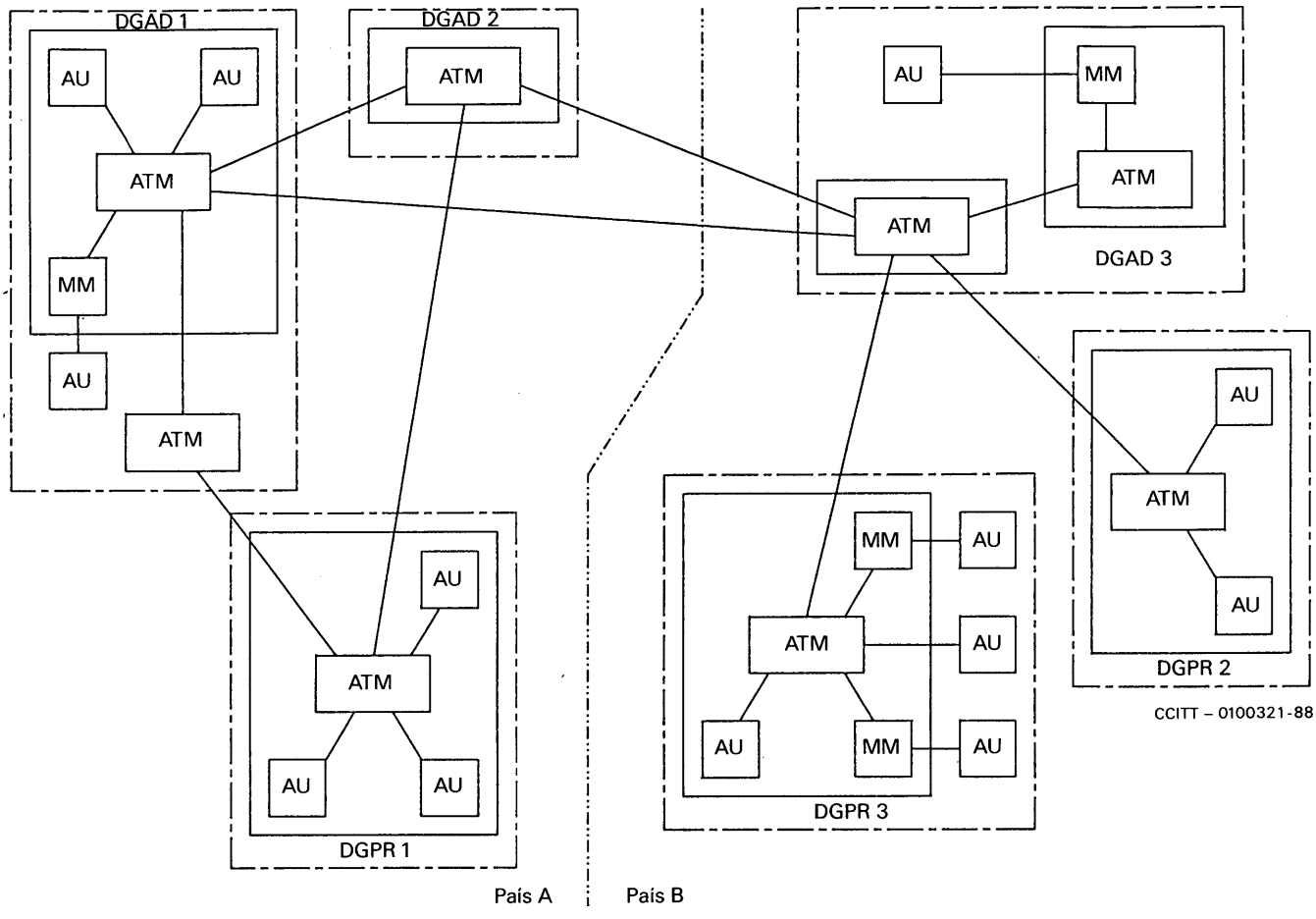


FIGURA 5/X.400

Relaciones entre los dominos de gestión

Nota 1 – Debe reconocerse que la provisión de soporte de sistemas privados de mensajería por miembros del CCITT cae dentro del marco de los reglamentos nacionales. Así, las posibilidades mencionadas en este punto pueden o no ser ofrecidas por una Administración que proporcione servicios de tratamiento de mensajes. Además, los AU descritos en la figura 5/X.400 no implican que el AU que pertenece a un DG debe encontrarse exclusivamente en el mismo país que su DG.

Nota 2 – Las interacciones directas entre los DGPR y las interacciones internas dentro de un DG están fuera del ámbito de esta Recomendación.

Nota 3 – Se considera que, en el contexto del CCITT una Administración que maneja un DGAD es un miembro de la UIT o una empresa privada de explotación reconocida (EPER) registrada por un país en la UIT.

7.3.3 *Dominio de gestión de administración*

En un país pueden existir uno o más DGAD. Un DGAD se caracteriza porque proporciona funciones de relevo entre otros dominios de gestión y la provisión del servicio de transferencia de mensajes para las aplicaciones proporcionadas dentro del DGAD.

Una Administración puede proporcionar a sus usuarios acceso al DGAD en una o más de las siguientes formas:

- usuario a AU proporcionado por la Administración,
- AU privado a ATM de la Administración,
- AU privado a MM de la Administración,
- ATM privado a ATM de la Administración,
- usuario a UA proporcionada por la Administración.

Véanse también los ejemplos de configuraciones de las figuras 3/X.400 y 4/X.400.

Los AU proporcionados por la Administración pueden existir como parte de un terminal inteligente que el usuario puede utilizar para acceder al STM. También pueden existir como parte del equipo residente de la Administración que forma parte del STM, en cuyo caso el usuario obtiene acceso al AU por medio de un dispositivo de entrada/salida (E/S).

En el caso de un AU privado, el usuario tiene un AU privado autónomo que interactúa con el ATM o la MM proporcionado por la Administración, utilizando las funciones de depósito, entrega y recuperación. Un AU privado autónomo puede asociarse con una o más MM, siempre que se respeten los convenios de denominación necesarios.

Un ATM privado como parte de un DGPR puede acceder a uno o más DGAD en un país, de acuerdo a los reglamentos nacionales.

El acceso se puede también dar por medio de las AU proporcionadas por la Administración, tal como se indica en los § 10 y 11.

7.3.4 *Dominio de gestión privado*

Una organización que no sea una Administración puede tener uno o más ATM, cero o más AU, UA y MM que forman un DGPR que puede interactuar con un DGAD, de DG a DG (ATM a ATM). Un DGPR se caracteriza porque proporciona funciones de mensajería dentro de ese dominio de gestión.

Se considera que un DGPR existe completamente dentro de un país. Dentro de ese país, el DGPR puede acceder a uno o más DGAD como se muestra en la figura 5/X.400. Sin embargo, en el caso de una interacción específica entre DGPR y DGAD (como cuando se transfiere un mensaje entre DG), se considera que el DGPR está asociado únicamente con dicho DGAD. Un DGPR no actuará como relevo entre dos DGAD.

En la interacción entre un DGPR y un DGAD, el DGAD asume la responsabilidad de las acciones del DGPR que están relacionadas con la interacción. Además, de garantizar que el DGPR proporciona debidamente el servicio de transferencia de mensajes, el DGAD debe asegurar que se realicen correctamente las funciones de contabilidad, registro cronológico, calidad de servicio, exclusividad de nombres y operaciones conexas del DGPR. Como asunto nacional, el nombre de un DGPR puede ser único a nivel nacional o relativo al DGAD asociado. Si un DGPR está asociado con más de un DGAD, puede tener más de un nombre.

7.4 *Memoria de mensajes*

Como los AU pueden realizarse con una gran variedad de equipos, incluyendo computadores personales, la MM puede completar un AU realizado, por ejemplo, en un computador personal, proporcionando un mecanismo de almacenamiento disponible en forma continua, más seguro, para aceptar la entrega de mensajes por cuenta del agente del usuario. La capacidad de recuperación de la MM proporciona, a los usuarios que se abonan a una MM, la capacidad básica de recuperación de mensajes aplicable potencialmente a todos los tipos de mensajes. La figura 6/X.400 muestra la entrega y posterior recuperación de mensajes que son entregados a una MM y el depósito indirecto de mensajes por medio de la MM.

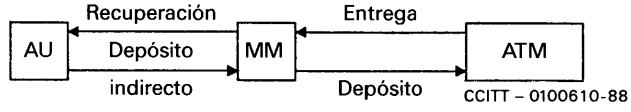


FIGURA 6/X.400

Depósito y entrega con una MM

Una AM actúa por cuenta de un solo usuario (una dirección O/D), es decir no proporciona a varios usuarios una capacidad MM común o compartida. Véase también DGPR3 de la figura 5/X.400.

Cuando existe el abono a una MM, todos los mensajes destinados al AU son entregados únicamente a la MM. El AU, si funciona «en línea», puede recibir alertas cuando ciertos mensajes son entregados a la MM. Los mensajes entregados a una MM se consideran, desde la perspectiva del STRM, como entregados.

Cuando un AU deposita un mensaje por medio de la MM, la MM en general es transparente y lo deposita en el ATM antes de confirmar al AU el éxito del depósito. Sin embargo, la MM puede ampliar el mensaje, si el AU solicita el reenvío de mensajes existentes en la MM.

Los usuarios también cuentan con la capacidad de solicitar a la MM que reenvíe automáticamente ciertos mensajes inmediatamente después de entregados.

Los elementos de servicio describen las características de una MM se definen en el anexo B y se clasifican en el § 19. Los usuarios disponen de una posibilidad, sobre la base de diversos criterios, de obtener cuentas y listas de mensajes, de capturar mensajes y de borrar mensajes, contenidos en ese momento en la MM.

7.4.1 *Configuraciones físicas*

La MM puede encontrarse situada físicamente, respecto al ATM, de diversas maneras. La MM puede estar ubicado junto al AU, junto al ATM, o ser autónomo. Desde un punto de vista exterior, un AU y una MM coubicados no pueden diferenciarse de un AU autónomo. La coubicación de la MM con el ATM ofrece ventajas significativas que probablemente lo conviertan en la configuración predominante.

7.4.2 *Configuraciones de organización*

Los DGAD o los DGPR pueden operar MM. En el caso de una MM suministrada por una Administración, el abonado puede proporcionar su propio AU o hacer uso de un AU proporcionado por la Administración por medio de un dispositivo de entrada/salida. En ambos casos, todos los mensajes de abonados son entregados a la MM para su ulterior recuperación.

Las configuraciones físicas y de organización descritas anteriormente son únicamente ejemplos y pueden existir otros casos igualmente válidos.

8 Servicio de transferencia de mensajes

El STRM proporciona el servicio de transferencia de mensajes general, con almacenamiento y retransmisión, independientemente de la aplicación. Los elementos de servicio que configuran las características del servicio TRM se definen en el anexo B y se clasifican en el § 19. El servicio público de transferencia de mensajes proporcionado por las Administraciones se describe en la Recomendación F.410.

8.1 *Depósito y entrega*

El STRM proporciona los medios que permiten a los AU intercambiar mensajes. Hay dos interacciones básicas entre los ATM y los AU y/o MM.

1) La interacción de depósito es el medio por el cual un AU o MM de origen transfiere a un ATM el contenido de un mensaje y el sobre de depósito. El sobre de depósito contiene la información que necesita el STRM para proporcionar los elementos de servicio solicitados.
2) La interacción de entrega es el medio por el cual el ATM transfiere a un AU o MM destinatario el contenido de un mensaje más el sobre de entrega. El sobre de entrega contiene información relativa a la entrega del mensaje.

En las interacciones de depósito y de entrega, la responsabilidad del mensaje se transfiere entre el STRM y el AU o la MM.

8.2 *Transferencia*

Comenzando en el ATM del originador, cada ATM transfiere el mensaje a otro ATM hasta que el mensaje alcanza al ATM de destino, el cual lo entrega entonces al AU o la MM de destino utilizando la interacción de entrega.

La interacción de transferencia es el medio por el cual un ATM transfiere a otro ATM el contenido de un mensaje más el sobre de transferencia. El sobre de transferencia contiene información relativa a la operación del STRM más la información que el STRM necesita para proporcionar los elementos de servicio solicitados por el AU de origen.

Los ATM transfieren mensajes que contienen muchos tipos de información codificada en binario. Los ATM no interpretan ni modifican el contenido de los mensajes a menos que realicen una conversión.

8.3 *Notificaciones*

Las notificaciones en el servicio de TRM pueden ser de entrega y de no entrega. Cuando un mensaje o sonda no puede ser entregado por el STRM, se genera una notificación de no entrega que se devuelve al originador en un informe que así lo indica. Además, un originador puede, al hacer el depósito, solicitar específicamente el acuse de la entrega correcta por medio del elemento de servicio de notificación de entrega.

8.4 *Agente de usuario*

El AU utiliza el servicio TRM proporcionado por el STRM. Un AU es una entidad funcional mediante la cual un usuario directo único efectúa un tratamiento de mensajes.

Los AU se agrupan en clases basadas en el tipo del contenido de los mensajes que pueden tratar. El STRM proporciona a los AU la posibilidad de identificar su clase al enviar mensajes a otros AU. Los AU de una misma clase se denominan AU cooperantes, puesto que cooperan entre sí para mejorar la comunicación entre sus respectivos usuarios.

Nota – Un AU puede admitir más de un tipo de contenido de mensajes y por lo tanto pertenecer a varias clases de AU.

8.5 *Memoria de mensajes*

La memoria de mensajes (MM) utiliza el servicio TRM proporcionado por el STRM. Una MM es una entidad funcional asociada con un AU de usuario. El usuario puede utilizarlo para entregar mensajes y para extraer mensajes que hayan sido entregados a la MM.

8.6 *Unidad de acceso*

Una unidad de acceso (UA) emplea el servicio TRM proporcionado por el STRM. Un UA es una entidad funcional asociada con un ATM para proporcionar la intercomunicación entre el STM y otro sistema o servicio.

8.7 *Empleo del STRM en la prestación de diversos servicios*

El STRM es utilizado por servicios específicos a una aplicación para proporcionar servicios de tratamiento de mensajes de diversos tipos. El servicio de mensajería interpersonal, descrito en el § 9 es un ejemplo de lo anterior. Sobre la base del STRM, pueden establecerse otros servicios, ya sea con Recomendaciones correspondientes o como aplicaciones privadas.

9 Servicio de mensajería interpersonal (MIP)

El servicio de mensajería interpersonal (MIP) proporciona a un usuario los elementos que lo ayudarán a comunicar con otros usuarios del servicio MIP. El servicio MIP utiliza las capacidades del servicio TRM para enviar y recibir mensajes interpersonales. Los elementos de servicio que describen las características del servicio MIP se definen en el anexo B, y se clasifican en el § 19. La prestación del servicio público de mensajería interpersonal por las Administraciones se describe en la Recomendación F.420.

9.1 *Modelo funcional del servicio de mensajería interpersonal (MIP)*

La figura 7/X.400 muestra el modelo funcional del servicio MIP. Los AU utilizados en el servicio MIP (AU de MIP) comprenden una clase específica de AU cooperantes. Las unidades de acceso opcionales que se muestran (ATLM, UATLXP) permiten a los usuarios teletex y télex intercomunicar con el servicio MIP. La unidad de acceso opcional (ATLM) también permite a los usuarios teletex participar en el servicio MIP (véase también el § 11). La unidad de acceso de entrega física (UAEF) opcional permite a los usuarios de MIP enviar mensajes a usuarios fuera del servicio MIP que no tienen acceso al STM. El almacén de mensajes puede ser utilizado opcionalmente por los usuarios MIP para recibir la entrega de mensajes en su nombre.

9.2 *Estructura de los mensajes IP*

La clase MIP de AU crea mensajes que tienen un contenido específico para el MIP. El contenido específico que se envía de un AU de MIP a otro es el resultado de la composición y envío por un originador de un mensaje denominado mensaje IP. En la figura 8/X.400 se muestra la estructura de un mensaje IP y su relación con la estructura básica del mensaje STM. Cuando se transfiere a través del STRM el mensaje IP se transmite con un sobre.

En la figura 9/X.400 se muestra una analogía entre un memorándum de oficina típico y la estructura del mensaje IP correspondiente. El mensaje IP contiene información (por ejemplo, a:, cc:, asunto,) que es proporcionada por el usuario y transformada por el AU de MIP en el encabezamiento de mensaje IP. La información principal que el usuario desea comunicar (el cuerpo del memorándum) está contenida dentro del cuerpo del mensaje IP. En este ejemplo, el cuerpo contiene dos tipos de información codificada: texto y facsímil, que conforman lo que se denomina partes del cuerpo. En general, un cuerpo de mensaje IP puede consistir en varias partes del cuerpo, cada una de las cuales puede ser un tipo de información codificada diferente, tal como voz, texto, facsímil y gráficos.

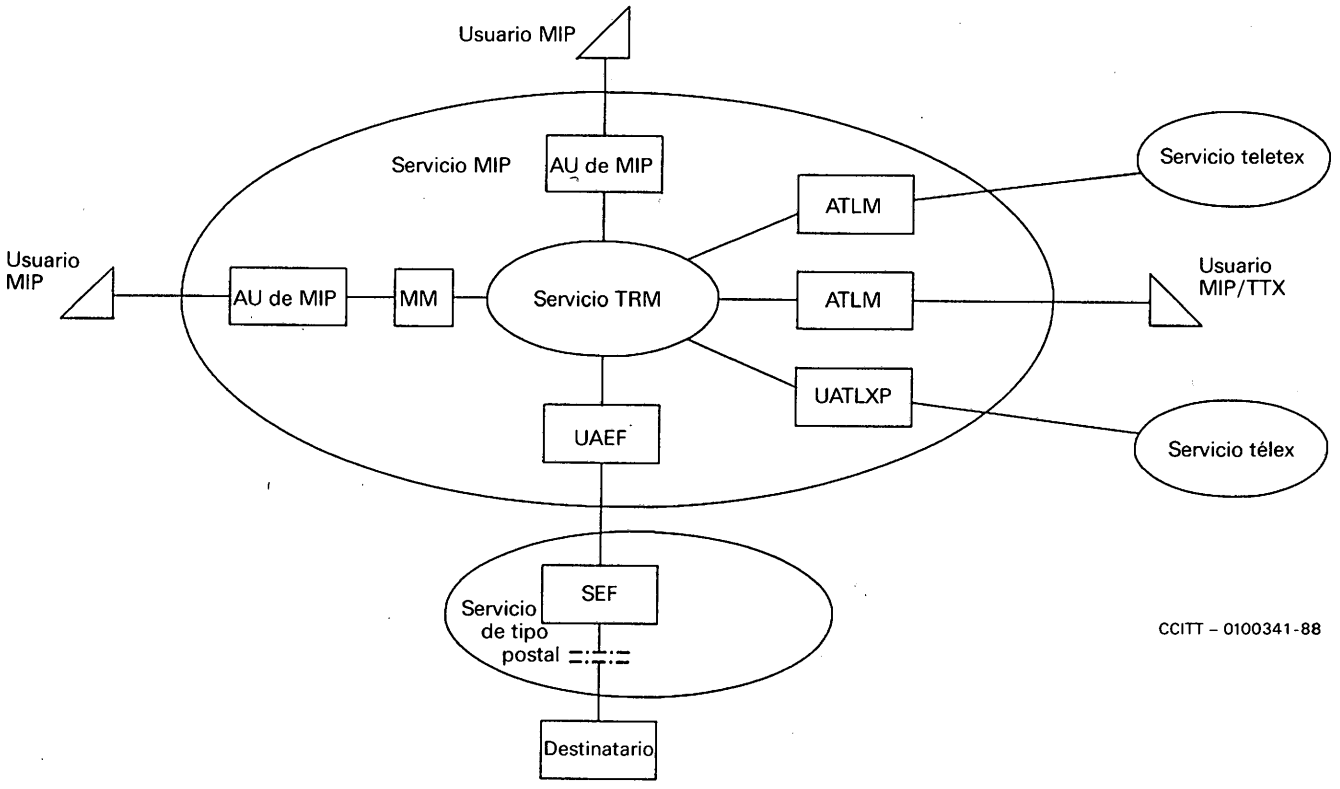


FIGURA 7/X.400

Modelo funcional del servicio MIP

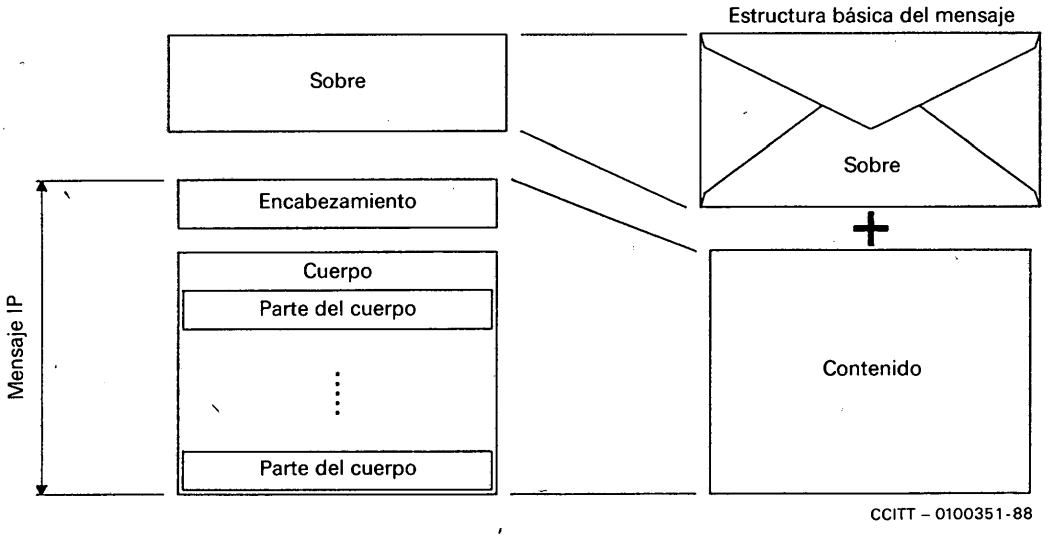


FIGURA 8/X.400

Estructura del mensaje IP

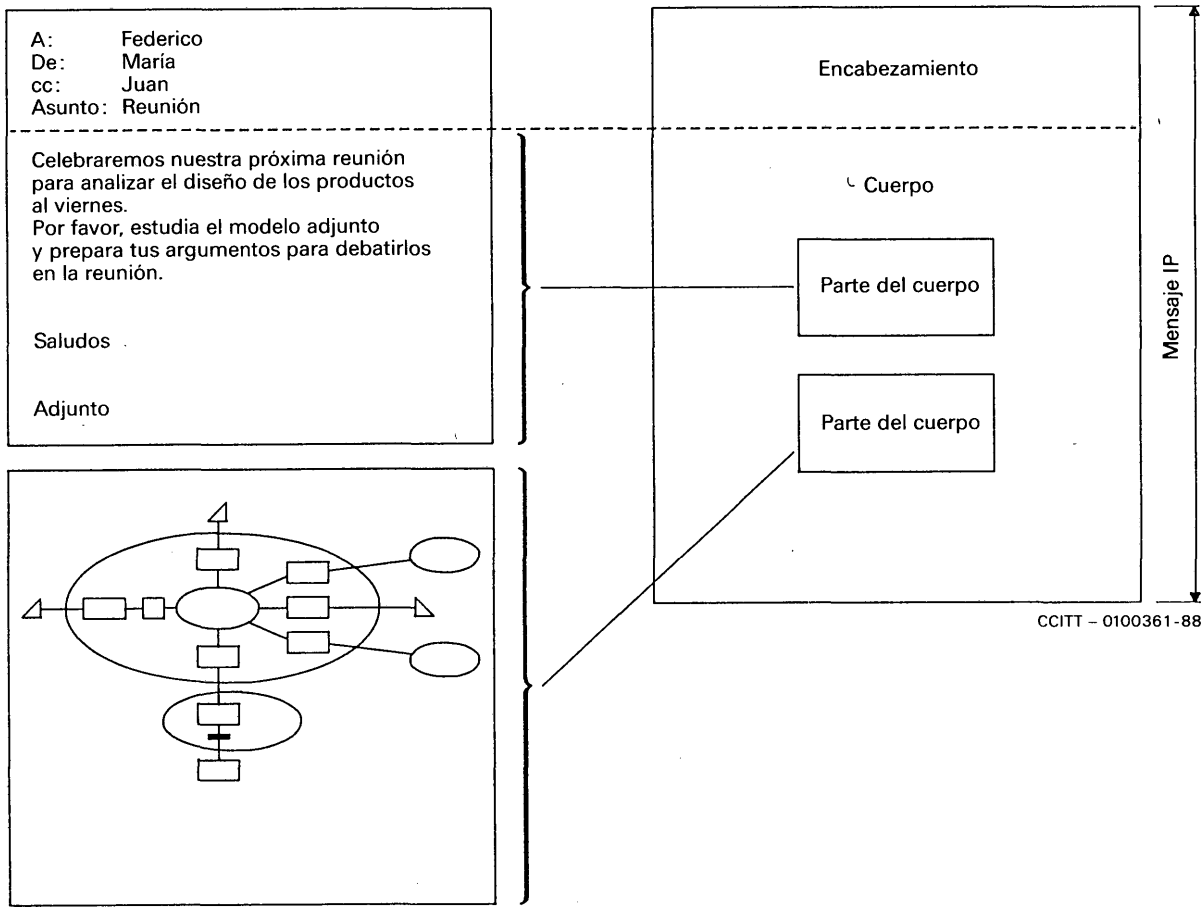


FIGURA 9/X.400

Estructura del mensaje IP correspondiente a un memorándum típico

9.3 *Notificaciones IP*

En el servicio MIP, un usuario puede solicitar la notificación de la recepción o de la no recepción de un mensaje por un destinatario. Estas notificaciones son solicitadas por un originador y se generan como resultado de alguna acción (como la lectura o no lectura del mensaje) del destinatario. En ciertos casos la notificación de no recepción la genera automáticamente el AU del destinatario.

10 Intercomunicación con los servicios de entrega física

10.1 *Introducción*

El valor de los sistemas de tratamiento de mensajes puede aumentar conectándolos a sistemas de entrega física (EF), como el servicio postal tradicional. Esto permitirá la entrega física (por ejemplo en copia impresa) de mensajes originados dentro del STM a destinatarios ajenos al STM y en algunos casos permitirá devolver notificaciones del servicio EF a un originador STM. La capacidad de originar mensajes en el servicio EF para su depósito en el STM por medio de la UAEF requiere ulterior estudio. La capacidad de intercomunicación entre los servicios EF y TM es una capacidad facultativa del STM y se puede emplear para cualquier aplicación como la MIP. Todos los usuarios del STM tendrán la posibilidad de generar mensajes para su ulterior entrega física. La figura 10/X.400 muestra el modelo funcional de este interfuncionamiento. La provisión de intercomunicación entre los servicios públicos de tratamiento de mensajes ofrecidos por las Administraciones y los servicios de EF se describe en la Recomendación F.415. Los elementos de servicio que describen las características de esta intercomunicación se definen en el anexo B y se clasifican en el § 19.

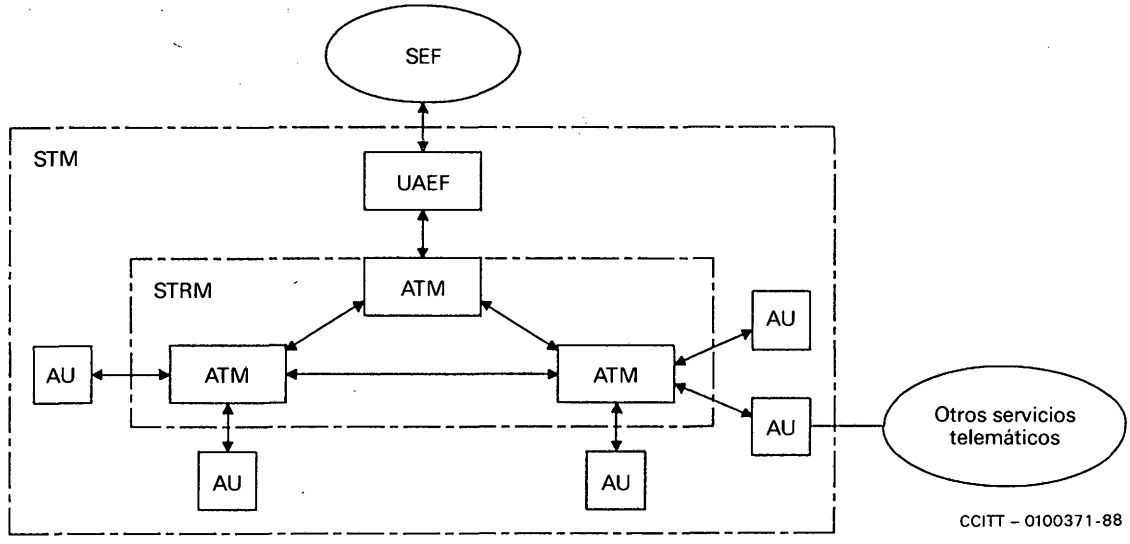


FIGURA 10/X.400

Modelo funcional del interfuncionamiento entre STM y SEF

Un sistema de entrega física es un sistema, explotado por un dominio de gestión, que transporta y entrega mensajes físicos. Un mensaje físico es un objeto físico que comprende un sobre de remisión y su contenido. Un ejemplo de un SEF lo constituye el servicio postal. Un ejemplo de un mensaje físico es una carta escrita en papel y su correspondiente sobre de papel.

Una unidad de acceso de entrega física (UAEF) convierte un mensaje de usuario TM a una forma física, proceso que se denomina transformación física. Un ejemplo de este proceso es la impresión de un mensaje y su colocación automática en un sobre de papel. La UAEF transfiere el mensaje que ha sufrido la transformación física a un SEF, para que éste lo siga transmitiendo y, finalmente, efectúe la entrega física.

Una UAEF puede considerarse como un conjunto de AU, cada uno de los cuales está identificado por una dirección postal. Para cumplir sus funciones, una UAEF debe admitir las interacciones de depósito (notificaciones) y de entrega con el STRM, y también cooperar con otros AU. De esta manera se proporciona la intercomunicación entre el STM y el SEF, como parte del servicio de transferencia de mensajes.

Para que los usuarios TM puedan dirigir mensajes que habrán de ser entregados físicamente por un SEF existe una forma de dirección adecuada, que se describe en el § 12.

10.2 *Configuraciones de organización*

En la figura 11/X.400 se muestran posibles correspondencias de organización del modelo funcional descrito anteriormente. En cada modelo (A y B), el término «dominio de EF» designa el dominio de responsabilidad de una organización que proporciona un servicio EF. En el caso A, el dominio del SEF comprende un STM y un SEF. El límite entre el dominio de EF y el resto del STM es un límite entre dominios de gestión (DG). En el caso B, el dominio de EF comprende sólo el SEF; la UAEF no forma parte del dominio de EF. El límite entre el dominio de EF y el STM se encuentra en el punto en el que la UAEF transfiere mensajes físicos al SEF.

11 Acceso especializado

11.1 *Introducción*

El modelo funcional del STM (figura 1/X.400) contiene unidades de acceso (UA) que permiten el acceso entre el STM y otros sistemas y servicios de comunicación. El modelo muestra una unidad de acceso genérica entre el STM y los servicios telemáticos.

También se muestra una unidad de acceso de entrega física (UAEF) que permite la entrega física de mensajes STM a los destinatarios sin necesidad de un terminal para el acceso al STM. El acceso a los servicios de entrega física está disponible para cualquier aplicación que emplee el STRM, a través de una UAEF que se describe en el § 10.

A continuación se describen otras formas de acceso.

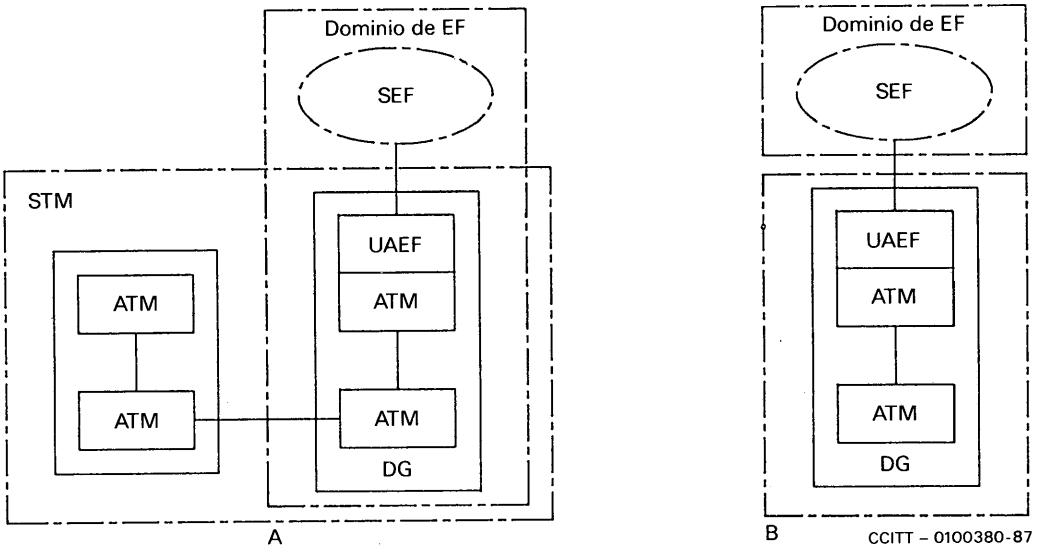


FIGURA 11/X.400

Configuraciones de la intercomunicación de los Servicios TM/EF

11.2 *Acceso teletex*

11.2.1 *Acceso registrado al servicio MIP*

La unidad de acceso especializada definida para el acceso telemático, el agente telemático (ATLM), se destina específicamente a los terminales teletex (TTX). Este ATLM proporciona un acceso teletex al servicio MIP, como se muestra en la figura 7/X.400. Las disposiciones técnicas de este acceso se definen en la Recomendación T.330. El ATLM permite a los usuarios de terminales teletex la plena participación en el servicio MIP.

11.2.2 *Acceso (público) no registrado al servicio MIP*

La unidad de acceso especializada definida para el acceso telemático, agente telemático (ATLM), también proporciona acceso público al servicio MIP para usuarios TTX que no son usuarios registrados del servicio MIP. Esto se muestra en la figura 7/X.400. Las disposiciones técnicas de este acceso se definen en la Recomendación T.330. La intercomunicación entre el servicio MIP y el servicio teletex se define en la Recomendación F.422.

11.3 *Acceso télex*

11.3.1 *Acceso registrado al servicio MIP*

En las Recomendaciones técnicas se define una unidad de acceso al télex (UATLX) para permitir la intercomunicación entre los usuarios MIP y los usuarios télex. La prestación de un servicio con este tipo de UA es asunto nacional.

11.3.2 *Acceso (público) no registrado al servicio MIP*

Se define una unidad de acceso especializada para permitir la intercomunicación entre los usuarios MIP y los usuarios télex. Esta unidad de acceso (UA) proporciona acceso público al servicio MIP para usuarios télex que no son usuarios registrados del servicio MIP y se denomina unidad de acceso télex pública (UATLXP). Se muestra en la figura 7/X.400. Los usuarios télex no son abonados del servicio MIP, pero utilizan algunas de las prestaciones del servicio MIP para transmitir mensajes a los usuarios del MIP. Los usuarios MIP también pueden enviar mensajes a usuarios télex por medio de esta UA. La intercomunicación entre el servicio MIP y el servicio télex se define en la Recomendación F.421.

Nota – Otros tipos de unidades de acceso requieren ulterior estudio (por ejemplo para facsímil, videotex, etc.).

PARTE 3 – CAPACIDADES DEL STM

12 Denominación y direccionamiento

12.1 *Introducción*

En un STM, la entidad principal que hay que denominar es el usuario (originador y destinatario de los mensajes). Además, las listas de distribución (LD) tienen nombres que se emplean en el STM. Los usuarios del STM y las LD se identifican mediante nombres O/D. Los nombres O/D están compuestos por nombres de guía y/o direcciones O/D, cuyas descripciones se ofrecen en este apartado.

12.2 *Nombres de guía*

Los usuarios del servicio TM y las LD pueden identificarse mediante un nombre, denominado nombre de guía. Un nombre de guía debe ser buscado en una guía para encontrar la dirección O/D correspondiente. La estructura y los componentes de los nombres de guía se describen en las Recomendaciones de la serie X.500.

Un usuario puede lograr acceso directo a un sistema de guía para encontrar la dirección O/D de un usuario, o las direcciones O/D de los miembros de una LD (ambas acciones se encuentran fuera del ámbito de estas Recomendaciones). Como alternativa, un usuario puede utilizar el nombre de guía y hacer que el STM consulte la guía para encontrar automáticamente la dirección (o direcciones) O/D correspondientes, como se describe en el § 14.

No es necesairo que un usuario STM o una LD tengan un nombre de guía, a menos que figuren en una guía. A medida que las guías se utilicen cada vez más, se prevé que los nombres de guía serán el método preferido para que los usuarios STM se identifiquen entre sí.

12.3 *Nombres O/D*

Cada usuario TM o LD tendrá uno o más nombres O/D. Un nombre O/D se compone de un nombre de guía, una dirección O/D, o ambos.

Para depositar un mensaje se puede utilizar uno o ambos componentes de un nombre O/D. Si sólo se suministra el nombre de guía, el STM tendrá acceso a una guía para intentar determinar la dirección O/D, que utilizará después para encaminar el mensaje y entregarlo. Si no se indica el nombre de guía, utilizará la dirección O/D dada. Cuando se indiquen ambos elementos al efectuar el depósito, el STM utilizará la dirección O/D, pero cursará el nombre de la guía, y presentará ambos al destinatario. Si la dirección O/D no es válida, intentará utilizar el nombre de guía como se indica anteriormente.

12.4 *Direcciones O/D*

Una dirección O/D contiene información que pemite al STM identificar unívocamente a un usuario a fin de entregarle un mensaje o devolverle una notificación. (El prefijo «O/D» reconoce el hecho de que el usuario puede actuar como originador o como destinatario del mensaje o de la notificación de que se trata.)

Una dirección O/D es una colección de informaciones denominadas atributos. La Recomendación X.402 especifica una serie de atributos normalizados a partir de los cuales pueden construirse direcciones O/D. El que los atributos sean normalizados significa que su sintaxis y su semántica son los que se definen en la Recomendación X.402. Además, de los atributos normalizados, y para satisfacer las necesidades de los sistemas de mensajería existentes, hay atributos definidos según el dominio, cuya sintaxis y semántica son definidas por los dominios de gestión.

Se han definido varias formas de direcciones O/D, cada una con su propia finalidad. Esas formas y finalidades son las siguientes:

- *Dirección O/D nemotécnica:* proporciona al usuario un medio práctico de identificar a otros usuarios cuando no existe una guía. Se utiliza también para identificar una lista de distribución.
- *Dirección O/D de terminal:* proporciona un medio de identificar a los usuarios con terminales que pertenecen a diversas redes.
- *Dirección O/D numérica:* proporciona un medio para identificar a los usuarios mediante teclados numéricos.
- *Dirección O/D postal:* proporciona un medio para identificar a los originadores y destinatarios de mensajes físicos.

13 Utilización de la guía por el STM

13.1 *Introducción*

La guía definida en las Recomendaciones de la serie X.500 proporciona capacidades útiles para el empleo y el suministro de diversos servicios de telecomunicación. Este apartado describe cómo se puede utilizar la guía en el tratamiento de mensajes; en otras Recomendaciones de la serie X.400 se pueden encontrar más detalles.

Las capacidades de la guía utilizadas en el tratamiento de mensajes se agrupan en las siguientes cuatro categorías:

a) *Nombres cómodos para el usuario:* el originador o destinatario de un mensaje puede ser identificado mediante su nombre de guía, en lugar de su dirección O/D, orientada a la máquina. En todo momento el STM puede obtener la dirección a partir del nombre consultando la guía.

b) *Listas de distribución (LD):* un grupo cuyos miembros estén registrados en la guía puede ser utilizado como una lista de distribución. El originador simplemente proporciona el nombre de la lista. En el punto de expansión de la LD, el STM puede obtener, consultando la guía, los nombres de guía (y a continuación, las direcciones O/D) de los destinatarios individuales.

c) *Capacidades de AU del destinatario:* las capacidades STM de un destinatario (u originador) pueden registrarse en su inscripción de la guía. En todo momento, el STM puede informarse de esas capacidades consultando la guía (y actuar en consecuencia).

d) *Autenticación:* antes de que dos entidades funcionales STM (dos ATM, o un AU y un ATM) se comuniquen entre sí, cada una establecerá la identidad de la otra. Esto puede efectuarse utilizando las capacidades de autenticación del STM sobre la base de la información almacenada en la guía.

Además, un usuario puede tener acceso directo a la guía, por ejemplo, para determinar la dirección O/D o las capacidades STM de otro usuario. Se suministra el nombre del usuario a la guía, la cual responde con la información solicitada.

13.2 *Modelo funcional*

Tanto los AU como los ATM pueden utilizar la guía. Un AU puede presentar a la guía el nombre de guía del destinatario deseado, y obtener de la guía la dirección O/D del mismo. El AU puede proporcionar el nombre de guía y la dirección O/D al STRM. Otro AU puede limitarse a suministrar al STRM el nombre de guía del destinatario. El STRM pedirá a la guía la dirección O/D del destinatario y la añadirá al sobre. El ATM originador normalmente realiza la búsqueda del nombre o de la dirección O/D.

En la figura 12/X.400 se muestra un modelo funcional que describe ese proceso.

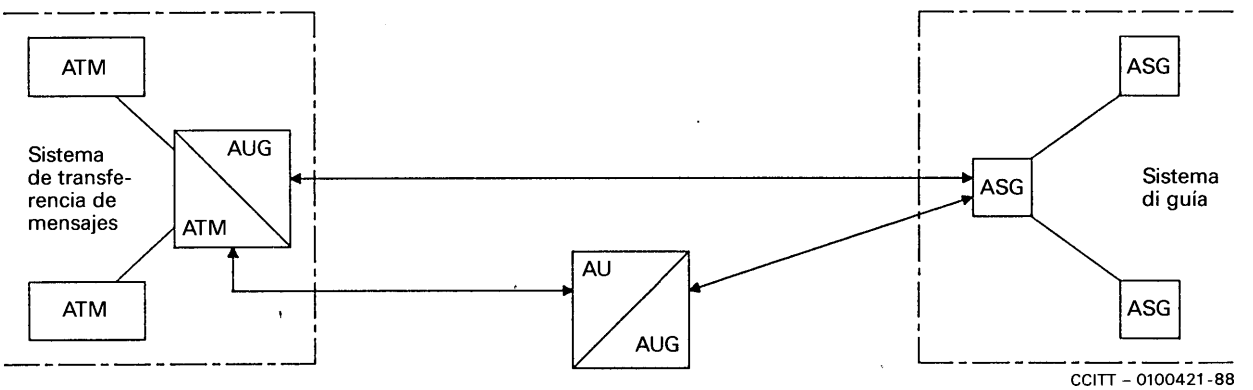


FIGURA 12/X.400

Modelo funcional del interfuncionamiento entre el STM y la guía

13.3 *Configuraciones físicas*

En la figura 13/X.400 se muestran algunas configuraciones físicas posibles del modelo funcional indicado anteriormente. Cuando un agente de usuario de guía (AUG) y un agente de sistema de guía (ASG) están realizados en sistemas físicamente separados, un protocolo normalizado de guía, definido en las Recomendaciones de la serie X.500, regula sus interacciones. Con frecuencia, resultará conveniente que un AU o un ATM esté situado en el mismo lugar que un AUG/ASG. No obstante, pueden darse otras configuraciones físicas.

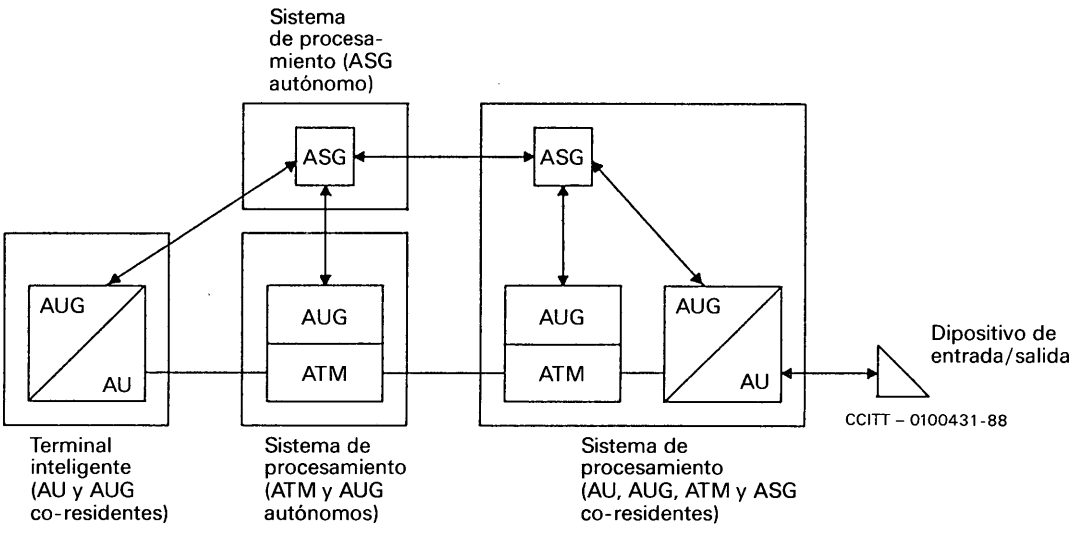


FIGURA 13/X.400

Configuraciones físicas para el interfuncionamiento entre el STM y la guía

14 Listas de distribución en el STM

14.1 *Introducción*

La posibilidad de utilizar una lista de distribución (LD) es una capacidad facultativa del STM, proporcionada por medio del servicio TRM. La expansión de la LD permite al emisor hacer que un mensaje se transmita a un grupo de destinatarios, dando el nombre del grupo en vez del nombre de cada uno de los destinatarios finales.

14.2 *Propiedades de una LD*

La propiedades de una LD pueden describirse como sigue:

- *Miembros de LD:* usuarios y otras LD que recibirán mensajes dirigidos a la LD.
- *Permiso de depósito de LD:* lista de usuarios y otras LD a los que se permite hacer uso de la LD para enviar mensajes a los miembros de la LD.
- *Punto de expansión de la LD:* cada LD tiene una dirección O/D inequívoca. Esta dirección O/D identifica el punto de expansión, que es el dominio o ATM donde se añaden a la lista de destinatarios los nombres de los miembros de la LD. El mensaje se transporta al punto de expansión, antes de la expansión, como se indica en la figura 14/X.400.
- *Propietario de LD:* usuario responsable de la gestión de una LD.

14.3 *Depósito*

El depósito de un mensaje a una LD es similar al depósito de un mensaje a un usuario. El originador puede incluir el nombre O/D de la LD, el nombre de guía, la dirección O/D, o ambos (para más detalles véase el § 12). El originador no necesita saber que el nombre O/D utilizado es el de una LD. Sin embargo, el originador puede, utilizando el elemento de servicio prohibición de expansión de la LD, prohibir al STRM la expansión de un mensaje que por inadvertencia se ha dirigido a una LD.

14.4 *Utilización de una guía por la LD*

Una guía puede o no ser utilizada para almacenar información sobre las propiedades de la LD. Entre la información que puede almacenarse está la siguiente: miembros de la LD, propietario de la LD, permiso de depósito de la LD y punto de expansión de la LD.

14.5 *Expansión de la LD*

En el punto de expansión, el ATM responsable de la expansión de la LD:

a) Consultará la información sobre la LD, por ejemplo en la guía, utilizando los derechos de acceso otorgados al ATM. (*Nota* – Como esto lo hace el ATM en el punto de expansión, el soporte de las LD en el STM no requiere una guía interconectada globalmente.)

b) Verificará si la expansión está o no permitida, comparando la identidad del emisor con el permiso de depósito de la LD.

c) Si se permite la expansión, añadirá los miembros de la LD a la lista de destinatarios del mensaje y les transmitirá el mensaje.

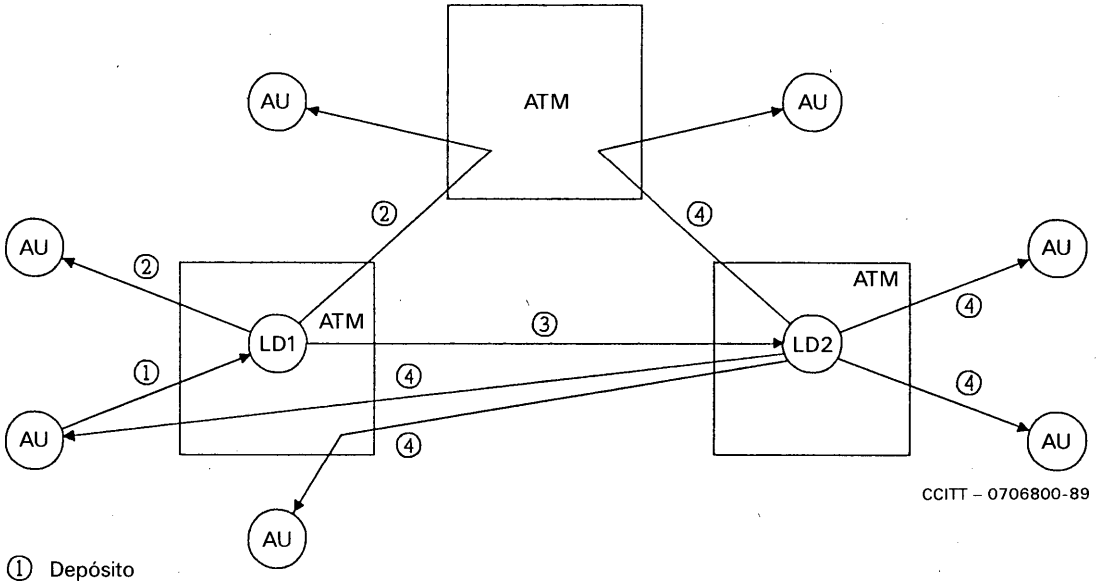


FIGURA 14/X.400

Expansión de la lista de distribución

14.6 *Jerarquización*

Un miembro de una LD puede ser otra LD, como se indica en la figura 14/X.400. En este caso el mensaje es reenviado desde el punto de expansión de la LD progenitora hacia el punto de expansión LD miembro para ulterior expansión. De este modo durante cada expansión sólo se añaden al mensaje los miembros de una LD.

Durante la expansión de una LD anidada, la identidad de la LD progenitora (por ejemplo, LD1 en la figura 14/X.400), en vez de la identidad del originador del mensaje, se compara con el permiso de depósito de la LD miembro (por ejemplo, LD2 en la figura 14/X.400).

Nota – Pueden definirse estructuras de LD que se refieren a una LD anidada particular más de una vez a diferentes niveles del anidamiento. El depósito en una de esas LD progenitoras puede causar que un destinatario reciba copias múltiples del mismo mensaje. El mismo resultado puede ocurrir si se direcciona un mensaje a LD múltiples que contienen un miembro común. La correlación de dichas copias puede hacerse en el AU del destinatario y/o en el AM.

14.7 *Control de repetición*

Si cierta LD es directa o indirectamente miembro de sí misma (situación que puede surgir, y que es válida), o cuando las LD están combinadas con redireccionamiento, el mensaje podría volver a la misma lista y circular indefinidamente. El STRM detecta esta posible situación y evita que se produzca.

14.8 *Entrega*

A la entrega del mensaje, el destinatario se entera que recibió el mensaje como miembro de una LD, y por medio de qué LD o cadena de LD lo obtuvo.

14.9 *Control del bucle de encaminamiento*

Un mensaje puede originarse en un dominio/ATM, extenderse a un segundo dominio/ATM y después ser devuelto a un miembro de la LD en el primer dominio/ATM. El STRM no tratará esto como un error de bucle de encaminamiento.

14.10 *Notificaciones*

Las notificaciones de entrega y de no entrega pueden generarse tanto en el punto de expansión de la LD (por ejemplo, si se niega el permiso de depósito) como en el momento de la entrega al destinatario final.

Cuando un mensaje procedente de una LD genera una notificación, esta notificación es enviada a la LD de la cual provino el mensaje. Entonces la LD, según la pauta seguida por la lista, transmitirá la notificación al propietario de la lista, a la LD o al originador del que obtuvo el mensaje, o ambos, como se indica en la figura 15/X.400.

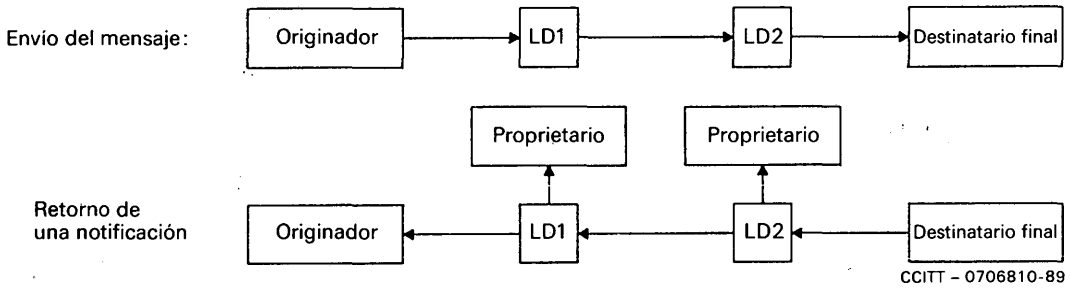


FIGURA 15/X.400

Notificaciones LD

Nota – Cuando las notificaciones son enviadas al originador tras la expansión de la LD, el originador puede recibir muchas notificaciones de entrega/no entrega para un destinatario (la propia LD) especificado por el originador. El originador puede incluso recibir más de una notificación de un destinatario final, si dicho destinatario recibió el mensaje más de una vez a través de listas diferentes.

14.11 *Política de tratamiento de la LD*

Un ATM puede o no proporcionar diferentes pautas sobre el tratamiento de las LD. Dichas pautas, o políticas, determinarán si las notificaciones generadas a la entrega a miembros de la LD deben hacerse retornar por medio de las LD anteriores, o al originador si no hay tales LD anteriores, y/o al propietario de la lista. Si la pauta es que sólo se envíen notificaciones al propietario de la lista, entonces el originador recibirá las notificaciones si las solicitó, únicamente durante la expansión de dicha LD. Para poder cumplir con esta restricción, al realizar la expansión el STRM reajustará las solicitudes de notificación de acuerdo con la pauta para la lista.

15 Capacidades de seguridad del STM

15.1 *Introducción*

Dada la naturaleza distribuida del STM es conveniente disponer de mecanismos de protección contra diversos riesgos que puedan afectar a la seguridad del sistema. A continuación se describe la naturaleza de esos riesgos y las capacidades que se pueden utilizar para contrarrestarlos.

15.2 *Riesgos que afectan a la seguridad del STM*

15.2.1 *Riesgos de acceso*

El acceso de un usuario no válido al STM es uno de los principales riesgos que afectan a la seguridad del sistema. Si se puede evitar que los usuarios no válidos utilicen el sistema, se reducirán considerablemente los riesgos de seguridad.

15.2.2 *Riesgos entre mensajes*

Los riesgos entre mensajes provienen de agentes no autorizados, ajenos a la comunicación del mensaje, y pueden manifestarse de las siguientes maneras:

- *Impostura:* Un usuario que no tiene prueba de la identidad de la persona con la que comunica puede ser fácilmente engañado por un impostor y revelar información importante.
- *Modificación del mensaje:* Un mensaje genuino, que ha sido modificado por un agente no autorizado mientras era transferido a través del sistema, puede engañar al destinatario del mensaje.
- *Reproducción:* Los mensajes cuyos originadores y contenidos son genuinos pueden ser observados por un agente no autorizado, que podrá así reproducirlos de modo que el destinatario deseado del mensaje reciba esa reproducción en una fecha posterior. El móvil de esta acción puede ser extraer más información del destinatario deseado, o confundirlo.
- *Análisis de tráfico:* El análisis de tráfico de mensajes entre los usuarios TM puede permitir averiguar a un espía si se transmiten datos entre dos usuarios, cuántos, y con qué frecuencia. Aunque no pueda determinarse el contendio de los mensajes, el espía puede deducir una cierta cantidad de información a partir de las características del tráfico cursado (por ejemplo, continuo, por ráfagas, esporádico o nulo).

15.2.3 *Riesgos intra-mensajes*

Estos riesgos tienen su origen en los participantes reales en la comunicación del mensaje, y pueden manifestarse de la siguiente manera:

- *No reconocimiento de mensajes:* Uno de los participantes reales en la comunicación puede negar su intervención en la misma. Ello podría acarrear consecuencias importantes, si se realizan transacciones financieras a través del STM.
- *Violación del nivel de seguridad:* Si un dominio de gestión dentro del STM emplea niveles diferentes de autorizaciones de seguridad (por ejemplo, nivel público, personal, privado o confidencial para la compañía), deberá impedirse que los usuarios envíen o reciban mensajes para los que su autorización de seguridad sea insuficiente a fin de no comprometer la seguridad del dominio de gestión.

15.2.4 *Riesgo de las memorias de datos*

El STM tiene cierto número de memorias de datos que deben ser protegidos contra los siguientes riesgos:

- *Modificación de la información de encaminamiento:* La modificación no autorizada del contenido de la guía podría conducir a un encaminamiento indebido de los mensajes e incluso a su pérdida, en tanto que la modificación no autorizada de la memoria de datos de entrega diferida o de la memoria de datos de retención para entrega podría engañar o confundir al destinatario deseado.
- *Entrega anticipada:* Un agente no autorizado podría hacer una copia de un mensaje de entrega diferida y enviarla al destinatario deseado mienstras el ATM retiene la entrega del original. Ello podría engañar al destinatario del mensaje y hacer que conteste al originador antes de lo esperado por éste, o simplemente confundir al destinatario deseado.

15.3 *Modelo de seguridad*

Pueden proporcionarse características de seguridad ampliando las capacidades de los componentes del sistema de tratamiento de mensajes de modo que incluyan diversos mecanismos de seguridad.

Hay dos aspectos de la seguridad en el tratamiento de mensajes: gestión de acceso y administración seguras y mensajería segura.

15.3.1 *Gestión de acceso y administración seguras*

En este punto, las capacidades se refieren al establecimiento de una asociación autenticada entre componentes adyacentes, y al establecimiento de parámetros de seguridad para dicha asociación. Esto puede aplicarse a un par cualquiera de componentes del sistema de tratamiento de mensajes: AU/ATM, ATM/ATM, MM/ATM, etc.

15.3.2 *Mensajería segura*

En este punto, las capacidades se refieren a la aplicación de las características de seguridad para proteger mensajes en el sistema de tratamiento de mensajes, de acuerdo con una política de seguridad definida. Esto incluye elementos de servicio que permitan a diversos componentes verificar el origen de los mensajes y la integridad de su contenido, y elementos de servicio para evitar la revelación no autorizada del contenido del mensaje.

Las capacidades de esta sección abarcan la aplicación de características de seguridad para proteger mensajes depositados directamente en el sistema de transferencia de mensajes por un agente de usuario, almacenador de mensajes o una unidad de acceso. No abarcan la aplicación de características de seguridad para proteger la comunicación entre los usuarios y el sistema de tratamiento de mensajes, o la comunicación de usuario TM a usuario TM (una gran parte de la comunicación de usuario TM a usuario TM está protegida entre dos AU). Por consiguiente no se aplican, por ejemplo, a la comunicación entre un terminal de usuario distante y su AU ni a la comunicación entre estos equipos terminales de usuario y otros usuarios del STM. Las capacidades de seguridad para proteger la comunicación de usuario TM son para ulterior estudio.

Muchos de los elementos de servicio de la mensajería segura proporcionan una capacidad de originador a destinatario y requieren del uso de agentes de usuario con capacidades de seguridad. No requieren el uso de un sistema de transferencia de mensajes con prestaciones de seguridad. [Por ejemplo, puede aplicarse disponiendo la confidencialidad del contenido que el originador cifre el contenido del mensaje y que el destinatario lo descifre, con diversos parámetros de seguridad transferidos dentro del sobre del mensaje. Tal mensaje puede ser transmitido por cualquier STRM que pueda tratar el formato del contenido (octetos no formateados) y tratar transparentemente los campos de seguridad en el sobre.]

Algunos de los elementos de servicio de mensajería segura inplican la interacción con el sistema de transferencia de mensajes y requieren el uso de agentes de transferencia de mensaje con capacidades de seguridad. (Por ejemplo, incuestionabilidad del depósito requiere que el ATM, en el que se deposita el mensaje, contenga mecanismos para generar un campo de prueba de depósito.)

Algunos de los elementos de servicio de mensajería segura se aplican a la MM así como a los AU y ATM, por ejemplo el etiquetado de seguridad del mensaje. Sin embargo, en general, la MM es transparente a las características de seguridad que se aplican entre los AU del originador y del destinatario.

En el cuadro 2/X.400 se presenta el alcance de los elementos de servicio de mensajería segura. Se describen los elementos de servicio atendiendo a cuál componente STM es el «proveedor» y cuál el «usuario» del servicio de seguridad. Por ejemplo, la autenticación de origen de sonda es generada por un AU de origen y puede ser utilizada por los ATM por los que pasa la sonda.

Esta Recomendación describe el uso de servicio de seguridad por el AU, y el ATM. La forma en que estas características se aplican a las unidades de acceso requiere ulterior estudio.

15.4 *Características de seguridad del STM*

Los elementos de servicio que describen las características de seguridad del STM se definen en el anexo B y se clasifican en el § 19. A continuación se presenta una descripción general de dichas capacidades:

- *Autenticación del origen del mensaje:* Permite al destinatario, o a cualquier ATM por el que pasa el mensaje, autenticar la identidad del originador de un mensaje.
- *Autenticación del origen del informe:* Permite al originador autenticar el origen de un informe de entrega/no entrega.
- *Autenticación del origen de la sonda:* Permite a cualquier ATM por el que pasa la sonda, autenticar el origen de la sonda.
- *Prueba de entrega:* Permite al originador de un mensaje autenticar el mensaje entregado y su contenido así como la identidad del (de los) destinatario(s).
- *Prueba de depósito:* Permite al originador de un mensaje autenticar que el mensaje fue depositado en el STRM para entrega al (a los) destinatario(s) especificado(s) inicialmente.
- *Gestión de acceso seguro:* Proporciona la autenticación entre componentes adyacentes y el establecimiento del contexto de seguridad.
- *Integridad del contenido:* Permite al destinatario verificar que el contenido original de un mensaje no ha sido modificado.
- *Confidencialidad del contenido:* Impide la revelación no autorizada del contenido del mensaje a una parte que no sea el destinatario deseado.

- *Confidencialidad del flujo del mensaje:* Permite al originador de un mensaje asegurar que el flujo del mensaje a través del STM se mantenga secreto.
- *Integridad de la secuencia de mensajes:* Permite al originador proporcionar a un destinatario la prueba de que se ha conservado la secuencia de los mensajes.
- *No rechazo del origen:* Proporciona al (a los) destinatario(s) de un mensaje una prueba del origen del mensaje y su contenido, lo caul le(s) protegerá contra cualquier intento del originador de negar falsamente haber enviado el mensaje o su contenido.
- *No rechazo de la entrega:* Proporciona al originador del mensaje una prueba de la entrega del mensaje, lo cual le protegerá contra cualquier intento del destinatario de negar falsamente haber recibido el mensaje o su contenido.
- *No rechazo del depósito:* Proporciona al originador de un mensaje una prueba del depósito del mensaje, lo cual le protegerá contra cualquier intento del STRM de negar falsamente que el mensaje fue depositado para entrega al (a los) destinatario(s) especificado(s) inicialmente.
- *Etiquetado de seguridad de los mensajes*: Proporciona una capacidad para categorizar un mensaje, indicando su sensibilidad, lo que determina el tratamiento del mensaje según la política de seguridad en vigor.

CUADRO 2/X.400

Suministro y utilización de los elementos del servicio de mensajería segura por los componentes del STM

Elementos de servicio	Usuario STM de origen	STM	Usuario STM de destino
Autenticación del origen del mensaje	P	U	U
Autenticación del origen del informe	U	P	–
Autenticación de origen de la sonda	P	U	–
Prueba de entrega	U	–	P
Prueba de depósito	U	P	–
Gestión de acceso seguro	P	U	P
Integridad del contenido	P	–	U
Confidencialidad del contenido	P	–	U
Confidencialidad del flujo del mensaje	P	–	–
Integridad de la secuencia de mensaje	P	–	U
No rechazo del origen	P	–	U
No rechazo del depósito	U	P	–
No rechazo de la entrega	U	–	P
Etiquetado de seguridad del mensaje	P	U	U

P El componente STM es un proveedor del servicio.

U El componente STM es un usuario del servicio.

15.5 *Gestión de la seguridad*

Los aspectos de un esquema asimétrico de gestión de claves para ofrecer las prestaciones antes mencionadas son proporcionados por el marco de autenticación del sistema de guía, descrito en la Recomendación X.509. La guía almacena copias certificadas de claves públicas para usuarios del STM, que pueden emplearse para proporcionar autenticación y facilitar el intercambio de claves para su utilización en mecanismos de confidencialidad de datos y de integridad de datos. Los certificados pueden leerse de la guía utilizando el protocolo de acceso a la guía descrito en la Recomendación X.519.

Las Recomendaciones sobre otros tipos de esquemas de gestión de claves, incluyendo la encripción simétrica, para ofrecer las prestaciones de seguridad, requieren ulterior estudio.

16 Conversión en el STM

El STRM proporciona funciones de conversión que permiten a los usuarios introducir mensajes en uno o más formatos codificados, denominados tipos de información codificada (TIC), y hacer que se entreguen en otros TIC a usuarios con diferentes capacidades AU y tipos de terminal. Esta capacidad es inherente al STRM y aumenta la posibilidad de entrega al adaptar el mensaje a las capacidades de terminal de los destinatarios. Los TIC disponibles en el STM se enumeran en la Recomendación X.411. Las conversiones y el uso de los elementos de servicio relacionados con la conversión están disponibles para TIC no definidos en la Recomendación X.411, pero admitidos por ciertos dominios, sea bilateralmente entre estos dominios o dentro de un mismo dominio.

Los usuarios del TM tienen cierto control sobre el proceso de conversión a través de diversos elementos de servicio que se describen en el anexo B. Entre ellos figura la posibilidad de que el usuario solicite expresamente la conversión necesaria o, absteniéndose de hacerlo, deje que el STRM determine la necesidad de efectuar la conversión y el tipo correspondiente. Los usuarios también tienen la posibilidad de solicitar que no se efectúe una conversión, o que no se la realice si implicase una pérdida de información. Cuando el STRM realiza una conversión en un mensaje, informa al AU al que se le entrega ese mensaje que se ha realizado la conversión y cuáles eran los TIC originales.

El proceso de conversión de los mensajes IP puede efectuarse en partes determinadas del cuerpo de tipos específicos, cuando éstas están presentes. En la Recomendación X.408 se describen los aspectos generales de la conversión y se indican detalladamente las reglas específicas para la conversión entre diferentes TIC.

Las conversiones detalladas en la Recomendación X.408 son aquellas entre télex, AI5, teletex, facsímil G3, G4 clase 1 y videotex, voz y modo mixto.

17 Utilización del STM en la prestación de servicios públicos

El sistema de tratamiento de mensajes se utiliza en la prestación de servicios públicos TM, que ofrecen las Administraciones a sus abonados. Estos servicios públicos TM se definen en las Recomendaciones de la serie F.400 del CCITT, y comprenden:

- Servicio público de transferencia de mensajes (Rec. F.410).
- Servicio público de mensajería interpersonal (Rec. F.420).

Además, las Administraciones ofrecen servicios públicos complementarios que permiten la intercomunicación entre los servicios del CCITT y los servicios TM públicos mencionados anteriormente, de la siguiente manera:

- Intercomunicación con servicios públicos de entrega física (Rec. F.415).
- Intercomunicación entre el servicio MIP y el servicio télex (Rec. F.421).
- Intercomunicación entre el servicio MIP y el servicio teletex (Rec. F.422).

La Recomendación F.401 describe los aspectos de denominación y direccionamiento para los servicios TM públicos.

PARTE 4 – ELEMENTOS DE SERVICIO

18 Finalidad

Los elementos de servicio son características, funciones o capacidades particulares del STM. Todos los elementos de servicio aplicables al STM se definen en el anexo B, y se enumeran en orden alfabético inglés con un número de referencia correspondiente. La realización de esos elementos de servicio del STM se describen en otras Recomendaciones de la serie X.400.

Los elementos de servicio están asociados a los diversos servicios prestados por el STM. Hay elementos de servicio para el servicio de transferencia de mensajes que suministran una capacidad de transporte básica para enviar y recibir mensajes entre los AU. Hay elementos de servicio para el servicio de mensajería interpersonal, que permiten el envío y la recepción de mensajes entre una clase particular de AU denominados AU de MIP. Hay elementos de servicio para el servicio de entrega física, que permiten a los usuarios del TM enviar mensajes a fin de que se entreguen por medios físicos a destinatarios que no son usuarios del TM. Hay elementos de servicio disponibles específicamente para el uso de almacenes de mensajes.

Los elementos de servicio para el servicio MIP incluyen los disponibles para el servicio TRM, el servicio EF y el almacén de mensajes, así como los específicos, aplicables al servicio MIP.

En el cuadro 3/X.400 se indican todos los elementos de servicio disponibles en el STM, precisándose con cuáles de los servicios actualmente definidos (servicio TRM, servicio MIP y servicio EF) están específicamente asociados o si son específicos de la memoria de mensajes, y se da el número de referencia correspondiente a la definición del anexo B.

CUADRO 3/X.400

Elementos de servicio STM

Elementos de servicio	TRM	MIP	EF	MM	Referencia del anexo B
Gestión de acceso	X				B.1
Reproducción física adicional			X		B.2
Destinatario alternativo autorizado	X				B.3
Asignación de destinatario alternativo	X				B.4
Indicación de usuarios autorizantes		X			B.5
Indicación de reenvío automático		X			B.6
Reproducción física básica			X		B.7
Indicación de destinatario de copia ciega		X			B.8
Indicación de encripción de parte del cuerpo		X			B.9
Confidencialidad del contenido	X				B.10
Integridad del contenido	X				B.11
Indicación del tipo de contenido	X				B.12
Prohibición de conversión	X				B.13
Prohibición de conversión en caso de pérdida de información	X				B.14
Indicación de convertido	X				B.15
Recogida en ventanilla			X		B.16
Recogida en ventanilla con aviso			X		B.17
Indicación de referencia recíproca		X			B.18
Entrega diferida	X				B.19
Cancelación de entrega diferida	X				B.20
Notificación de entrega	X				B.21
Indicación de hora de entrega	X				B.22
Entrega por servicio burofax			X		B.23
Designación de destinatario por nombre de guía	X				B.24
Revelación de otros destinatarios	X				B.25
Indicación de historia de la expansión de LD	X				B.26
Expansión de LD prohibida	X				B.27
SCU (servicio correo urgente)			X		B.28
Indicación de fecha de expiración		X			B.29
Conversión explícita	X				B.30
Indicación de mensaje IP reenviado		X			B.31
Selección de grado de entrega	X				B.32
Retención para entrega	X				B.33
Conversión implícita	X				B.34
Indicación de importancia		X			B.35
Indicación de copia incompleta		X			B.36
Indicación de mensaje IP		X			B.37
Indicación de idioma		X			B.38
Designación de la última entrega	X				B.39
Confidencialidad del flujo del mensaje	X				B.40
Identificación de mensaje	X				B.41
Autenticación del origen del mensaje	X				B.42
Etiquetado de seguridad del mensaje	X				B.43
Integridad de la secuencia del mensaje	X				B.44
Entrega a múltiples destinos	X				B.45
Cuerpos de múltiples partes		X			B.46
Notificación de no entrega	X				B.47

CUADRO 3/X.400 *(continuación)*

Elementos de servicio	TRM	MIP	EF	VMM	Referencia del anexo B
Indicación de petición de notificación de no recepción		X			B.48
No rechazo de la entrega	X				B.49
No rechazo del origen	X				B.50
No rechazo del depósito	X				B.51
Indicación de obsolescencia		X			B.52
Correo ordinario			X		B.53
Indicación de tipos de información codificada originales	X				B.54
Indicación de originador		X			B.55
Destinatario alternativo solicitado por el originador	X				B.56
Notificación de entrega física por el STM			X		B.57
Notificación de entrega física por el SEF			X		B.58
Reenvío físico permitido			X		B.59
Reenvío físico prohibido			X		B.60
Prevención de notificación de no entrega	X				B.61
Indicación de destinatarios primarios y de copia		X			B.62
Sonda	X				B.63
Autenticación de origen de sonda	X				B.64
Prueba de entrega	X				B.65
Prueba de depósito	X				B.66
Indicación de petición de notificación de recepción		X			B.67
Redireccionamiento desautorizado por el originador	X				B.68
Redireccionamiento de mensajes entrantes	X				B.69
Correo certificado			X		B.70
Correo certificado para el destinatario en persona			X		B.71
Indicación de petición de respuesta		X			B.72
Indicación de mensaje IP de respuesta		X			B.73
Autenticación de origen de informe	X				B.74
Petición de la dirección reenviante			X		B.75
Método de entrega solicitado	X				B.76
Entrega restringida	X				B.77
Devolución del contenido	X				B.78
Gestión de acceso seguro	X				B.79
Indicación de sensibilidad		X			B.80
Entrega especial			X		B.81
Alerta de mensaje almacenado				X	B.82
Reenvío automático de mensaje almacenado				X	B.83
Supresión de mensaje almacenado				X	B.84
Captura de mensaje almacenado				X	B.85
Listado de mensajes almacenados				X	B.86
Resumen de mensajes almacenados				X	B.87
Indicación de asunto		X			B.88
Indicación de hora de depósito	X				B.89
Cuerpo tipificado		X			B.90
Correo inentregable con devolución de mensaje físico			X		B.91
Uso de lista de distribución	X				B.92
Registro de capacidades de usuario/AU	X				B.93

19 Clasificación

19.1 *Finalidad de la clasificación*

Los elementos de servicio del STM se clasifican en pertenecientes a un servicio básico (llamado también base para EF y MM) y facilidades facultativas de usuario. Los elementos de servicio pertenecientes a un servicio básico son inherentes a ese servicio; constituyen el servicio básico y siempre se los proporciona y están disponibles para la utilización del mismo.

Otros elementos de servicio, denominados facilidades facultativas de usuario, pueden ser seleccionados por el abonado o usuario, bien mensaje por mensaje o por un periodo de tiempo convenido. Cada facilidad facultativa de usuario visible para el usuario se clasifica como esencial o adicional. Las facilidades facultativas de usuario esenciales (E) deberán estar disponibles para todos los usuarios STM. Las facilidades facultativas de usuario adicionales (A) pueden estar disponibles para uso nacional, e internacional sobre la base de acuerdos bilaterales.

19.2 *Servicio de transferencia de mensajes básico*

El servicio TRM básico permite a un AU depositar y recibir mensajes. Si un mensaje no puede ser entregado, se informa al AU de origen por medio de una notificación de no entrega. Cada mensaje es identificado de una manera única e inequívoca. Para facilitar una comunicación significativa, el AU puede especificar el o los tipos de información codificada que podrán contener los mensajes que le sean entregados. Cada mensaje entregado va acompañado de la indicación del tipo de contenido, del o los tipos de información codificada originales, de cualquier conversión realizada, y el o los tipos de información codificada resultantes. Además, para cada mensaje se indica la hora del depósito y la de entrega. Los elementos de servicio TRM que pertenecen al servicio TRM básico se enumeran en el cuadro 4/X.400.

CUADRO 4/X.400

Elementos de servicio pertenecientes al servicio TRM básico

Elementos de servicio	Referencia del anexo B
Gestión de acceso	B.1
Indicación del tipo de contenido	B.12
Indicación de conversión	B.15
Indicación de la hora de entrega	B.22
Identificación de mensajes	B.41
Notificación de no entrega	B.47
Indicación de tipos de información codificada originales	B.54
Indicación de la hora de depósito	B.89
Registro de capacidades de usuario/AU	B.93

19.3 *Facilidades facultativas de usuario del servicio TRM*

Las facilidades facultativas de usuario del servicio TRM pueden seleccionarse mensaje por mensaje o para un periodo de tiempo convenido. Cada facilidad facultativa de usuario visible para el usuario se clasifica como esencial o adicional, según lo estipulado en el § 19.1. En el cuadro 5/X.400 se enumeran los elementos de servicio que conforman las facilidades facultativas de usuario del servicio TRM, con su clasificación y su disponibilidad (PM: por mensaje; AC: acuerdo contractual). Las facilidades facultativas de usuario para el servicio EF y almacén de mensajes, si bien forman parte de las facilidades facultativas de usuario del servicio TRM, no se indican en el presente cuadro por estar sujetas a que se suministre una UAEF o un MM, y son objeto de clasificaciones distintas en los cuadros 6/X.400 a 9/X.400.

CUADRO 5/X.400

Facilidades facultativas de usuario del servicio TRM

Elementos de servicio	Clasificación	Disponible	Referencia del anexo B
Destinatario alternativo autorizado	E	PM	B.3
Asignación de destinatario alternativo	A	AC	B.4
Confidencialidad del contenido	A	PM	B.10
Integridad del contenido	A	PM	B.11
Prohibición de conversión	E	PM	B.13
Prohibición de conversión en caso de pérdida de información	A	PM	B.14
Entrega diferida	E	PM	B.19
Cancelación de entrega diferida	E	PM	B.20
Notificación de entrega	E	PM	B.21
Designación de destinatarios por el nombre de guía	A	PM	B.24
Revelación de otros destinatarios	E	PM	B.25
Indicación de historia de la expansión de la LD	E	PM	B.26
Prohibición de expansión de LD	A	PM	B.27
Conversión explícita	A	PM	B.30
Selección de grado de entrega	E	PM	B.32
Retención para entrega	A	AC	B.33
Conversión implícita	A	AC	B.34
Designación de la última entrega	A	PM	B.39
Confidencialidad del flujo de mensajes	A	PM	B.40
Autenticación del origen del mensaje	A	PM	B.42
Etiquetado de securidad de mensajes	A	PM	B.43
Integridad de la secuencia de mensajes	A	PM	B.44
Entrega a múltiples destinos	E	PM	B.45
No rechazo de la entrega	A	PM	B.49
No rechazo del origen	A	PM	B.50
No rechazo del depósito	A	PM	B.51
Destinatario alternativo solicitado por el originador	A	PM	B.56
Prevención de notificación de no entrega	A	PM	B.61
Sonda	E	PM	B.63
Autenticación del origen de la sonda	A	PM	B.64
Prueba de entrega	A	PM	B.65
Prueba de depósito	A	PM	B.66
Redireccionamiento desautorizado por el originador	A	PM	B.68
Redireccionamiento de mensajes entrantes	A	AC	B.69
Autenticación de origen del informe	A	PM	B.74
Método de entrega solicitado	E [a)]	PM	B.76
Entrega restringida	A	AC	B.77
Devolución del contenido	A	PM	B.78
Gestión de acceso seguro	A	AC	B.79
Utilización de lista de distribución	A	PM	B.92

[a)] No implica que se proporcionen todos los métodos de entrega que puedan ser solicitados.

19.4 *Intercomunicación de los servicios TM/EF de base*

Puede proporcionarse la intercomunicación de los servicios TM/EF de base para mejorar el servicio TRM, permitiendo que los mensajes se entreguen a los destinatarios en un formato físico (típicamente una copia impresa) mediante un servicio de entrega material tal como el servicio postal. Esta capacidad puede ser empleada por cualquier aplicación que utilice el servicio TRM. En el cuadro 6/X.400 se enumeran los elementos de servicio TM/EF que pertenecen a la intercomunicación TM/EF de base disponibles por cada destinatario. Cuando se proporcione esta intercomunicación a través de UAEF, se admitirán todos los elementos de servicio del cuadro 6/X.400.

CUADRO 6/X.400

Elementos de servicio pertenecientes a la intercomunicación de los servicios TM/EM de base

Elementos de servicio	Referencia del anexo B
Reproducción física básica	B.7
Correo ordinario	B.53
Reenvío físico permitido	B.59
Correo inentregable con devolución de mensaje físico	B.91

19.5 *Facilidades facultativas de usuario para la intercomunicación de los servicios TM/EF*

Los elementos de servicio TM/EF de base (§ 19.4) junto con las facilidades facultativas de usuario enumeradas a continuación, pueden utilizarse juntos para proporcionar intercomunicación de los servicios TM/EF. Esta capacidad puede ser utilizada por cualquier aplicación que emplee el servicio TRM ampliado. Las facilidades facultativas de usuario del servicio EF pueden seleccionarse por cada destinatario, y se enumeran en el cuadro 7/X.400.

CUADRO 7/X.400

Facilidades facultativas de usuario para interconexión de servicios TM/EM

Elementos de servicio	Clasificación	Referencia del anexo B
Reproducción física adicional	A	B.2
Recogida en ventanilla	E	B.16
Recogida en ventanilla con aviso	A	B.17
Entrega por el servicio Burofax	A	B.23
SCU (servicio correo urgente)	E	B.28
Notificación de entrega física por el STM	A	B.57
Notificación de entrega física por el SEF	A	B.58
Reenvío físico prohibido	A	B.60
Correo certificado	A	B.70
Correo certificado para el destinatario en persona	A	B.71
Petición de dirección reenviante	A	B.75
Entrega especial [a]	E	B.81

[a] Por lo menos uno de los dos elementos será admitido por la UAEF y el SEF asociado.

19.6 *Memoria de mensajes de base*

La memoria de mensajes de base se encuentra disponible en forma facultativa para proporcionar el almacenamiento y la gestión de mensajes entrantes, actuando como intermediario entre un AU y un ATM. La MM puede usarse en cualquier aplicación que utilice el servicio TRM. Los elementos de servicio que pertenecen a la memoria de mensajes de base se indican en el cuadro 8/X.400. Cuando se proporciona una MM, se deben admitir todos los elementos de servicio que se muestran en el cuadro 8/X.400.

CUADRO 8/X.400

Memoria de mensajes de base

Elementos de servicio	Referencia del anexo B
Suprimir mensaje almacenado	B.84
Capturar mensaje almacenado	B.85
Listar mensajes almacenados	B.86
Resumen de mensajes almacenados	B.87

19.7 *Facilidades facultativas de usuario de la MM*

Los elementos de servicio de la MM de base (§ 19.6) junto con las facilidades facultativas de usuario que se indican más adelante, pueden emplearse conjuntamente para un uso potenciado de una memoria de mensajes. La MM potenciada se puede emplear en cualquier aplicación que utilice el servicio TRM. Los elementos de servicio que comprenden las facilidades facultativas de usuario MM se indican en el cuadro 9/X.400.

CUADRO 9/X.400

Facilidades facultativas de usuario de la MM

Elementos de servicio	Clasificación	Referencia del anexo B
Alerta de mensaje almacenado	A	B.82
Reenvío automático de mensaje almacenado	A	B.83

19.8 *Servicio de mensajería interpersonal básico*

El servicio de mensajería interpersonal básico, que utiliza el servicio TRM, permite a un usuario enviar y recibir mensajes IP. Un usuario prepara los mensajes IP con la ayuda de su agente de usuario (AU). Los agentes de usuario cooperan entre sí para facilitar la comunicación entre sus respectivos usuarios. Para enviar un mensaje IP, el usuario de origen deposita el mensaje en su AU, especificando el nombre O/D del destinatario que debe recibir el mensaje IP. El mensaje IP, junto con el cual se transmite un identificador, es enviado por el AU de origen al AU de destino a través del servicio de transferencia de mensajes.

Después de haber sido entregado satisfactoriamente al AU de destino, el mensaje IP puede ser recibido por el destinatario. Para facilitar una comunicación significativa, un destinatario puede especificar el o los tipos de información codificada que podrán contener los mensajes IP que permitirá sean entregados a su AU. Cada mensaje IP entregado va acompañado de la indicación del o los tipos de información codificada originales, de cualquier conversión o conversiones que se hayan realizado, y del o los tipos de información codificada resultante. Además, en cada mensaje IP se especifican la hora de depósito y la hora de entrega. En el servicio básico se proporciona una notificación de no entrega. En el cuadro 10/X.400 se enumeran los elementos de servicio MIP que pertenecen al servicio MIP básico.

CUADRO 10/X.400

Elementos de servicio pertenecientes al servicio MIP básico

Elementos de servicio	Referencia del anexo B
Gestión acceso	B.1
Indicación de tipo de contenido	B.12
Indicación conversión	B.15
Indicación de hora de entrega	B.22
Identificación de mensaje IP	B.37
Identificación de mensaje	B.41
Notificación de no entrega	B.47
Indicación de los tipos de información codificada originales	B.54
Indicación de hora de depósito	B.89
Cuerpo tipificado	B.90
Registro de capacidades de usuario/AU	B.93

19.9 *Facilidades facultativas de usuario del servicio MIP*

Un conjunto de elementos de servicio del servicio MIP son facilidades facultativas de usuario. Estas facilidades pueden seleccionarse mensaje por mensaje o por un periodo de tiempo convenido, y se enumeran en los cuadros 11/X.400 y 12/X.400, respectivamente. Las facilidades de usuario locales pueden ser proporcionadas convenientemente junto con algunas de estas facilidades facultativas de usuario.

Las facilidades facultativas de usuario del servicio MIP seleccionadas mensaje por mensaje son clasificadas tanto para el origen como para el destino por los AU. Si un DG ofrece estas facilidades facultativas de usuario para ser originadas por los AU, el usuario puede crear y enviar mensajes IP de acuerdo con los procedimientos definidos para el elemento de servicio asociado. Si un DG ofrece estas facilidades facultativas de usuario para su recepción por los AU, AM y UA, el AU, la MM y UAEF receptor podrá recibir y reconocer la indicación asociada con el elemento de servicio correspondiente e informar al usuario de la facilidad facultativa de usuario solicitada. Cada facilidad de usuario se clasifica como adicional (A) o esencial (E) para los AU desde estas dos perspectivas.

Nota – Con el protocolo de acceso descrito en las Recomendaciones T.330, los terminales teletex pueden utilizar el servicio MIP básico y las facilidades facultativas de usuario proporcionadas por el sistema de tratamiento de mensajes.

CUADRO 11/X.400

Facilidades facultativas de usuario MIP seleccionables mensaje por mensaje

Elementos de servicio	Origen	Recepción	Referencia del anexo B
Reprodución física adicional	A	A	B.2
Destinatario alternativo autorizado	A	A	B.3
Indicación de los usuarios autorizantes	A	E	B.5
Indicación reenvío automático	A	E	B.6
Reproducción física básica	A	E*	B.7
Indicación de destinatario de copia ciega	A	E	B.8
Indicación de encripción de parte del cuerpo	A	E	B.9
Confidencialidad de contenido	A	A	B.10
Integridad del contenido	A	A	B.11
Prohibición de conversión	E	E	B.13
Prohibición de conversión en caso de pérdida de información		N/A	B.14
Recogida en ventanilla	A	E*	B.16
Recogida en ventanilla con aviso	A	A	B.17
Indicación de referencia recíproca	A	E	B.18
Entrega diferida	E	N/A	B.19
Cancelación de entrega diferida	A	N/A	B.20
Notificación de entrega	E	N/A	B.21
Entrega por el servicio burofax	A	A	B.23
Designación de destinatarios por el nombre de guía	A	N/A	B.24
Revelación de otros destinatarios	A	E	B.25
Indicación de historia de la expansión de la LD	N/A	E	B.26
Prohibición de expansión de la LD	A	A	B.27
SCU (servicio de correo urgente) [a]	A	E*	B.28
Indicación de fecha de expiración	A	E	B.29
Conversión explícita	A	N/A	B.30
Indicación de mensaje IP reenviado	A	E	B.31
Selección de grado de entrega	E	E	B.32
Indicación de importancia	A	E	B.35
Indicación de copia incompleta	A	A	B.36
Indicación de idioma	A	E	B.38
Designación de la última entrega	A	N/A	B.39
Confidencialidad del flujo del mensaje	A	N/A	B.40
Autenticación del origen del mensaje	A	A	B.42
Etiquetado de seguridad del mensaje	A	A	B.43
Integridad de la secuencia de mensajes	A	A	B.44
Entrega a múltiples destinos	E	N/A	B.45
Cuerpo de múltiples partes	A	E	B.46
Indicación de petición de notificación de no recepción	A	E	B.48
No rechazo de la entrega	A	A	B.49
No rechazo del origen	A	A	B.50
No rechazo del depósito	A	A	B.51
Indicación de obsolencia	A	E	B.52
Correo ordinario	A	E*	B.53
Indicación de originador	E	E	B.55
Destinatario alternativo solicitado por el originador	A	N/A	B.56
Notificación de entrega física por el STM	A	A	B.57
Notificación de entrega física por el SEF	A	E*	B.58
Autorización de reenvío físico	A	E*	B.59

CUADRO 11/X.400 *(continuación)*

Elementos de servicio	Origen	Recepción	Referencia del anexo B
Prohibición de reenvío físico	A	E*	B.60
Prevención de notificación de no entrega	A	N/A	B.61
Indicación de destinatarios primarios y de copia	E	E	B.62
Sonda	A	N/A	B.63
Autenticación del origen de la sonda	A	A	B.64
Prueba de entrega	A	A	B.65
Prueba de depósito	A	A	B.66
Indicación de petición de notificación de recepción	A	A	B.67
Redireccionamiento desautorizado por el originador	A	N/A	B.68
Correo certificado	A	A	B.70
Correo certificado para el destinatario en persona	A	A	B.71
Indicación de petición de respuesta	A	E	B.72
Indicación de mensaje IP de respuesta	E	E	B.73
Autenticación del origen del informe	A	A	B.74
Petición de dirección reenviante	A	A	B.75
Petición de metodo de entrega	E	N/A	B.76
Devolución de contenido	A	N/A	B.78
Indicación de sensibilidad	A	E	B.80
Entrega especial [a)]	A	E*	B.81
Supresión de mensajes almacenados	N/A	E**	B.84
Captura mensajes almacenados	N/A	E**	B.85
Listado de mensajes almacenados	N/A	E**	B.86
Resumen de mensajes almacenados	N/A	E**	B.87
Indicación de asunto	E	E	B.88
Correo inentregable con devolución de mensaje físico	A	E*	B.91
Utilización de lista de distribución	A	A	B.92

E Facilidad facultativa de usuario esencial, que hay que proporcionar.

E* Facilidad facultativa de usuario esencial que se aplica únicamente a las UAEF.

E** Facilidad facultativa de usuario esencial que se aplica únicamente a las MM.

A Facilidad facultativa de usuario adicional, que puede proporcionarse.

N/A No aplicable.

[a)] Cuando menos SCE o entrega especial deberán ser admitidos por la UAE y el SEF asociado.

Nota – En los casos de recepción por los AU de elementos de servicio clasificados como A puede ser necesario un acuerdo bilateral.

CUADRO 12/X.400

Facilidades facultativas de usuario MIP acordadas contractualmente por un periodo determinado

Elementos de servicio	Clasificación	Referencia del anexo B
Asignación de destinatario alternativo	A	B.4
Retención para entrega	A	B.33
Conversión implícita	A	B.34
Redireccionamiento de mensajes entrantes	A	B.69
Entrega restringida	A	B.77
Gestión de acceso seguro	A	B.79
Alerta de mensaje almacenado	A	B.82
Reenvío automático de mensaje almacenado	A	B.83

ANEXO A

(a la Recomendación X.400)

Glosario de términos

Nota – Las explicaciones proporcionadas no son necesariamente definiciones en el sentido estricto. Véanse también las definiciones del anexo B y las proporcionadas en otras Recomendaciones de la serie X.400 (especialmente la Recomendación X.402) de donde se tomaron muchos de los términos. Los términos tienen diferentes niveles de abstracción, que dependen de su origen.

A.1 **unidad de acceso (UA)**

E: access unit (AU)

F: unité d'accès (UA)

En el contexto de un sistema de tratamiento de mensajes, objeto funcional, componente del STM, que enlaza otro sistema de comunicación (por ejemplo un sistema de entrega física o la red télex) con el STRM y por medio del cual sus patronos efectúan tratamiento de mensajes como usuarios indirectos.

En el contexto de servicios de tratamiento de mensajes, la unidad que permite a los usuarios de un servicio intercomunicar con servicios de tratamiento de mensajes tales como el servicio MIP.

A.2 **destinatario real**

E: actual recipient

F: destinataire effectif

En el contexto del tratamiento de mensajes, destinatario potencial con relación al cual se efectúa una entrega o afirmación.

A.3 **administración**

E: administration

F: administration

En el contexto del CCITT una Administración (miembro de la UIT) o una empresa privada de explotación reconocida.

A.4 **nombre de dominio de administración**

E: administration domain name

F: nom d'un domaine d'administration

En el contexto del tratamiento de mensajes, atributo normalizado de una forma de nombre que identifica un DGAD con relación al país indicado por un nombre de país.

A.5 **dominio de gestión de administración (DGAD)**

E: administration management domain (ADMD)

F: domaine de gestion d'administration (DGAD)

Dominio de gestión que comprende sistemas de mensajería manejados por una Administración.

A.6 **destinatario alternativo**

E: alternate recipient

F: destinataire suppléant

En el contexto del tratamiento de mensajes, usuario o lista de distribución a los que el originador puede (pero no necesita) solicitar que un mensaje o sonda sea transmitido únicamente si no puede transmitirse a cierto destinatario preferido.

A.7 **atributo**

E: attribute

F: attribut

En el contexto del tratamiento de mensajes, elemento de información, componente de una lista de atributos, que describe a un usuario o lista de distribución y que también puede localizarlo en relación a la estructura física u organizacional del STM (o la red subyacente).

A.8 **lista de atributos**

E: attribute list

F: liste d'attributs

En el contexto del tratamiento de mensajes, estructura de datos, conjunto ordenado de atributos, que constituyen una dirección O/D.

A.9 **tipo de atributo**

E: attribute type

F: type d'attribut

Identificador que designa una clase de información (por ejemplo nombres personales). Forma parte de un atributo.

A.10 **valor de atributo**

E: attribute value

F: valeur d'attribut

Instancia de la clase de información designada por un tipo de atributo (por ejemplo, un nombre personal especial). Forma parte de un atributo.

A.11 **servicio básico**

E: basic service

F: service de base

En el contexto del tratamiento de mensajes, suma de características inherentes a un servicio.

A.12 **cuerpo**

E: body

F: corps

Componente de un mensaje. Otros componentes son el encabezamiento y el sobre.

A.13 **parte del cuerpo**

E: body part

F: partie du corps

Componente del cuerpo de un mensaje.

A.14 **nombre común**

E: common name

F: nom courant

En el contexto del tratamiento de mensajes, atributo normalizado de una forma de dirección O/D, que identifica al usuario o lista de distribución, con relación a la entidad designada por otro atributo (por ejemplo un nombre de organización).

A.15 **contenido**

E: content

F: contenu

En el contexto del tratamiento de mensajes, objeto de información, parte de un mensaje, que el STRM no examina ni modifica, salvo para conversión durante el transporte del mensaje.

A.16 **tipo de contenido**

E: content type

F: type de contenu

En el contexto del tratamiento de mensajes, identificador, en el sobre del mensaje, que identifica el tipo (por ejemplo sintaxis y semántica) del contenido del mensaje.

A.17 **conversión**

E: conversion

F: conversion

En el contexto del tratamiento de mensajes, suceso de transmisión en el que un ATM transforma parte del contenido de un mensaje de un tipo de información codificada a otro, o bien altera una sonda de manera que aparezca que los mensajes descritos fueron así modificados.

A.18 **nombre de país**

E: country name

F: nom de pays

En el contexto del tratamiento de mensajes, atributo normalizado de una forma de nombre que identifica a un país. Un nombre de país es una designación unívoca de un país con fines de envío y recepción de mensajes.

Nota – En el contexto de entrega física se aplican reglas adicionales. (Véase también nombre del país de entrega física y la Recomendación F.415.)

A.19 **entrega**

E: delivery

F: remise

En el contexto del tratamiento de mensajes, paso de transmisión en el que un ATM transporta un mensaje o informa al AM o AU de un destinatario potencial del mensaje o del originador del mensaje de asunto del informe o sonda.

A.20 **informe de entrega**

E: delivery report

F: rapport de remise

En el contexto del tratamiento de mensajes, informe que acusa la entrega, no entrega, exportación o afirmación del mensaje de asunto o sonda, o la expansión de una lista de distribución.

A.21 **depósito directo**

E: direct submission

F: dépôt direct

En el contexto del tratamiento de mensajes, paso de transmisión en el que el AU o MM del originador transmite un mensaje o sonda a un ATM.

A.22 **usuario directo**

E: direct user

F: utilisateur direct

En el contexto del tratamiento de mensaje, usuario que efectúa tratamiento de mensajes por uso directo del STRM.

A.23 **guía**

E: directory

F: annuaire

Colección de sistemas abiertos que cooperan para proporcionar servicios de guía.

A.24 **nombre de guía**

E: directory name

F: nom d'annuaire

Nombre de una inscripción en una guía.

Nota – En el contexto del tratamiento de mensajes, inscripción en la guía que permitirá extraer la dirección O/D para el depósito de un mensaje.

A.25 **agente de sistema de guía (ASG)**

E: directory system agent (DSA)

F: agent de système d'annuaire (ASA)

Proceso de aplicación ISA que forma parte de la guía, y cuyo papel es proporcionar a los AUG y/o a otros ASG, acceso a la base de información de la guía.

A.26 **agente de usuario de guía (AUG)**

E: directory user agent (DUA)

F: agent d'usager d'annuaire (AUA)

Proceso de aplicación ISA que representa a un usuario que obtiene acceso a la guía. Cada AUG sirve a un solo usuario, de modo que la guía puede controlar el acceso a la información de la guía en base a los nombres de AUG. Los AUG pueden también proporcionar una gama de facilidades locales para ayudar a los usuarios a satisfacer sus solicitudes (indagaciones) e interpretar las respuestas.

A.27 **lista de distribución (LD)**

E: distribution list (DL)

F: liste de distribution (LD)

En el contexto del tratamiento de mensajes, objeto funcional, componente del entorno de tratamiento de mensajes, que representa un grupo predeterminado de usuarios y otras listas de distribución y que es un destinatario potencial de los objetos de información por un STM.

Los miembros de la lista pueden contener nombres de O/D que identifican a usuarios o a otras listas de distribución.

A.28 **expansión de una lista de distribución**

E: distribution list expansion

F: allongement de liste de distribution

En el contexto del tratamiento de mensajes, suceso de transmisión en el que un ATM hace que una lista de distribución sea sustituida por los miembros de la misma, que serán los destinatarios inmediatos del mensaje.

A.29 **nombre de lista de distribución**

E: distribution list name

F: nom de liste de distribution

Nombre O/D asignado para representar un conjunto de direcciones O/D y nombres de guía.

A.30 **dominio**

E: domain

F: domaine

Véase dominio de gestión.

A.31 **atributos definidos por el dominio**

E: domain defined attributes

F: attributs définis d'un domaine

Atributos opcionales de una dirección O/D asignados a nombres bajo la responsabilidad de un dominio de gestión.

A.32 **elemento de servicio**

E: element of service

F: élément de service

Unidad funcional para segmentar y describir características de tratamiento de mensajes.

A.33 **tipo de información codificada (TIC)**

E: encoded information type (EIT)

F: type de codage (TC)

En el contexto del tratamiento de mensajes, identificador, en el sobre de un mensaje, que identifica un tipo de información codificada representada en el contenido del mensaje. Identifica el medio y formato (por ejemplo texto AI5, facsímil grupo 3) de una porción individual del contenido.

A.34 **sobre**

E: envelope

F: enveloppe

En el contexto del tratamiento de mensajes, objeto de información, parte de un mensaje, cuya composición varía de un paso de transmisión a otro y que identifica diversamente al originador del mensaje y los destinatarios potenciales, documenta su pasado y dirige su ulterior transmisión por el STRM, y caracteriza su contenido.

A.35 **conversión explícita**

E: explicit conversion

F: conversion explicite

En el contenido del tratamiento de mensajes, conversión en la que el originador selecciona los tipos inicial y final de información codificada.

A.36 **componentes de ampliación de dirección de entrega física**

E: extension of physical delivery address components

F: développement de composants d'adresse de remise physique

Atributo normalizado de una dirección postal O/D como medio para proporcionar información adicional sobre el punto de entrega física en una dirección postal, por ejemplo el nombre de un barrio, el número de un apartamento y del piso en un edificio grande.

A.37 **componentes de ampliación de dirección postal O/D**

E: extension of postal O/R address components

F: développement de composants d'adresse postale E/D

Atributo normalizado de una dirección postal O/D como medio para proporcionar información adicional que especifique al destinatario en una dirección postal, por ejemplo, por una unidad de organización.

A.38 **dirección postal O/D formatizada**

E: formatted postal O/R address

F: adresse postale E/D formatée

Dirección O/D basada en una dirección postal con atributos.

A.39 **encabezamiento**

E: heading

F: en-tête

Componente de un mensaje IP. Otros componentes son el sobre y el cuerpo.

A.40 **destinatario inmediato**

E: immediate recipient

F: destinataire direct

En el contexto del tratamiento de mensajes, uno de los destinatarios potenciales asignados a un caso particular de un mensaje o sonda (por ejemplo un caso creado por división).

A.41 **conversión implícita**

E: implicit conversion

F: conversion implicite

En el contexto del tratamiento de mensajes, conversión en la que el ATM elige los tipos de información codificada inicial y final.

A.42 **depósito indirecto**

E: indirect submission

F: dépôt indirect

En el contexto del tratamiento de mensajes, etapa de transmisión en el que un AU originador transfiere un mensaje o sonda a un ATM a través de una MM.

A.43 **usuario indirecto**

E: indirect user

F: utilisateur indirect

En el contexto del tratamiento de mensajes, usuario que participa en el tratamiento de mensajes por el uso indirecto del STM, es decir, por medio de otro sistema de comunicación (por ejemplo un sistema de entrega física o una red télex) al que está enlazado el STM.

Nota – Los usuarios indirectos se comunican con usuarios directos del STM por medio de unidades de acceso.

A.44 **intercomunicación**

E: intercommunication

F: intercommunication

En el contexto del tratamiento de mensajes, relación entre servicios en la que uno de los servicios es un servicio de tratamiento de mensajes que permite al usuario del servicio de tratamiento de mensajes comunicarse con usuarios de otros servicios.

Nota – Como ejemplos pueden citarse la intercomunicación entre el servicio MIP y el servicio télex, así como la intercomunicación entre los servicios de tratamiento de mensajes y los servicios de entrega física.

A.45 **servicio de mensajería interpersonal**

E: interpersonal messaging service

F: service de messagerie de personne à personne

Servicio de mensajería entre usuarios que pertenecen al mismo dominio de gestión o a diferentes dominios de gestión, por medio de tratamiento de mensajes, basado en el servicio de transferencia de mensajes.

A.46 **Mensaje IP**

E: IP-message

F: message PP

Contenido de un mensaje en el servicio MIP.

A.47 **atributos postales locales**

E: local postal attributes

F: attributs postaux locaux

Atributos normalizados de una dirección postal O/D como medio para distinguir entre lugares que tienen un mismo nombre (por ejemplo por nombre de provincia, nombre de país, o atributo geográfico) en una dirección postal.

A.48 **dominio de gestión (DG)**

E: management domain (MD)

F: domaine de gestion (DG)

En el contexto del tratamiento de mensajes, grupo de sistema de mensajería –de los cuales al menos uno contiene o realiza un ATM– que es manejado por una sola organización. Es un bloque constructivo primario utilizado en la construcción organizacional del STM. Se refiere a una zona de organización para la prestación de servicios.

Nota – Un dominio de gestión puede, pero no tiene necesariamente que, coincidir con una zona geográfica.

A.49 **nombre de dominio de gestión**

E: management domain name

F: nom d'un domaine de gestion

Designación unívoca de un dominio de gestión para el envío y la recepción de mensajes.

A.50 **miembros**

E: members

F: membres

En el contexto del tratamiento de mensajes, grupo de usuarios y listas de distribución implicados por un nombre de lista de distribución.

A.51 **mensaje**

E: message

F: message

Instancia de la clase primaria de objeto de información transmitida por medio de transferencia de mensajes y que comprende un sobre y un contenido.

A.52 **tratamiento de mensajes (TM)**

E: message handling (MH)

F: messagerie (traitement des messages) (M)

Tarea distribuida de procesamiento de información que integra las subtareas intrínsecamente relacionadas de transferencia de mensajes y el almacenamiento de mensajes.

A.53 **entorno de tratamiento de mensajes**

E: message handling environment

F: environnement de traitement de messages

Entorno en el que se realiza el tratamiento de mensajes incluyendo STM, usuarios y listas de distribución.

Suma de todos los componentes de los sistemas de tratamiento de mensajes.

Nota – Ejemplos de componentes.

- agentes de transferencia de mensajes,
- agentes de usuario,
- almacenes de mensajes,
- unidades de acceso,
- usuarios.

A.54 **servicio de tratamiento de mensajes**

E: message handling service

F: service de messagerie

Servicio proporcionado por medio de sistemas de tratamiento de mensajes.

Nota 1 – El servicio puede ser proporcionado por medio de los dominios de gestión de la administración o dominios de gestión privados.

Nota 2 – Ejemplos de servicios de tratamiento de mensajes:

- servicio de mensajería interpersonal (servicio MIP),
- servicio de transferencia de mensajes (servicio TRM).

A.55 **sistema de tratamiento de mensajes (STM)**

E: message handling system (MHS)

F: système de messagerie (STM)

Objeto funcional componente del entorno del tratamiento de mensajes, que transporta objetos de información de una parte a otra.

A.56 **almacenamiento de mensajes**

E: message storage

F: mémorisation des messages

Almacenamiento automático para extracción posterior de objetos de información transmitidos por transferencia de mensaje. Es un aspecto del tratamiento de mensajes.

A.57 **memoria de mensajes (MM); almacenador de mensajes (AM)**

E: message store (MS)

F: mémoire des messages (MM)

Objeto funcional, componente del STM, que proporciona a un solo usuario directo capacidades de almacenamiento de mensajes.

A.58 **transferencia de mensajes (TRM)**

E: message transfert (MT)

F: transfert de messages (TM)

Transporte de objetos de información no efectuado en tiempo real entre partes que utilizan computadores como intermediarios. Es un aspecto del tratamiento de mensajes.

A.59 **agente de transferencia de mensajes (ATM)**

E: message transfert agent (MTA)

F: agent de transfert de messages (ATM)

Objeto funcional, componente del STRM, que transmite efectivamente objetos de información a usuarios y listas de distribución.

A.60 **servicio de transferencia de mensajes**

E: message transfer service

F: service de transfert de messages

Servicio relativo al depósito, transferencia y entrega de mensajes para otros servicios de mensajería.

A.61 **sistema de transferencia de mensajes (STRM)**

E: message transfer system (MTS)

F: système de transfert de messages (système TM)

Objeto funcional consiste en uno o más agentes de transferencia de mensajes y que provea la transferencia de mensajes con almacenamiento y retransmisión entre agentes de usuario, memorias de mensajes y unidades de acceso.

A.62 **sistema de mensajería**

E: messaging system

F: système de messagerie

Un sistema de computador (que puede pero no tiene necesariamente que ser un sistema abierto) que contiene o realiza uno o más objetos funcionales. Es un bloque constructivo utilizado en la construcción física del STM.

A.63 **dirección O/D nemotécnico**

E: mnemonic O/R address

F: adresse mnémonique E/D

Dirección O/D que identifica nemotécnicamente a un usuario o lista de distribución con relación al DGAD por medio de la cual se accede al usuario o se expande la lista de distribución. Identifica un DGAM, y a un usuario o lista de distribución con relación a ese DGAD.

A.64 **autoridad de denominación**

E: naming authority

F: autorité responsable de l'appellation

Autoridad responsable de la atribución de nombres.

A.65 **dirección de red**

E: network address

F: adresse réseau

En el contexto del tratamiento de mensajes, atributo normalizado de una forma de dirección O/D, que proporciona la dirección de red de un terminal. Comprende las cifras del plan de numeración internacional para los puntos de acceso a la red.

A.66 **no entrega**

E: non-delivery

F: non-remise

En el contexto del tratamiento de mensajes, suceso de transmisión en el que un ATM determina que el STRM no puede entregar un mensaje a uno o más de los destinatarios inmediatos, o no puede entregar el informe al originador del mensaje o sonda en cuestión.

A.67 **acceso no registrado**

E: non-registered access

F: accès non homologué

En el contexto de los servicios de tratamiento de mensajes, acceso al servicio a través de medios de telecomunicación que estén a disposición del público en general por parte de usuarios que no han sido registrados explícitamente por el proveedor del servicio ni tienen asignada una dirección O/D.

A.68 **dirección O/D numérica**

E: numeric O/R address

F: adresse numérique E/D

En el contexto del tratamiento de mensajes, dirección O/D que identifica numéricamente a un usuario en relación con un DGAD por medio del cual se gana acceso al usuario. Identifica un DGAD y un usuario con relación a ese DGAD. Identifica a un usuario de los STRM por medio de un teclado numérico.

A.69 **identificador de usuario numérico**

E: numeric user identifier

F: identificateur numérique d'utilisateur

Atributo de una dirección O/D como una secuencia única de información numérica para identificar a un usuario.

A.70 **dirección O/D**

E: O/R address

F: adresse E/D

En el contexto del tratamiento de mensajes, lista de atributos que distingue a un usuario o LD de otro e identifica el punto de acceso del usuario al STM o el punto de expansión de la lista de distribución.

A.71 **nombre O/D**

E: O/R name

F: nom E/D

En el contexto del tratamiento de mensajes, objeto de información por medio del cual un usuario puede ser designado como el originador, o usuario o lista de distribución designados como destinatario potencial de un mensaje o sonda. Un nombre O/D permite distinguir un usuario o lista de distribución de otro, u otra, y también puede identificar su punto de acceso al STM.

A.72 **facilidades facultativas de usuario**

E: optional user facilities

F: services complémentaires offerts en option à l'utilisateur

En el contexto de los servicios de tratamiento de mensajes, son elementos de servicio que pueden ser seleccionados por el usuario sobre una base contractual (periodo de tiempo convenido) o para cada mensaje.

Nota 1 – Las facilidades facultativas de usuario se clasifican en esenciales y adicionales.

Nota 2 – Las facilidades facultativas de usuario esenciales deben ponerse a la disposición de todos los usuarios de tratamiento de mensajes.

Nota 3 – Las facilidades facultativas de usuario adicionales se ponen a disposición para uso nacional, o internacional sobre la base de acuerdos bilaterales entre los proveedores del servicio.

A.73 **nombre de la organización**

E: organization name

F: nom d'organisation

Atributo normalizado de una dirección O/D como designación unívoca de una organización con la finalidad de enviar y recibir mensajes.

A.74 **nombre de la unidad organizadora**

E: organizational unit name

F: nom d'une unité d'organisation

Atributo normalizado de una dirección O/D como designación unívoca de una unidad organizacional de una organización con la finalidad de enviar y recibir mensajes.

A.75 **originador**

E: originator

F: expéditeur

En el contexto de tratamiento de mensajes, el usuario (pero no la lista de distribución) que es la fuente final de un mensaje o sonda.

A.76 **nombre personal**

E: personal name

F: nom personnel

En el contexto de tratamiento de mensajes, atributo normalizado de una forma de dirección O/D que identifica a una persona relacionada a la entidad designada por otro atributo (por ejemplo un nombre de organización).

Nota – Los componentes pueden ser, por ejemplo:

- apellido,
- nombre (de pila),
- iniciales,
- calificador de generación.

A.77 **entrega física (EF)**

E: physical delivery (PD)

F: remise physique (RP)

ARCHIVES U.I.T. GENÈVE

Entrega de un mensaje en forma física, por ejemplo una carta, a través del sistema de entrega física.

A.78 **unidad de acceso de entrega física (UAEF)**

E: physical delivery access unit (PDAU)

F: unité d'accès de remise physique (UARP)

Unidad de acceso que somete los mensajes (pero no las sondas ni los informes) a reproducción física.

A.79 **componentes de dirección de entrega física**

E: physical delivery address components

F: composants d'une adresse de remise physique

En una dirección postal, contiene la información necesaria para la entrega física local dentro de la zona de entrega física de la oficina de entrega física, es decir, una dirección-calle, una dirección-apartado postal, una dirección de lista de correos o, como otra posibilidad, un nombre unívoco.

Nota – La información generalmente está limitada a una línea de hasta 30 caracteres gráficos imprimibles. Se puede suministrar información adicional utilizando el tipo de atributo «ampliación de componentes de dirección de entrega física».

A.80 **nombre de país de entrega física**

E: physical delivery country name

F: nom du pays de remise physique

En el contexto de entrega física, descripción unívoca del país del destino final.

A.81 **dominio de entrega física**

E: physical delivery domain

F: domaine de remise physique

Dominio de responsabilidad de una organización que presta servicios de entrega física y, opcionalmente un ATM/UAEF.

A.82 **componentes de dirección de oficina de entrega física**

E: physical delivery office address components

F: composants d'une adresse de bureau de remise physique

En una dirección postal, contienen la información que especifica la oficina responsable de la entrega física local.

Nota – La información generalmente está limitada a una línea de hasta 30 caracteres gráficos imprimibles. En algunos países el código postal va después de los componentes de dirección de oficina de entrega física, en una línea aparte (posiblemente junto con el nombre de país).

A.83 **nombre de oficina de entrega física**

E: physical delivery office name

F: nom du bureau de remise physique

Atributo normalizado de una dirección O/D postal, en el contexto de la entrega física, que especifica el nombre de la ciudad, localidad, etc. en donde está situada la oficina de entrega física, o donde se realiza la entrega física.

A.84 **número de oficina de entrega física**

E: physical delivery office number

F: numéro du bureau de remise physique

Atributo normalizado y, en una dirección postal O/D, medio para distinguir entre dos o más oficinas de entrega física en una ciudad, etc.

A.85 **nombre de la organización de entrega física**

E: physical delivery organization name

F: nom d'organisation de remise physique

Nombre de forma libre de la entidad destinataria dentro de la dirección postal, tomando en cuenta las limitaciones de longitud especificadas.

A.86 **nombre personal de entrega física**

E: physical delivery personal name

F: nom personnel de remise physique

En una dirección postal, nombre de forma libre del destinatario individual, que contiene el apellido y, opcionalmente, los nombres, iniciales, títulos y calificador de generación, tomando en cuenta las limitaciones de longitud especificadas.

A.87 **servicio de entrega física**

E: physical delivery service

F: service de remise physique

Servicio proporcionado por un sistema de entrega física.

A.88 **nombre del servicio de entrega física**

E: physical delivery service name

F: nom du service de remise physique

Atributo normalizado de una dirección postal O/D en forma del nombre del servicio en el país que recibe electrónicamente el mensaje en nombre del servicio de entrega física.

A.89 **sistema de entrega física (SEF)**

E: physical delivery system (PDS)

F: système de remise physique (SRP)

Sistema que realiza la entrega física. Un tipo importante de servicio de entrega física es el sistema postal.

A.90 **mensaje físico**

E: physical message

F: message physique

Objeto físico que incluye un sobre de relevo y su contenido, por ejemplo una carta.

A.91 **reproducción física**

E: physical rendition

F: conversion physique

Transformación de un mensaje STM en un mensaje físico, por ejemplo imprimiendo el mensaje en papel e introduciéndolo en un sobre de papel.

A.92 **código postal**

E: postal code

F: code postal

Atributo normalizado de una dirección postal O/D para especificar la zona geográfica, y en el contexto del STM, utilizado para el encaminamiento de mensajes.

A.93 **dirección postal O/D**

E: postal O/R address

F: adresse postale E/D

En el contexto de tratamiento de mensajes, dirección O/D que identifica a un usuario por medio de su dirección postal. Identifica al servicio de entrega física por medio del cual se accede al usuario y proporciona la dirección postal del usuario.

A.94 **componentes de dirección postal O/D**

E: postal O/R address components

F: composants d'une adresse postale E/D

En una dirección postal, contienen la información para describir al emisor o destinatario por medio de su nombre (nombre personal de entrega física, nombre de organización de entrega física).

Nota – En una dirección postal, se limita, en general, la información a una línea de 30 caracteres imprimibles. Puede proporcionarse información adicional utilizando el tipo de atributo «componentes de ampliación de la dirección postal O/D».

A.95 **dirección-apartado de correos**

E: post office box address (P.O. box address)

F: adresse de case postale

Atributo normalizado en la dirección postal que indica que se solicita la entrega física mediante un apartado de correos. Lleva un número de apartado de correos para la distribución a dicho apartado.

A.96 **dirección-lista de correos**

E: poste restante address

F: adresse poste restante

Atributo normalizado en la dirección postal que indica que se solicita la entrega física en ventanilla. También puede llevar un código.

A.97 **destinatario potencial**

E: potential recipient

F: destinataire potentiel

En el contexto del tratamiento de mensajes, cualquier usuario o lista de distribución hacia la cual se transporta un mensaje o sonda en el curso de la transmisión. En forma equivalente, destinatario substituto o miembro, alternativo o preferido.

A.98 **receptor preferido**

E: preferred recipient

F: destinataire préféré

En el contexto del tratamiento de mensajes, uno de los usuarios y listas de distribución, que el originador elige como destino preferido de la sonda o mensaje.

A.99 **nombre de dominio privado**

E: private domain name

F: nom d'un domaine privé

En el contexto del tratamiento de mensajes, atributo normalizado de una forma de dirección O/D que identifica a un DGPR con relación al DGAD denotado por un nombre de dominio de administración.

Nota – Son administradas por el DGAD al que está asociado el DGPR.

A.100 **dominio de gestión privado (DGPR)**

E: private management domain (PRMD)

F: domaine de gestion privé (DGPR)

En el contexto del tratamiento de mensajes, dominio de gestión que incluye sistemas de mensajería manejados por una organización que no es una Administración.

A.101 **sonda**

E: probe

S: essai

En el contexto del tratamiento de mensajes, ejemplo de una clase secundaria de objetos de información transmitidos por medio de transferencia de mensajes, que describe una clase de mensajes, y que se utiliza para determinar la entregabilidad de dichos mensajes.

A.102 **servicio público de tratamiento de mensajes**

E: public message handling service

F: service public de messagerie

Servicio de tratamiento de mensajes ofrecido por una Administración.

A.103 **servicios públicos**

E: public services

F: services publics

En el contexto de las telecomunicaciones, los servicios ofrecidos por las Administraciones.

A.104 **recepción**

E: receipt

F: réception

En el contexto del tratamiento de mensajes, paso de transmisión en el que, ora un AU transmite un mensaje o informe a su usuario directo, o el sistema de comunicación que sirve al usuario indirecto, transmite dicho objeto de información a ese usuario.

A.105 **destinatario**

E: recipient

F: destinataire

Véase destinatario real.

A.106 **repetición**

E: recursion

F: récursivité

En el contexto del tratamiento de mensajes, el hecho de que un mensaje vuelva a la misma lista de distribución de origen y potencialmente circule indefinidamente.

A.107 **redireccionamiento**

E: redirection

F: réacheminement

En el contexto del tratamiento de mensajes, suceso de transmisión en el que un ATM reemplaza a un usuario, entre los destinatarios inmediatos del mensaje, por otro usuario que fue seleccionado previamente por el primer usuario para dicho mensaje.

A.108 **acceso registrado**

E: registered access

F: accès homologué

En el contexto de los servicios de tratamiento de mensajes, acceso al servicio por parte de usuarios que han sido registrados por el proveedor del servicio para utilizarlo y a los que se ha asignado una dirección O/D.

A.109 **informe**

E: report

F: rapport

En el contexto del tratamiento de mensajes, ejemplo de una clase secundaria de objeto de información transmitida por medio de transferencia de mensajes. Es generado por el STRM e informa del resultado o progreso de la transmisión de un mensaje o sonda a uno o más destinatarios potenciales.

A.110 **recuperación**

E: retrieval

F: extraction

En el contexto del tratamiento de mensajes, paso de transmisión en el cual una memoria de mensajes de un usuario transporta un mensaje o informa al AU del usuario. El usuario es un destinatario real del mensaje o el originador del mensaje o sonda de asunto.

A.111 **capacidades de seguridad**

E: security capabilities

F: capacité de sécurité

En el contexto del tratamiento de mensajes, mecanismos que protegen contra diversos riesgos de seguridad.

A.112 **acceso especializado**

E: specialized access

F: accès spécialisé

En el contexto del tratamiento de mensajes, participación de unidades de acceso especializadas que proporcionan la intercomunicación entre servicios de tratamiento de mensajes y otros servicios de telecomunicación.

A.113 **atributo normalizado**

E: standard attribute

F: attribut normalisé

Atributo cuyo tipo está ligado a cierta clase de información.

A.114 **dirección-calle**

E: street address

F: adresse de rue

Un atributo normalizado en la dirección postal que proporciona información para la distribución local y la entrega física, es decir el nombre de la calle, el identificador de la calle (como calle, plaza, avenida) y el número de la casa.

A.115 **asunto**

E: subject

F: objet

En el contexto del tratamiento de mensajes, la información, parte del encabezamiento, que resume el contenido del mensaje tal como lo ha especificado el originador.

A.116 **mensaje de asunto**

E: subject message

F: message objet

Mensaje que es el asunto de un informe.

A.117 **sonda de asunto**

E: subject probe

F: essai objet

Sonda que es el asunto de un informe.

A.118 **depósito**

E: submission

F: dépôt

Depósito directo o depósito indirecto.

A.119 **destinatario sustituto**

E: substitute recipient

F: destinataire substitut

En el contexto del tratamiento de mensajes, usuario o lista de distribución hacia el cual un destinatario miembro, alternativo o preferido (pero no otro substituto), puede haber elegido redireccionar mensajes (pero no sondas).

A.120 **identificador de terminal**

E: terminal identifier

F: identificateur de terminal

Atributo normalizado en una dirección O/D que proporciona información para identificar un terminal entre varios.

Nota – Pueden citarse como ejemplos el distintivo télex o y el identificador de terminal de teletex.

A.121 **dirección O/D de terminal**

E: terminal O/R address

F: adresse terminale E/D

En el contexto del tratamiento de mensajes, dirección O/D que identifica a un usuario por medio de la dirección de red de su terminal y que puede identificar el DGAM a través del cual se accede a ese terminal. Los terminales identificados pueden pertenecer a redes diferentes.

A.122 **tipo de terminal**

E: terminal type

F: type de terminal

Atributo normalizado de una dirección O/D que indica el tipo de un terminal.

Nota – Ejemplos: télex, teletex, facsímil G3, facsímil G4, AI5, terminal videotex.

A.123 **transferencia**

E: transfer

F: transfert

En el contexto del tratamiento de mensajes, un paso de transmisión en el que un ATM transporta un mensaje, sonda o informe a otro ATM.

A.124 **sistema de transferencia**

E: transfer system

F: système de transfert

Sistema de mensajería que contiene un ATM; opcionalmente puede contener una o más unidades de acceso, pero no contendrá ni un AU, ni un almacenador de mensajes.

A.125 **transmisión**

E: transmittal

F: transmission

Transporte o tentativa de transporte de un mensaje desde su originador hasta sus destinatarios potenciales, o de una sonda desde su originador hasta ATM capaces de afirmar cualquier entregabilidad descrita del mensaje a sus destinatarios potenciales. También incluye el transporte o tentativa de transporte, al originador del mensaje o sonda, de cualquier informe provocado por el mensaje o sonda. Es una secuencia de pasos y sucesos de transmisión.

A.126 **dirección postal O/D no formatizada**

E: unformatted postal O/R address

F: adresse postale E/D non formatée

Dirección O/D basada en una dirección postal no formatizada.

A.127 **nombre postal exclusivo**

E: unique postal name

F: nom postal unique

En una dirección postal, atributo normalizado que describe el punto de entrega física por medio de un nombre único, por ejemplo el de un edificio.

A.128 **usuario**

E: user

F: usager/utilisateur

En el contexto del tratamiento de mensajes, objeto funcional (por ejemplo una persona), componente del entorno de tratamiento de mensajes que, más bien que proporcionar, interviene en el tratamiento de mensajes y que es una fuente o destino potencial de los objetos de información transportados por el STM.

A.129 **agente de usuario (AU)**

E: user agent (UA)

F: agent d'usager (AU)

En el contexto del tratamiento de mensajes, objeto funcional, componente del STM, por medio del cual un usuario directo individual interviene en tratamiento de mensajes.

Componente del STM con el que interactúa el usuario.

ANEXO B

(a la Recomendación X.400)

Definiciones de los elementos de servicio

Nota – Las abreviaturas que aparecen en el renglón de los epígrafes tienen los siguientes significados:

TRM Transferencia de mensajes

MIP Mensajería interpersonal

EF Entrega física

MM Memoria de mensajes

PD Por cada destinatario (disponible por cada uno de los destinatarios)

B.1 *Gestión de acceso* TRM

Este elemento de servicio permite a un AU y a un ATM establecer accesos entre sí y tratar información asociada con el establecimiento del acceso.

El elemento permite al AU y al ATM identificar y validar recíprocamente sus identidades. Permite al AU especificar su dirección O/D y mantener la seguridad de acceso. Cuando se logra la seguridad de acceso por medio de contraseñas, éstas pueden actualizarse periódicamente.

Nota – El elemento de servicio gestión de acceso seguro proporciona una forma más segura de gestión de acceso.

B.2 *Reproducción física adicional* EF PD

Este elemento de servicio permite a un usuario originador solicitar a la UAEF que suministre las facilidades de reproducción adicionales (por ejemplo, clase de papel, impresión en color, etc.). Se requiere un acuerdo bilateral para utilizar este elemento de servicio.

B.3 *Destinatario alternativo autorizado* TRM

Este elemento de servicio permite a un AU de origen especificar que el mensaje depositado puede entregarse a otro destinatario como se indica más adelante.

Un DG de destino interpretará todos los atributos de usuario para seleccionar un AU destinatario. Cabe distinguir tres casos:

1) Todos los atributos concuerdan exactamente con los de un AU de abonado. Se trata de entregar el mensaje a este AU.
2) Los atributos suministrados son insuficientes, o concuerdan con los de más de un AU de abonado. El mensaje no puede entregarse.
3) Se suministra por lo menos el conjunto mínimo de atributos requeridos por el DG de destino. Sin embargo, teniendo en cuenta todos los atributos, éstos no concuerdan con los de ningún AU.

En el tercer caso, un DG que admite el elemento de servicio asignación de destinatario alternativo puede entregar el mensaje a un AU que haya sido asignado para recibir tales mensajes. A este AU se le notificará la dirección O/D del destinatario deseado especificada por el originador. La entrega a este AU se comunicará al originador mediante una notificación de entrega, si así lo ha solicitado.

B.4 *Asignación de destinatario alternativo* TRM

Este elemento de servicio confiere a un AU la facultad de que se le entreguen mensajes para los cuales no hay concordancia exacta entre los atributos de destinatario especificados y el nombre del usuario. Este AU se especifica en términos de uno o más atributos para los cuales debe haber una concordancia exacta, y uno o más atributos para los cuales es aceptable cualquier valor. Por ejemplo, una organización puede establecer un AU para recibir todos los mensajes para los cuales el nombre del país, el nombre de dominio de gestión de administración y el nombre de la organización (por ejemplo, el nombre de la compañía) concuerdan exactamente, pero el nombre personal del destinatario no corresponde a ninguna persona conocida por un STM en esa organización. Esto permite a la organización tratar manualmente los mensajes para estas personas.

Para que reasigne un mensaje a un destinatario alternativo, el originador debe haber solicitado el elemento de servicio destinatario alternativo autorizado.

B.5 *Indicación de los usuarios autorizantes* MIP

Este elemento de servicio permite al originador indicar al destinatario los nombres de la o las personas que autorizaron su envío. Por ejemplo, una persona puede autorizar una acción particular que se comunica subsiguientemente a los interesados por otra persona, por ejemplo, una secretaria. Se considera que la primera persona autoriza su envío mientras que la segunda es la que envió el mensaje (originador). Esto no implica autorización en el nivel de firma.

B.6 *Indicación de reenvío automático* MIP

Este elemento de servicio permite al destinatario determinar que un cuerpo de un mensaje IP entrante contiene un mensaje IP que ha sido reenviado automáticamente. De este modo, el destinatario puede distinguir cuándo un mensaje IP entrante contiene en el cuerpo un mensaje IP reenviado (como se describe en el § B.31). Al igual que el mensaje IP reenviado, un mensaje IP reenviado automáticamente puede ir acompañado de información (por ejemplo, impresión de la hora, indicación de conversión) asociada con su entrega original.

Nota – La indicación de que se ha producido el reenvío automático de un mensaje IP permite al AU de la MIP destinataria, si así se elige, evitar otro reenvío automático y por ende la posibilidad de bucles. Además, el AU de la MIP destinataria puede elegir o no el reenvío automático basado en otros criterios (por ejemplo, clasificación de sensibilidad).

Cuando un AU de MIP reenvía automáticamente un mensaje IP, lo hace constar en el mismo. Si se ha solicitado notificación de recepción/no recepción para el mensaje de usuario así reenviado automáticamente, el AU de MIP genera una notificación de no recepción informando al originador de ese reenvío automático del mensaje IP. La notificación incluye facultativamente un comentario suministrado por el destinatario deseado originalmente. Ningún AU de MIP genera otra notificación aplicable al mensaje IP reenviado automáticamente.

B.7 *Reproducción física básica* EF PD

Este elemento de servicio permite a la UAEF proporcionar las facilidades básicas de transformación para convertir el mensaje STM en un mensaje físico. Esta es la acción por defecto que debe ejecutar la UAEF.

B.8 *Indicación de destinatario de copia ciega* MIP PD

Este elemento de servicio permite al originador proporcionar los nombres O/D de uno o más usuarios adicionales o LD que son destinatarios deseados del mensaje IP que se envía. Estos nombres no se revelan a los destinatarios primarios ni a los destinatarios de copias. El hecho de revelar o no a los destinatarios adicionales la presencia de los otros es un asunto de carácter local.

B.9 *Indicación de cifrado de parte del cuerpo* MIP

Este elemento de servicio permite al originador indicar al destinatario que una parte específica del cuerpo del mensaje IP que se envía ha sido cifrada. Puede utilizarse el cifrado para impedir una inspección o modificación no autorizada de la parte del cuerpo. El destinatario puede utilizar este elemento de servicio para determinar que alguna parte (o partes) del cuerpo del mensaje IP deben ser descifradas. Sin embargo, este elemento de servicio, por sí mismo, no cifra ni descifra ninguna parte del cuerpo.

B.10 *Confidencialidad del contenido* TRM

Este elemento de servicio permite al originador de un mensaje proteger el contenido del mensaje contra su revelación a otro que no sea el destinatario o los destinatarios deseados. La confidencialidad del contenido se entiende para cada mensaje y puede utilizar técnicas de cifrado simétricas o asimétricas.

B.11 *Integridad del contenido* TRM PD

Este elemento de servicio permite al originador del mensaje proporcionar al destinatario del mensaje un medio de verificar que el contenido del mensaje no ha sido modificado. La integridad del contenido se entiende para cada destinatario y puede utilizar una técnica de cifrado simétrica o asimétrica.

B.12 *Indicación de tipo de contenido* TRM

Este elemento de servicio permite a un AU de origen indicar el tipo de contenido para cada mensaje depositado. Al AU destinatario pueden habérsele entregado uno o más tipos de contenido. Un ejemplo de tipo de contenido es el contenido generado por la clase MIP de AU cooperantes.

B.13 *Prohibición de conversión* TRM

Este elemento de servicio permite a un AU ordenar al STRM que no efectúe conversiones del tipo de información codificada implícitas para un determinado mensaje depositado.

B.14 *Prohibición de conversión en caso de pérdida de información* TRM

Este elemento de servicio permite a un AU de origen ordenar al STRM que no efectúe conversiones del tipo de información codificada para un determinado mensaje depositado si dichas conversiones pudieran ocasionar una pérdida de información. La pérdida de información se trata con detalle en la Recomendación X.408.

En caso de que se seleccionaran este elemento de servicio y de prohibición de conversión, se dará prioridad a este último.

Nota – Este elemento de servicio no ofrecerá protección contra una posible pérdida de información en ciertos casos en los que el destinatario utiliza un dispositivo entrada/salida cuyas capacidades son desconocidas para el ATM.

B.15 *Indicación de conversión* TRM PD

Este elemento de servicio permite al STRM indicar al AU destinatario que el STRM realizó la conversión del tipo de información codificada en un mensaje entregado. El AU destinatario es informado de los tipos resultantes.

B.16 *Recogida en ventanilla* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que mantenga el mensaje físico listo para la recogida en ventanilla en la oficina de correos especificada por el originador, o en la oficina de correos más cercana a la dirección del destinatario que ofrece el servicio de recogida de ventanilla.

B.17 *Recogida en ventanilla con aviso* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que mantenga el mensaje físico listo para la recogida en ventanilla en la oficina de correos especificada por el originador, o en la oficina de correos más cercana a la dirección del destinatario que ofrece el servicio de recogida en ventanilla, e informe al destinatario por vía telefónica, télex o teletex utilizando el número suministrado por el originador.

B.18 *Indicación de referencia recíproca* MIP

Este elemento de servicio permite al originador asociar al mensaje IP que se envía los identificadores globales exclusivos de uno o más mensajes IP. Esto permite al AU de MIP del destinatario, por ejemplo, extraer del registro una copia de los mensajes IP referenciados.

B.19 *Entrega diferida* TRM

Este elemento de servicio permite a un AU de origen ordenar al STRM que no entregue un mensaje que deposita antes de una fecha y hora determinadas. La entrega se efectuará lo más próxima posible a la fecha y hora especificadas, pero no antes. La fecha y hora especificadas para la entrega diferida están sujetas a un límite que es definido por el dominio de gestión del originador.

Nota – El almacenamiento del mensaje se efectuará en el país originador.

B.20 *Cancelación de entrega diferida* TRM

Este elemento de servicio permite que un AU de origen ordene al STRM que cancele un mensaje de entrega diferida depositado con anterioridad. Es posible que la tentativa de cancelación no siempre tenga éxito. Los posibles motivos de fallo son: expiración del plazo de entrega diferida, o que el mensaje ha sido reenviado ya dentro del STRM.

B.21 *Notificación de entrega* TRM PD

Este elemento de servicio permite a un AU de origen solicitar que se le envíe una notificación explícita cuando un mensaje depositado ha sido correctamente entregado a un AU o unidad de acceso de destino. La notificación se relaciona con el mensaje depositado mediante un identificador de mensaje e incluye la fecha y hora de la entrega. En caso de un mensaje con múltiples destinos, el AU de origen puede solicitar este elemento de servicio por cada destinatario.

Cuando un mensaje se entrega después de la expansión de la lista de distribución, entonces, según la pauta de la lista de distribución, la notificación podrá enviarse al propietario de la lista o al originador del mensaje o a ambos.

La notificación de entrega no implica que el AU o el usuario hayan realizado ninguna acción, por ejemplo examinar el contenido del mensaje.

B.22 *Indicación de hora de entrega* TRM PD

Este elemento de servicio permite al STRM indicar a un AU destinatario la fecha y hora en la que el STRM entregó un mensaje. En el caso de entrega física, este elemento de servicio indica la fecha y hora en la que la UAEF asumió la responsabilidad de imprimir y entregar el mensaje físico.

B.23 *Entrega por el servicio burofax* EF PD

Este elemento de servicio permite al usuario de origen ordenar a la UAEF y el SEF asociado que utilicen el servicio burofax para el transporte y la entrega.

B.24 *Designación de destinatarios por el nombre de guía* TRM PD

Este elemento de servicio permite a un AU de origen utilizar un nombre de guía en vez de una dirección O/D de un destinatario individual.

B.25 *Revelación de otros destinatarios* TRM

Este elemento de servicio permite que un AU de origen, al depositar un mensaje con múltiples destinos, ordene al STRM que revele los nombres O/D de todos los demás destinatarios a cada AU destinatario cuando le entregue el mensaje. Los nombres O/D revelados serán los suministrados por el AU de origen. Si se utiliza una expansión de LD, sólo se revelará el nombre de LD especificado por el originador y no los nombres de sus miembros.

B.26 *Indicación de historia de la expansión de la LD* TRM

Este elemento de servicio proporciona a un destinatario, en el momento de la entrega, información sobre la(s) lista(s) de distribución por las cuales llegó el mensaje. Es un asunto local en lo que se refiere a la cantidad de información que se presenta al destinatario.

B.27 *Prohibición de expansión de la LD* TRM

Este elemento de servicio permite al usuario originador especificar que si cualesquiera de los destinatarios puede, directamente o por reasignación, referirse a una lista de distribución, no habrá expansión. En su lugar se devolverá al AU de origen una notificación de no entrega, a menos que se haya solicitado la prevención de notificación de no entrega.

B.28 *SCU (servicio de correo urgente)* EF PD

Este elemento de servicio permite al usuario de origen ordenar al SEF que transporte y entregue el mensaje físico producido a partir del mensaje STM, por medio del servicio acelerado de circulación y entrega de cartas (tal como el SCU o servicio local equivalente) en el país de destino.

B.29 *Indicación de fecha de expiración* MIP

Este elemento de servicio permite al originador indicar al destinatario la fecha y hora después de la cual considera que el mensaje IP no es válido. La finalidad de este elemento de servicio es indicar la evaluación del originador de la aplicabilidad actual de un mensaje IP. No se especifica la acción particular del AU de MIP en nombre de su destinatario, ni la acción del propio destinatario. Posibles acciones pudieran ser archivar o suprimir el mensaje IP después de transcurrida la fecha de expiración.

B.30 *Conversión explícita* TRM PD

Este elemento de servicio permite a un AU originador pedir que el STRM realice una conversión especificada, tal como la requerida cuando hay interfuncionamiento entre diferentes servicios telemáticos. Cuando se entrega un mensaje después que se ha realizado la conversión, se informa al AU destinatario de los tipos de información codificada originales así como los tipos de información codificada actuales del mensaje.

Nota 1 – Este elemento de servicio está destinado a permitir el interfuncionamiento con terminales/servicios telemáticos.

Nota 2 – Cuando se utilizan nombres LD junto con este elemento de servicio, la conversión se aplicará a todos los miembros de la LD.

B.31 *Indicación de mensaje IP reenviado* MIP

Este elemento de servicio permite que se envíe un mensaje IP reenviado, o un mensaje IP reenviado más su «información de entrega», como el cuerpo (o como una de las partes del cuerpo) de un mensaje IP. Junto con la parte del cuerpo se envía una indicación de que se transmite la parte del cuerpo. En un cuerpo de múltiples partes, las partes del cuerpo reenviadas pueden incluirse junto con las partes del cuerpo de otros tipos. La «información de entrega» es la información transportada por el STRM cuando se entrega un mensaje IP (por ejemplo, indicaciones hora de entrega e indicación de conversión). Sin embargo, la inclusión de esta información de entrega junto con un mensaje IP reenviado no garantiza en modo alguno que esta información de entrega sea válida por el STRM.

Los elementos de servicio indicación de petición de notificación recepción e indicación de notificación de no recepción no son afectados por el reenvío de un mensaje IP.

B.32 *Selección de grado de entrega* TRM

Este elemento de servicio permite a un AU de origen solicitar que la transferencia por conducto del STRM se efectúe con carácter *urgente* o *no urgente*, en lugar de *normal*. Los periodos de tiempos definidos para las transferencias urgente y no urgente son respectivamente más corto y más largo que el definido para la transferencia normal. Esta indicación también se envía al destinatario con el mensaje.

B.33 *Retención para entrega* TRM

Este elemento de servicio permite a un AU destinatario solicitar que el STRM retenga sus mensajes y sus notificaciones de retorno para su entrega en un momento posterior. El AU indica al STRM cuándo estará indisponible para aceptar la entrega de mensajes y notificaciones del STRM y también, cuándo volverá a estar disponible para ello. El STRM puede indicar al AU que hay mensajes en espera debido a los criterios que el AU ha establecido para su retención. La responsabilidad de la gestión de este elemento de servicio incumbe al ATM de destino.

Los criterios para solicitar que se retenga la entrega de un mensaje son: el tipo de información codificada, el tipo del contenido, la longitud máxima del contenido y la prioridad. El mensaje será retenido hasta que expire el plazo de entrega máximo para ese mensaje, a menos que el destinatario libere la retención antes de su expiración.

Nota – El elemento de servicio retención para entrega es distinto de la facilidad de almacenamiento de mensajes. El elemento de servicio de retención para entrega proporciona almacenamiento temporal para facilitar la entrega y solamente después de que el mensaje se ha transferido al AU de destinatario, se devuelve la notificación de entrega. La facilidad de almacenamiento de mensajes aumenta el almacenamiento de un AU y puede utilizarse para almacenar mensajes durante un periodo de tiempo ampliado. A diferencia del elemento de servicio retención para entrega, las notificaciones de entrega se devuelven tan pronto como el mensaje se transfiere (es decir, se entrega) al almacén de mensajes.

B.34 *Conversión implícita* TRM

Este elemento de servicio permite que el STRM efectúe para un AU de destino, durante un periodo de tiempo, toda conversión requerida por mensajes antes de entregarlos. Este elemento de servicio no lo solicitan explícitamente ni el AU de origen ni el de destino. Si las capacidades de tipo de información codificada del AU de destino permiten más de un tipo de conversión, se efectúa la más apropiada. Cuando se entrega un mensaje después que se ha realizado la conversión, se indican al AU destinatario los tipos de información codificada original así como los tipos de información codificada actual del mensaje.

B.35 *Indicación de importancia* MIP

Este elemento de servicio permite al originador indicar a los destinatarios su evaluación de la importancia del mensaje IP enviado. Se definen tres niveles de importancia: *poca*, *normal* y *mucha*.

Este elemento de servicio no está relacionado con el elemento de servicio selección de grado de entrega proporcionado por el STRM. No se especifica la acción particular realizada por el destinatario o por su AU de MIP basada en la categorización de importancia. La finalidad es permitir al AU de MIP destinatario, por ejemplo, presentar mensajes IP por orden de importancia o alertar al destinatario sobre la llegada de mensajes IP de mucha importancia.

B.36 *Indicación de copia incompleta* MIP

Este elemento de servicio permite al originador indicar que este mensaje IP es una copia incompleta de un mensaje IP con la misma identificación de mensaje IP, y que esa parte o esas partes del cuerpo y/o campos de encabezamiento del mensaje IP original están ausentes.

B.37 *Identificación del mensaje IP* MIP

Este elemento de servicio permite a los AU de MIP cooperantes transmitir un identificador globalmente único para cada mensaje IP enviado o recibido. El identificador de mensaje IP está compuesto de un nombre O/D del originador y un identificador que es único respecto a dicho nombre. Los AU de MIP y los usuarios utilizan este identificador para hacer referencia a mensajes IP previamente enviados o recibidos (por ejemplo, en notificaciones de recepción).

B.38 *Indicación de idioma* MIP

Este elemento de servicio permite a un AU de origen indicar el tipo o tipos de idioma de un mensaje IP depositado.

B.39 *Designación de la última entrega* TRM

Este elemento de servicio permite a un AU de origen especificar el último plazo para la entrega del mensaje. Si el STRM no puede efectuar la entrega en el plazo especificado, el mensaje no se entrega y se cancelará. En el caso de los mensajes con múltiples destinatarios, el último plazo de entrega puede expirar antes de que se haya efectuado la entrega a todos los destinatarios, pero ello no anulará ninguna entrega que haya tenido lugar.

B.40 *Confidencialidad del flujo del mensaje* TRM

Este elemento de servicio permite al originador del mensaje proteger la información que podría derivarse de la observación del flujo del mensaje.

Nota – Sólo se admite una forma limitada de este elemento de servicio.

B.41 *Identificación de mensajes* TRM

Este elemento de servicio permite al STRM proporcionar a un AU un identificador único para cada mensaje depositado en el STRM, o entregado por éste. Los AU y el STRM utilizan este identificador para hacer referencia a un mensaje previamente depositado en relación con elementos de servicio tales como notificación de entrega y no entrega.

B.42 *Autenticación del origen del mensaje* TRM PD

Este elemento de servicio permite al originador de un mensaje proporcionar al (a los) depositario(s) del mensaje y a cualquier ATM a través del cual el mensaje sea transferido, un medio de autentificar el origen del mensaje (por ejemplo, una firma). La autenticación del origen del mensaje puede proporcionarse, o bien al (a los) destinatario(s) del mensaje y a cualquier ATM a través del cual el mensaje se ha transferido, mensaje por mensaje, utilizando una técnica de cifrado asimétrica, o bien únicamente al (a los) destinatario(s) del mensaje, destinatario por destinatario, utilizando una técnica asimétrica, o una técnica simétrica de cifrado.

B.43 *Etiquetado de seguridad del mensaje* TRM

Este elemento de servicio permite al originador de un mensaje (o sonda) asociar al mensaje (y a cualquier informe sobre el mensaje o sonda) una indicación de la sensibilidad del mensaje (una etiqueta de seguridad). La etiqueta de seguridad del mensaje puede ser utilizada por el STRM y el (los) destinatario(s) del mensaje para determinar el tratamiento del mensaje de acuerdo con la política de seguridad en vigor.

B.44 *Integridad de la secuencia de mensajes* TRM PD

Este elemento de servicio permite al originador del mensaje proporcionar al destinatario del mensaje un medio de verificar que se ha conservado la secuencia de mensajes del originador al destinatario (sin pérdida, cambio del orden o repetición de mensajes). La integridad de la secuencia de mensajes se entiende destinatario por destinatario, y para lograrla puede utilizarse una técnica de cifrado simétrica o asimétrica.

B.45 *Entrega a múltiples destinos* TRM PD

Este elemento de servicio permite a un AU de origen especificar que el mensaje que deposita se entregue a más de un AU destinatario. Este elemento de servicio no implica la entrega simultánea a todos los AU especificados.

B.46 *Cuerpo de múltiples partes* MIP

Este elemento de servicio permite al originador enviar a un destinatario o destinatarios un mensaje IP con un cuerpo que está dividido en varias partes. La naturaleza y atributos, o el tipo, de cada parte del cuerpo se transmiten junto con la parte del cuerpo.

B.47 *Notificación de no entrega* TRM PD

Este elemento de servicio permite al STRM notificar a un AU de origen que un mensaje no fue entregado al AU o a los AU destinatarios especificados. El motivo por el cual no se entregó el mensaje se incluye como parte de la notificación. Por ejemplo, el AU de destino puede ser desconocido para el STRM.

En el caso de un mensaje multidestino, una notificación de no entrega puede referirse a cualquiera o a todos los AU destinatarios a los cuales el mensaje no puede entregarse.

Cuando un mensaje no es entregado después de la expansión de la lista de distribución, entonces, según la pauta de la lista de distribución, la notificación puede ser enviada al propietario de la lista, al originador del mensaje o a ambos.

B.48 *Indicación de petición de notificación de no recepción* MIP PD

Este elemento de servicio permite al originador pedir que se le notifique cuando se estima que el mensaje IP no puede ser recibido. En el caso de un mensaje IP con múltiples destinatarios, el originador puede solicitar este elemento de servicio destinatario por destinatario.

El AU de origen transmite esta petición al AU de destino. El AU de destino produce automáticamente una notificación de no recepción cuando tiene lugar cualquiera de los sucesos siguientes:

1) El AU del destinatario reenvía automáticamente el mensaje IP a otro usuario.
2) El AU del destinatario descarta el mensaje IP antes de la recepción.
3) El abono del destinatario se ha terminado antes de que pueda recibir el mensaje IP.

Dado que la recepción puede producirse cuando haya transcurrido un periodo de longitud arbitraria desde la entrega, el hecho de que el destinatario no tome conocimiento del mensaje IP, incluso durante un periodo de tiempo prolongado (por ejemplo, durante un largo viaje de negocios) no constituye una no recepción y, en consecuencia, no se emite una notificación.

Nota – No se puede asignar ningún valor jurídico a este elemento de servicio.

B.49 *No rechazo de la entrega* TRM PD

Este elemento de servicio permite al originador del mensaje obtener del (de los) destinatario(s) del mensaje la prueba irrefutable de que el mensaje fue entregado al (a los) destinatario(s). Esto ofrecerá protección contra cualquier tentativa ulterior, por parte del (de los) destinatario(s) de negar haber recibido el mensaje o su contenido. El no rechazo de la entrega se ofrece al originador de un mensaje por cada destinatario, mediante técnicas de cifrado asimétricas.

B.50 *No rechazo del origen* TRM PD

Este elemento de servicio permite al originador del mensaje proporcionar al (a los) destinatario(s) del mensaje una prueba irrefutable del origen del mensaje. Esto ofrecerá protección contra cualquier tentativa ulterior, por parte del originador de anular el mensaje o su contenido. El no rechazo del origen se proporciona al (a los) destinatario(s) de un mensaje, mensaje por mensaje, mediante técnicas de cifrado asimétricas.

B.51 *No rechazo del depósito* TRM

Este elemento de servicio permite al originador del mensaje obtener una prueba irrefutable de que el mensaje fue depositado en el STRM para ser entregado al (a los) destinatario(s) especificados inicialmente. Esto ofrecerá protección contra cualquier tentativa ulterior, por parte del STRM, de negar haber recibido el mensaje para su entrega al (a los) destinatario(s) especificado(s) inicialmente. El no rechazo del depósito se proporciona al originador de un mensaje, mensaje por mensaje, mediante técnicas de cifrado asimétricas.

B.52 *Indicación de obsolescencia* MIP

Este elemento de servicio permite al originador indicar que uno o más mensajes IP que envió anteriormente son obsoletos. El mensaje IP que transmite esta indicación sustituye al mensaje IP obsoleto.

La acción que debe realizar el destinatario o su AU de MIP es un asunto de carácter local. Sin embargo, la finalidad es, por ejemplo, permitir al AU de MIP o al destinatario suprimir o archivar mensajes IP obsoletos.

B.53 *Correo ordinario* EF PD

Este elemento de servicio permite al SEF transportar y entregar la carta producida por un mensaje STM en el modo disponible mediante el servicio postal de cartas ordinarias en el país de destino. Esta es la acción por defecto para el transporte y entrega de un mensaje físico.

B.54 *Indicación de los tipos de información codificada originales* TRM

Este elemento de servicio permite a un AU originador especificar al STRM los tipos de información codificada de un mensaje depositado. Cuando se entrega el mensaje también se indican al AU destinatario los tipos de información codificada del mensaje especificados por el AU originador.

B.55 *Indicación de originador* MIP

Este elemento de servicio permite transmitir la identidad del originador al destinatario. La finalidad de este elemento de servicio MIP es identificar al originador de una manera cómoda para el usuario. En cambio, el STRM proporciona al destinatario la dirección O/D y el nombre de guía (si lo hay) autenticados del originador. Los nombres LD no se utilizarán en la indicación de originador.

B.56 *Destinatario alternativo solicitado por el originador* TRM PD

Este elemento de servicio permite a un AU de origen especificar, para cada destinatario deseado, un destinatario alternativo al que el STRM puede entregar el mensaje, en caso de no poder entregarlo a aquél. El destinatario alternativo puede ser una lista de distribución. A efectos de determinar el éxito o el fracaso (y, por tanto, las notificaciones de entrega y no entrega), la entrega al destinatario alternativo solicitado por el originador es equivalente a la entrega al destinatario deseado. Si el destinatario deseado ha solicitado el redireccionamiento de los mensajes entrantes, y si el AU de origen ha solicitado redireccionamiento autorizado por el originador, el sistema tratará primero de redireccionar el mensaje. Si no lo logra, el sistema intentará entregar el mensaje al destinatario alternativo designado.

B.57 *Notificación de entrega física por STM* EF PD

Este elemento de servicio permite al usuario de origen solicitar al STM que genere y devuelva una notificación explícita que informe al originador sobre el éxito o el fracaso de la entrega de un mensaje físico. La notificación proporciona información sobre la entrega, pero el SEF no proporciona ningún registro físico.

Nota 1 – La notificación incluye la fecha y hora de la entrega, basándose en la confirmación de entrega proporcionada por la persona que efectúa la entrega, el destinatario u otra persona autorizada. Esto está sujeto a la reglamentación nacional del país de destino y también depende del tipo de entrega solicitada (por ejemplo en el caso de correo certificado al destinatario en persona, el propio destinatario será la persona que efectúe la confirmación).

Nota 2 – Esta notificación no implica que el destinatario haya realizado una acción cualquiera (como el examen del contenido del mensaje).

Nota 3 – Cuando se solicita este elemento de servicio, y el mensaje físico no puede ser entregado, será devuelto o destruido según las disposiciones reglamentarias nacionales del país de destino, lo que significa que la acción por defecto del elemento de servicio B.91 queda anulada.

B.58 *Notificación de entrega física por el SEF* EF PD

Este elemento de servicio permite a un usuario de origen solicitar al SEF que genere y devuelva una notificación explícita que le informe del éxito o fracaso de la entrega del mensaje físico. La notificación sirve como dato de entrega, que el usuario de origen puede conservar como referencia.

Nota 1 – La notificación incluye la fecha y hora de la entrega, y en el caso de entrega correcta, la firma de la persona que confirma la entrega. La persona que confirma puede ser la persona a que se hace la entrega, el propio destinatario, u otra persona autorizada. Esto está sujeto a la reglamentación nacional del país de destino y también depende del tipo de entrega solicitada (por ejemplo en el caso de correo certificado al destinatario en persona, el propio destinatario será la persona que confirme).

Nota 2 – Esta notificación no implica que el destinatario haya realizado una acción cualquiera (como el examen del contenido del mensaje).

Nota 3 – Cuando se solicita este elemento de servicio, y el mensaje físico no puede ser entregado, será devuelto o destruido según las disposiciones reglamentarias nacionales del país de destino, lo que significa que la acción por defecto del elemento de servicio B.91 queda anulada.

B.59 *Autorización de reenvío físico* EF PD

Este elemento de servicio permite al SEF reenviar el mensaje físico a una dirección de reenvío si el destinatario ha cambiado de dirección y ha indicado esto al SEF. Esta es la acción por defecto que ejecuta el SEF.

B.60 *Prohibición de reenvío físico* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que no reenvíe el mensaje físico a la dirección de reenvío.

B.61 *Prevención de notificación de no entrega* TRM PD

Este elemento de servicio permite a un AU de origen ordenar al STRM que no devuelva una notificación de no entrega al AU de origen si estima que el mensaje que se deposita es inentregable. En el caso de mensajes con múltiples destinos, el AU de origen puede solicitar este elemento de servicio para cada destinatario.

B.62 *Indicación de destinatarios primarios y de copias* MIP

Este elemento de servicio permite al originador proporcionar los nombres del o de los usuarios o LD que son los destinatarios primarios deseados del mensaje IP, y los nombres de los cero o más usuarios o LD que son los destinatarios deseados de copias de mensaje IP. La finalidad es permitir que el destinatario determine la categoría en que se ha colocado a cada uno de los destinatarios especificados (incluido el propio destinatario). La distinción exacta entre estas dos categorías de destinatarios no se ha especificado. Sin embargo, podría suponerse, por ejemplo, que los destinatarios primarios han de realizar una acción relacionada con el mensaje IP, mientras que los destinatarios de copias reciben el mensaje IP solamente para información.

Nota – Como ejemplo de este elemento de servicio, en un memorándum típico, los destinatarios primarios se designan normalmente por la instrucción «a» mientras que «cc:» identifica a los destinatarios de copias.

B.63 *Sonda* TRM

Este elemento de servicio permite a un AU averiguar si un mensaje determinado podrá entregarse, antes de depositarlo efectivamente. El STRM proporciona la información de depósito y genera notificaciones de entrega y/o no entrega para indicar si podrá entregarse un mensaje con la misma información de depósito a los AU destinatarios especificados.

El elemento de servicio sonda comprende la facultad de comprobar si el tamaño tipo de contenido y/o los tipos de información codificada del mensaje harían imposible su entrega. La significación del resultado de una sonda depende de que el AU o los AU destinatarios hayan registrado en el STRM los tipos de información codificada, el tipo de contenido y el tamaño de mensaje máximo que pueden aceptar. Este elemento de servicio está sujeto a los mismos objetivos de plazo de entrega que la clase urgente. En el caso de las LD, una sonda no indica nada sobre la posibilidad de entrega satisfactoria a los miembros de la LD, sino solamente si el originador tiene derecho a entregar a la LD.

B.64 *Autenticación del origen de la sonda* TRM

Este elemento de servicio permite al originador de una sonda proporcionar, a cualquier ATM por el que se transfiere la sonda, un medio de autenticar el origen de la sonda (es decir una firma). La autenticación del origen de la sonda se hace sonda por sonda, mediante una técnica de cifrado asimétrica.

B.65 *Prueba de la entrega* TRM PD

Este elemento de servicio permite al originador de un mensaje obtener del (de los) destinatario(s) del mensaje el medio de autenticar la identidad del (de los) destinatario(s), así como del mensaje entregado y su contenido. La autenticación de los destinatarios del mensaje se proporciona al originador de un mensaje, para cada destinatario, mediante técnicas de cifrado simétricas o asimétricas.

B.66 *Prueba del depósito* TRM

Este elemento de servicio permite al originador de un mensaje obtener del STRM el medio de autenticar que el mensaje fue depositado para su entrega al destinatario deseado inicialmente. La autenticación del depósito del mensaje se proporciona mensaje por mensaje, mediante técnicas de cifrado simétricas o asimétricas.

B.67 *Indicación de petición de notificación de recepción* MIP PD

Este elemento de servicio permite al originador pedir que se le notifique la recepción del mensaje IP que se envía. En el caso de un mensaje con múltiples destinatarios, el originador puede solicitar este elemento de servicio destinatario por destinatario. Este elemento de servicio también invoca implícitamente la indicación de petición de notificación de no recepción.

El AU de origen transmite su petición al AU de destino. El destinatario puede ordenar a su AU que satisfaga esas peticiones, ya sea automáticamente (por ejemplo, cuando presenta por primera vez el mensaje IP en el terminal del destinatario), o en cumplimiento de su orden explícita. El destinatario también puede ordenar a su AU que, de manera general o caso por caso, haga caso omiso de esas peticiones.

B.68 *Redireccionamiento desautorizado por el originador* TRM

Este elemento de servicio permite a un AU de origen ordenar al STRM, si el destinatario ha solicitado el elemento de servicio redireccionamiento de mensajes entrantes, que el redireccionamiento no se aplique a un determinado mensaje depositado.

B.69 *Redireccionamiento de mensajes entrantes* TRM

Este elemento de servicio permite a un AU ordenar al STRM que dirija los mensajes entrantes que llevan su dirección a otro AU o a una LD durante un periodo de tiempo especificado, o hasta que sea revocado.

Nota 1 – Este es un servicio STRM que no precisa la entrega al destinatario deseado antes de que pueda tener lugar el redireccionamiento. En consecuencia, es diferente del elemento de servicio indicación de MIP reenviado automáticamente.

Nota 2 – Cuando están aplicando medidas de seguridad, en función de las etiquetas de seguridad, mensajes entrantes diferentes podrán ser redireccionados a distintos destinatarios alternativos, o no ser redireccionados en absoluto.

B.70 *Correo certificado* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que trate el mensaje físico como correo certificado.

B.71 *Correo certificado para el destinatario en persona* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que trate el mensaje físico como correo certificado, y que lo entregue únicamente al propio destinatario.

B.72 *Indicación de petición de respuesta* MIP PD

Este elemento de servicio permite al originador pedir que el destinatario envíe un mensaje IP en respuesta al mensaje IP que contiene la petición. El originador puede especificar también hasta qué fecha deberá enviarse la respuesta, y el usuario o usuarios y LD a los cuales el originador solicita (pero no exige) que estén entre los destinatarios preferidos de cualquier respuesta. El destinatario es informado de la fecha y nombres, pero le corresponde decidir si responde o no, y a quién.

Nota – Un destinatario de copia ciega deberá considerar cuidadosamente a quién envía una respuesta, a fin de que se conserve el significado del elemento de servicio indicación de destinatario de copia ciega.

B.73 *Indicación de mensaje IP de respuesta* MIP

Este elemento de servicio permite al originador de un mensaje IP indicar el (a los) destinatario(s) que este mensaje IP se envía como respuesta a otro mensaje IP. Según los deseos del originador del mensaje al que se responde, una respuesta, y la decisión final del originador de la respuesta, pueden ser enviadas:

1) a los destinatarios especificados en la indicación de petición de respuesta del mensaje al que se responde;
2) al originador del mensaje al que se responde;
3) al originador y a otros destinatarios;
4) a una lista de distribución, de la que el originador del mensaje al que se responde puede ser un miembro receptor;
5) a otros destinatarios, elegidos por el originador de la respuesta.

Los destinatarios de la respuesta la reciben como mensaje IP ordinario, junto con una indicación del mensaje IP al que se está respondiendo.

B.74 *Autenticación de origen del informe* TRM

Este elemento de servicio permite al originador de un mensaje (o sonda) autenticar el origen de un informe sobre la entrega o no entrega del mensaje (o sonda) de asunto (una firma). La autenticación del origen del informe se hace informe por informe, mediante una técnica de cifrado asimétrica.

B.75 *Petición de dirección reenviante* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que proporcione la dirección reenviante, si el destinatario cambió su dirección y lo indicó al SEF.

Este elemento de servicio puede utilizarse con el elemento de servicio autorización de reenvío físico o prohibición de reenvío físico. El suministro de la dirección reenviante por el SEF a un usuario de origen está sujeto a la reglamentación nacional del país de destino. La acción por defecto es el no suministro de la dirección reenviante.

B.76 *Método de entrega solicitado* TRM PD

Este elemento de servicio permite al usuario solicitar para cada destinatario, el método o métodos de entrega preferidos (por ejemplo, mediante una unidad de acceso). Si el método de entrega preferido no puede proporcionarse, no hay entrega.

B.77 *Entrega restringida* TRM

Este elemento de servicio permite a un AU de destino indicar al STRM que no está preparado para recibir mensajes de ciertos AU o LD de origen.

Nota 1 – Este elemento de servicio puede solicitarse de una de dos maneras:

a) Especificación por el AU de destino de los originadores no autorizados; todos los demás originadores se consideran autorizados.
b) Especificación por el AU de destino de los originadores autorizados; todos los demás originadores se consideran no autorizados.

Nota 2 – El servicio abstracto STRM especificado en la Recomendación X.411 no proporciona una realización técnica de este elemento de servicio. El que se proporcione puede ser objeto de una futura normalización.

B.78 *Devolución de contenido* TRM

Este elemento de servicio permite a un AU de origen pedir que el contenido de un mensaje depositado se devuelva con cualquier notificación de no entrega. Sin embargo, esto no se realizará si se ha efectuado cualquier conversión del tipo de información codificada en el contenido del mensaje.

B.79 *Gestión de acceso seguro* TRM

Este elemento de servicio permite a un usuario STRM establecer una asociación con el STRM, o al STRM establecer una asociación con un usuario STRM, o a un ATM establecer una asociación con otro ATM. También establece las credenciales fuertes de los objetos para que interactúen, así como el contexto, y el contexto de seguridad, de la asociación. La gestión de acceso seguro puede utilizar técnicas de cifrado simétricas o asimétricas. Cuando la seguridad de acceso se logra por medio de credenciales fuertes, éstas pueden actualizarse periódicamente.

B.80 *Indicación de sensibilidad* MIP

Este elemento de servicio permite al originador de un mensaje IP especificar directrices sobre el grado de seguridad del mensaje IP con relación a su recepción. La finalidad es que la indicación de sensibilidad controle puntos como los siguientes:

1) si el destinatario debe acreditar su identidad para recibir el mensaje IP;
2) si debe permitirse o no que el mensaje IP se imprima en una impresora compartida;
3) si el AU de MIP debe permitir o no al destinatario que reenvíe el mensaje IP recibido;
4) si debe autorizarse o no que el mensaje IP se reenvíe automáticamente.

La indicación de sensibilidad puede comunicarse al destinatario o ser interpretada directamente por su AU de MIP.

Si no se indica ningún nivel de sensibilidad, debe suponerse que el originador del mensaje IP no ha previsto ninguna restricción sobre la disposición ulterior del mensaje IP por parte del destinatario, y éste queda en libertad de reenviarlo, imprimirlo o proceder como estime conveniente.

Se definen tres niveles específicos de sensibilidad por encima del nivel por defecto:

- *Personal:* El mensaje IP se envía al destinatario como individuo, sin atender a su función. Sin embargo, ello no implica que el mensaje IP sea privado.
- *Privado:* El mensaje IP contiene información que sólo puede ser vista (u oída) por el destinatario, exclusivamente. El AU de MIP del destinatario puede proporcionar servicios para asegurar el cumplimiento de esta condición en nombre del originador del mensaje IP.
- *Confidencial para la compañía:* El mensaje IP contiene información que debe ser tratada de acuerdo con los procedimientos específicos de la compañía.

B.81 *Entrega especial* EF PD

Este elemento de servicio permite a un usuario de origen ordenar al SEF que transporte la carta producida a partir del mensaje STM mediante el sistema de circulación de la correspondencia ordinaria y que la entregue por un mensajero especial.

B.82 *Alerta de mensaje almacenado* MM

Este elemento de servicio permite al usuario de una MM registrar conjuntos importantes de criterios que pueden provocar el envío al usuario de una alerta, cuando llega a la MM un mensaje que satisface los criterios seleccionados. La generación de alerta puede efectuarse como sigue:

1) Si el AU está conectado «en línea» con la MM, el mensaje de alerta será enviado al AU en cuanto un mensaje que satisfaga los criterios registrados para la generación de alertas llegue a la MM. Si el AU está conectado «fuera de línea», entonces, la próxima vez que el AU se conecte a su MM después de llegar a la MM un mensaje que satisfaga los criterios registrados, el usuario será informado de que hay uno o más casos de alerta, cuyos detalles pueden precisarse mediante un resumen de mensajes almacenados.
2) Además, o como alternativa al N.º 1, la MM puede utilizar otros mecanismos para informar al usuario.

B.83 *Reenvío automático de mensajes almacenados* MM

Este elemento de servicio permite a un usuario de una MM registrar peticiones de que la MM reenvíe automáticamente mensajes seleccionados que le sean entregados. El usuario de la MM puede seleccionar, registrándolos, varios conjuntos de criterios elegidos entre los atributos disponibles en la MM, y los mensajes que satisfagan cada conjunto de criterios serán automáticamente reenviados a uno o más usuarios o LD. También se puede especificar la inclusión de un texto por criterio de selección con cada mensaje reenviado automáticamente.

B.84 *Supresión de mensajes almacenados* MM

Este elemento de servicio permite a un AU de destino suprimir algunos de sus mensajes en la MM. Los mensajes no pueden suprimirse si no han sido previamente listados.

B.85 *Captura de mensajes almacenados* MM

Este elemento de servicio permite a un AU de destino extraer de la MM algunos de sus mensajes, o porciones de un mensaje. El AU puede capturar un mensaje (o porciones de un mensaje) basándose en los mismos criterios de búsqueda que se pueden emplear para el listado de mensajes almacenados.

B.86 *Listado de mensajes almacenados* MM

Este elemento de servicio proporciona a un AU de destino una lista de información sobre algunos de sus mensajes almacenados en la MM. La información comprende los atributos del sobre y del contenido de un mensaje, y otros añadidos por la MM. El AU puede limitar el número de mensajes que se incluirán en la lista.

B.87 *Resumen de mensajes almacenados* MM

Este elemento de servicio proporciona a un AU de destino un cómputo del número de mensajes que satisfacen criterios especificados fundados en uno o más atributos de los mensajes almacenados en la MM.

B.88 *Indicación de asunto* MIP

Este elemento de servicio permite al originador indicar al destinatario o destinatarios el asunto del mensaje IP enviado. La información de asunto debe suministrarse al destinatario.

B.89 *Indicación de hora de depósito* TRM

Este elemento de servicio permite al STRM indicar a un AU de origen y al AU de destino la fecha y hora en que se depositó un mensaje en el STRM. En el caso de la entrega física, este elemento de servicio también permite al UAEF indicar la fecha y la hora de depósito del mensaje físico.

B.90 *Cuerpo tipificado* MIP

Este elemento de servicio permite que se transmitan la naturaleza y atributos del cuerpo del mensaje IP junto con el cuerpo. Debido a que el cuerpo puede sufrir conversiones, el tipo de cuerpo puede cambiar a lo largo del tiempo.

B.91 *Correo inentregable con devolución del mensaje físico* EF PD

Este elemento de servicio permite al SEF devolver el mensaje físico sin demora, con una indicación de motivo para el originador, si no puede ser entregado al destinatario. Esta es la acción por defecto que debe realizar el SEF.

Nota – En el caso de entrega por lista de correos, la devolución del mensaje físico se efectuará después de un cierto periodo de tiempo.

B.92 *Utilización de lista de distribución* TRM PD

Este elemento de servicio permite a un AU de origen especificar una lista de distribución en lugar de todos los destinatarios individuales (usuarios o LD anidadas) mencionados en ella. Los STRM añadirán los miembros de la lista a los destinatarios del mensaje y los enviarán a dichos miembros. Unas listas de distribución pueden ser miembros de otras listas de distribución, en cuyo caso la lista de destinatarios puede ser sucesivamente ampliada en diversos lugares, en el STRM.

B.93 *Registro de capacidades de usuario/AU* TRM

Este elemento de servicio permite a un AU indicar a su ATM, mediante su registro, cualquiera de las siguientes capacidades, o todas ellas, sin restricción, con respecto a la recepción de mensajes:

1) el o los tipos de contenido de los mensajes que está dispuesto a recibir;
2) la longitud máxima del contenido de los mensajes que está dispuesto a recibir;
3) el o los tipos de información codificada de los mensajes que está dispuesto a recibir.

El ATM no entregará a un AU un mensaje que no corresponda a las capacidades registradas, o que las rebase.

ANEXO C

(a la Recomendación X.400)

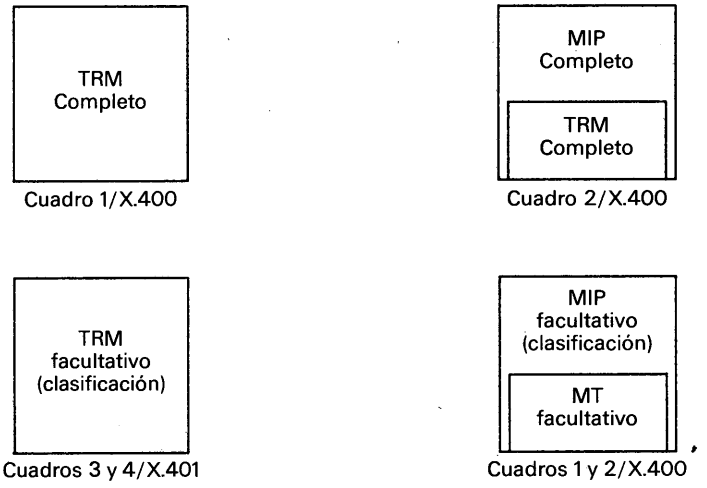
Cambio de los elementos de servicio a partir de 1984

C.1 *Nuevos elementos de servicio en 1988* (Véase el cuadro C-1/X.400.)

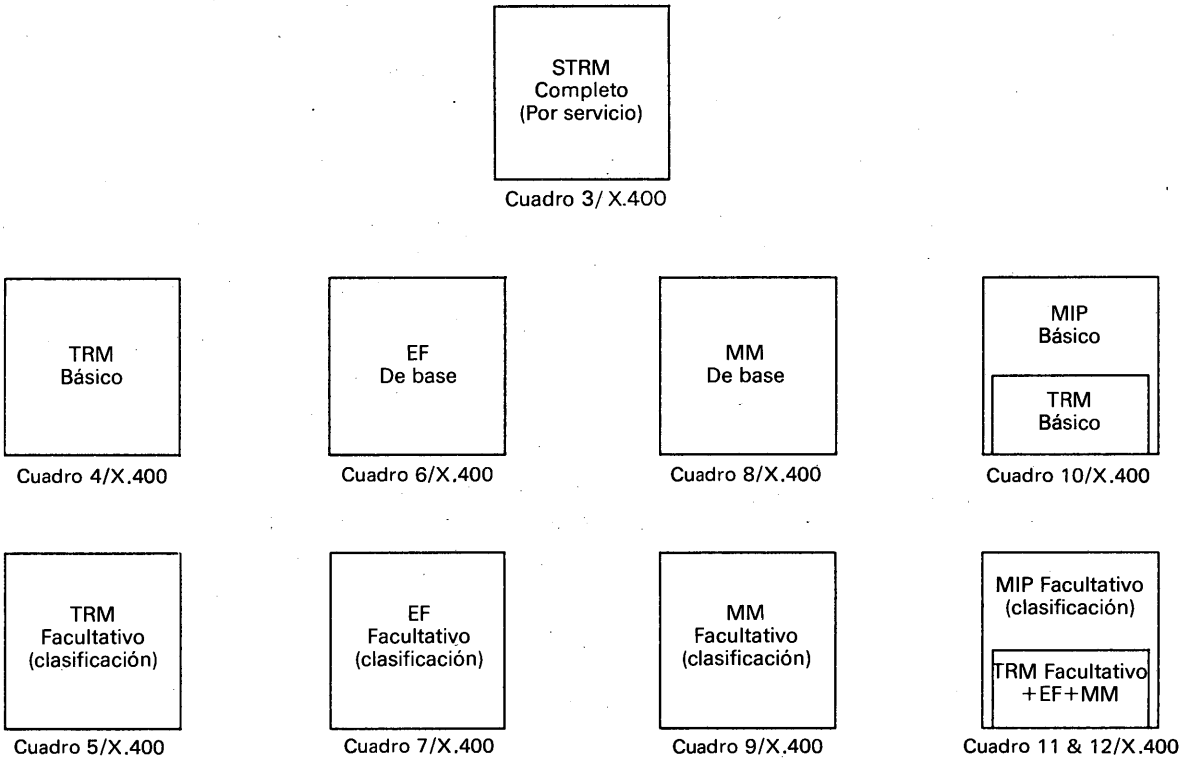
CUADRO C-1/X.400

Elementos de servicio	TRM	MIP	EF	MM	Referencias del anexo B
Reproducción física adicional			X		B.2
Reproducción física básica			X		B.7
Confidencialidad del contenido	X				B.10
Integridad del contenido	X				B.11
Prohibición de conversión en caso de pérdida de información	X				B.14
Recogida en ventanilla			X		B.16
Recogida en ventanilla con aviso			X		B.17
Entrega a través del servicio burofax			X		B.23
Designación de destinatario por nombre de guía	X				B.24
Indicación de historia de la expansión de la LD	X				B.26
Prohibición de expansión de la LD	X				B.27
SCU (servicio correo urgente)			X		B.28
Indicación de copia incompleta		X			B.36
Indicación de idioma		X			B.38
Designación de última entrega	X				B.39
Confidencialidad del flujo de mensajes	X				B.40
Autenticación del origen del mensaje	X				B.42
Etiquetado de seguridad del mensaje	X				B.43
Integridad de la secuencia de mensajes	X				B.44
No rechazo de la entrega	X				B.49
No rechazo del origen	X				B.50
No rechazo del depósito	X				B.51
Correo ordinario			X		B.53
Destinatario alternativo solicitado por el originador	X				B.56
Notificación de entrega física por el STM			X		B.57
Notificación de entrega física por el SEF			X		B.58
Reenvío físico permitido			X		B.59
Reenvío físico prohibido			X		B.60
Autenticación del origen de la sonda	X				B.64
Prueba de entrega	X				B.65
Prueba de depósito	X				B.66
Redireccionamiento desautorizado por el originador	X				B.68
Redireccionamiento de mensajes entrantes	X				B.69
Correo certificado			X		B.70
Correo certificado al destinatario en persona			X		B.71
Autenticación del origen del informe	X				B.74
Solicitud de dirección reenviante			X		B.75
Método de entrega solicitado	X				B.76
Entrega restringida	X				B.77
Gestión de acceso seguro	X				B.79
Entrega especial			X		B.81
Alerta de mensaje almacenado				X	B.82
Reenvío automático de mensaje almacenado				X	B.83
Supresión de mensaje almacenado				X	B.84
Captura de mensaje almacenado				X	B.85
Listado de mensajes almacenados				X	B.86
Resumen de mensajes almacenados				X	B.87
Correo no entregable con devolución del mensaje físico			X		B.91
Utilización de lista de distribución	X				B.92
Registro de capacidades del usuario/AU	X				B.93

C.2 *Correspondencia entre los cuadros relativos a los elementos de servicio en las versiones de 1984 y 1988 del Libro del CCITT* (Véase la figura C-1/X.400.)



a) Edición de 1984 del Libro Rojo



b) Edición de 1988 del Libro Azul (X.400)

FIGURA C-1/X.400

Correspondencia entre los cuadros relativos a los elementos de servicio

C.3 *Clasificación de los nuevos elementos de servicio*

Los nuevos elementos de servicio que se añadieron a las Recomendaciones de la serie X.400 de 1984 para crear las Recomendaciones de la serie X.400/F.400 de 1988 se clasifican, todos ellos, como facilidades facultativas de usuario adicionales, con las siguientes excepciones:

C.3.1 *Servicio TRM*

- indicación de historia de la expansión de la LD;
- método de entrega solicitado.

C.3.2 *Servicio MIP*

- indicación de historia de la expansión de la LD;
- indicación de idioma;
- método de entrega solicitado.

C.3.3 *Intercomunicación entre los servicios TM/EF*

Si bien algunos de los elementos de servicio utilizados en esta intercomunicación se clasifican como *de base* (véase la Recomendación X.400, § 19.4), y algunos se clasifican como facilidades facultativas de usuario esenciales (véase la Recomendación X.400, § 19.5), la provisión de la intercomunicación de los servicios TM/EF es en sí misma facultativa. Cuando se proporciona esta intercomunicación, los elementos de servicio de base y las facilidades facultativas de usuario deben ser admitidas tal como se clasifican en esta Recomendación.

C.3.4 *Memoria de mensajes*

Si bien algunos de los elementos de servicio utilizados con el almacén de mensajes se clasifican como *de base* (véase la Recomendación X.400, § 19.6), y otros se clasifican como facilidades facultativas de usuario esenciales (véase la Recomendación X.400, § 19.7), la provisión de una memoria de mensajes es en sí misma facultativa y por lo tanto las clasificaciones son únicamente aplicables al proveedor de un almacén de mensajes.

C.4 *Cambios en la clasificación de los elementos de servicio de 1984*

Todos los elementos de servicio de la versión de 1984 han conservado su clasificación con la siguiente excepción:

- petición de notificación de no recepción.

C.4.1 *Cambios diversos*

El elemento de servicio que en 1984 se denominaba tipos de información codificada registrada se conoce ahora como registro de capacidades de usuario, y se ha ampliado en su funcionalidad.

Para facilitar la lectura, se ha revisado la redacción de algunas de las definiciones de elementos de servicio de 1984.

ANEXO D

(a la Recomendación X.400)

Diferencias entre la Recomendación X.400 del CCITT y la norma de ISO 10021-1

(Este anexo no forma parte de la Recomendación)

Este anexo señala las principales diferencias que existen entre esta Recomendación y la norma internacional correspondiente de la ISO. Dado que, en muchos casos, las diferencias conciernen a la inclusión o exclusión de una palabra, oración o frase, y a que éstas ocurren en muchos sitios a todo lo largo del texto, este anexo no señala específicamente estos puntos. Más bien resume lo esencial de estas diferencias.

Las diferencias principales son las siguientes:

1) A lo largo del texto, el CCITT hace referencia a los servicios del CCITT y a su relación con el STM.
2) La figura 5/X.400 que muestra las relaciones entre los dominios de gestión y las notas correspondientes.
3) Los papeles desempeñados por el DGAD y el DGPR en la denominación.
4) La utilización del STM en la prestación de servicios públicos (§ 17).
5) En el texto de la ISO no figura la nota sobre la responsabilidad del almacenamiento de mensajes con entrega diferida (véase el § B.19 del anexo B).

Recomendación X.402

SISTEMAS DE TRATAMIENTO DE MENSAJES: ARQUITECTURA GLOBAL [1]

(Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión de mensajes controlados por computadores, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de los sistemas de tratamiento de mensajes;

(b) la necesidad de almacenar y transferir mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT;

(e) que las Recomendaciones de la serie X.500 definen los sistemas de guía;

(f) que los sistemas de tratamiento de mensajes se definen en la serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419;

(g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

(1) que los modelos abstractos de un sistema de tratamiento de mensajes se definen en la sección 2;

(2) que las configuraciones de un sistema de tratamiento de mensajes se definen en la sección 3;

(3) que la denominación, el direccionamiento y el encaminamiento en los sistemas de tratamiento de mensajes se definen en la sección 4;

(4) que el uso de la guía por los sistemas de tratamiento de mensajes se define en la sección 5;

(5) que la realización ISA de un sistema de tratamiento de mensajes se especifica en la sección 6.

---

[1] La Recomendación X.402 y la Norma ISO 10021-2 [Information Processing Systems – Text Communication – MOTIS – Overall Architecture] se elaboraron en estrecha colaboración y están técnicamente armonizadas, con excepción de las diferencias señaladas en el anexo F.

ÍNDICE

SECCIÓN 1 – *Introducción*

0 *Introducción*

1 *Objeto*

2 *Referencias*

- 2.1 Interconexión de sistemas abiertos
- 2.2 Sistemas de guía
- 2.3 Sistemas de tratamiento de mensajes

3 *Definiciones*

- 3.1 Interconexión de sistemas abiertos
- 3.2 Sistemas de guía
- 3.3 Sistemas de tratamiento de mensajes

4 *Abreviaturas*

5 *Convenios*

- 5.1 NSA.1
- 5.2 Grado
- 5.3 Términos

SECCIÓN 2 – *Modelos abstractos*

6 *Visión de conjunto*

7 *Modelo funcional*

- 7.1 Objetos funcionales primarios
- 7.2 Objetos funcionales secundarios
- 7.3 Objetos funcionales terciarios
- 7.4 Tipos de UA seleccionados

8 *Modelo de información*

- 8.1 Mensajes
- 8.2 Sondas
- 8.3 Informes

9 *Modelo operacional*

- 9.1 Transmisión
- 9.2 Funciones de la transmisión
- 9.3 Pasos de la transmisión
- 9.4 Eventos de la transmisión

10 *Modelos de seguridad*

- 10.1 Políticas de seguridad
- 10.2 Servicios de seguridad
- 10.3 Elementos de seguridad

SECCIÓN 3 – *Configuraciones*

11 *Visión de conjunto*

12 *Configuraciones funcionales*

12.1 Respecto a la guía
12.2 Respecto a la memoria de mensajes

13 *Configuraciones físicas*

13.1 Sistemas de mensajería
13.2 Configuraciones representativas

14 *Configuraciones organizativas*

14.1 Dominios de gestión
14.2 Configuraciones representativas

15 *El STM global*

SECCIÓN 4 – *Denominación, direccionamiento y encaminamiento*

16 *Visión de conjunto*

17 *Denominación*

17.1 Nombres de guía
17.2 Nombres de O/D

18 *Direccionamiento*

18.1 Listas de atributos
18.2 Juegos de caracteres
18.3 Atributos normalizados
18.4 Equivalencia de listas de atributos
18.5 Formas de direcciones O/D
18.6 Atributos condicionales

19 *Encaminamiento*

SECCIÓN 5 – *Uso de la guía*

20 *Visión de conjunto*

21 *Autenticación*

22 *Resolución de nombre*

23 *Ampliación de LD*

24 *Evaluación de capacidades*

SECCIÓN 6 – *Realización por ISA*

25 *Visión de conjunto*

26 *Elementos de servicio de aplicación*

26.1 El concepto de ESA
26.2 ESA simétricos y asimétricos
26.3 ESA de tratamiento de mensajes
26.4 ESA de apoyo

27 *Contextos de aplicación*

Anexo A – Clases de objetos de guía y atributos
Anexo B – Definición de referencia de identificadores de objetos
Anexo C – Definición de referencia de clases de objetos de guía y atributos
Anexo D – Amenazas contra la seguridad
Anexo E – Provisión de servicios de seguridad en la Recomendación X.411
Anexo F – Diferencias entre la Recomendación del CCITT y la Norma ISO
Anexo G – Índice

SECCIÓN 1 – INTRODUCCIÓN

0 Introducción

La presente Recomendación forma parte de una serie de Recomendaciones sobre el tratamiento de mensajes. Esta serie proporciona un amplio esquema de sistemas de tratamiento de mensajes (STM) constituidos por cualquier número de sistemas abiertos cooperantes.

Un STM tiene por objeto permitir a los usuarios el intercambio de mensajes, sobre la base de su almacenamiento y retransmisión. Un mensaje presentado en nombre de un usuario, el originador, es transportado por el sistema de transferencia de mensajes (STRM) y entregado a continuación a los agentes de uno o más usuarios adicionales, los destinatarios. Las unidades de acceso (UA) enlazan el STRM con sistemas de comunicación de otro tipo (por ejemplo, sistemas postales). El usuario recibe la ayuda de un agente de usuario (AU) para la preparación, el almacenamiento y la visualización de los mensajes. Facultativamente, puede recibir la ayuda de un dispositivo de almacenamiento de mensajes (AM) para almacenarlos. El STRM consta de cierto número de agentes de transferencia de mensajes (ATM) que, de manera colectiva, realizan la función de transferencia de almacenamiento y retransmisión de mensajes.

Esta Recomendación especifica la arquitectura global del STM, y sirve como introducción técnica al mismo.

El texto de la presente Recomendación es objeto de un acuerdo conjunto CCITT-ISO. La especificación correspondiente de la ISO es la ISO 10021-2.

1 Objeto

Esta Recomendación define la arquitectura global del STM y sirve como introducción técnica al mismo.

En otras Recomendaciones se especifican otros aspectos del tratamiento de mensajes. La Recomendación X.400 da una visión general, no técnica, del tratamiento de mensajes. La prueba de conformidad de los componentes del STM se describe en la Recomendación X.403. Los convenios establecidos al definir los servicios abstractos proporcionados por los componentes del STM se definen en la Recomendación X.407. Las reglas detalladas según las cuales el STRM convierte los contenidos de los mensajes de un TIC a otro se definen en la Recomendación X.408. El servicio abstracto que proporciona el STRM y el procedimiento que gobierna su operación distribuida se definen en la Recomendación X.411. El servicio abstracto proporcionado por el AM se define en la Recomendación X.413. Los protocolos de aplicación que gobiernan las interacciones de los componentes del STM se especifican en la Recomendación X.419. El sistema de mensajería interpersonal, que es una aplicación del tratamiento de mensajes, se define en la Recomendación X.420. El acceso telemático al sistema de mensajería interpersonal se especifica en la Recomendación T.330.

En el cuadro 1/X.402 se indican de manera resumida las Recomendaciones del CCITT y las normas internacionales de la ISO relacionadas con el tratamiento de mensajes.

CUADRO 1/X.402

Especificaciones para sistemas de tratamiento de mensajes

CCITT	ISO	Tema tratado
		Introducción
X.400 X.402	8505-1 8505-2	Visión de conjunto de sistemas y servicios Arquitectura global
		Aspectos diversos
X.403 X.407 X.408	– 8883-2 –	Pruebas de conformidad Convenios para la definición del servicio abstracto Reglas de conversión de tipo de información codificada
		Servicios abstractos
X.411 X.413	8883-1 TBS-1	Definición del servicio abstracto del STRM y procedimientos de operación distribuida Definición del servicio abstracto de almacenamiento de mensajes
		Protocolos
X.419	8505-2	Especificaciones de protocolo
		Sistema de mensajería interpersonal
X.420 T.330	9065 –	Sistema de mensajería interpersonal Acceso telemático al SMIP

La guía, que es el instrumento principal para la difusión de la información relacionada con las comunicaciones entre los componentes del STM, se define en las Recomendaciones de la serie X.500 (véase el cuadro 2/X.402).

El fundamento arquitectural del tratamiento de mesajes figura en otras Recomendaciones. El modelo de referencia de ISA se define en la Recomendación X.200. En las Recomendaciones X.208 y X.209 se definen la notación NSA.1 para la especificación de las estructuras de datos de los servicios abstractos y los protocolos de aplicación y las reglas de codificación asociadas. La manera de establecer y liberar asociaciones, el ACSE, se especifica en las Recomendaciones X.217 y X.227. En las Recomendaciones X.218 y X.228 se define el método ESTF de transporte fiable de las UDPA por las asociaciones. La manera de efectuar peticiones a otros sistemas abiertos, el ESOD, se especifica en las Recomendaciones X.219 y X.229.

En el cuadro 3/X.402 se indican, en síntesis, las Recomendaciones del CCITT y las normas internacionales de la ISO básicas para el tratamiento de mensajes.

CUADRO 2/X.402

Especificaciones para las guías

CCITT	ISO	Tema tratado
	Modelo	
X.200	7498	Modelo de referencia de ISA
X.500	9594-1	La guía – Visión de conjunto de conceptos, modelos y servicios
X.501	9594-2	La guía – Modelos
X.509	9594-8	La guía – Marco de autenticación
X.511	9594-3	La guía – Definición del servicio abstracto
X.518	9594-4	La guía – Procedimientos de operación distribuida
X.519	9594-5	La guía – Especificaciones de protocolos
X.520	9594-6	La guía – Tipos de atributos seleccionados
X.521	9594-7	La guía – Clases de objetos seleccionados

CUADRO 3/X.402

Especificaciones para los fundamentos del STM

CCITT	ISO	Tema tratado
	Modelo	
X.200	7498	Modelo de referencia de ISA
	NSA.1	
X.208 X.209	8824 8825	Notación de sintaxis abstracta uno Reglas básicas de codificación
	Control de asociación	
X.217 X.227	8649 8650	Definición de servicios Especificación del protocolo
	Transferencia fiable	
X.218 X.228	9066-1 9066-2	Definición de servicios Especificación del protocolo
	Operaciones a distancia	
X.219 X.229	9072-1 9072-2	Definición de servicios Especificación del protocolos

La presente Recomendación está estructurada como a continuación se indica. La sección 1 es la de introducción. En la sección 2 se presentan los modelos abstractos de tratamiento de mensajes. En la sección 3 se especifica la manera de configurar el STM para satisfacer una diversidad de exigencias de tipo funcional, físico u organizativo. En la sección 4 se describe la denominación y el direccionamiento de usuarios y listas de distribución y el encaminamiento hacia ellos de los objetos de información. En la sección 5 se indican los usos que el STM puede hacer de la guía. En la sección 6 se describe cómo se realiza el STM utilizando la ISA. Los anexos contienen importante información suplementaria.

No se establecen requisitos de conformidad en relación con esta Recomendación.

2 Referencias

En esta Recomendación y en otras de la misma serie se citan los documentos que se indican a continuación.

2.1 *Interconexión de sistemas abiertos*

En esta Recomendación y en otras de la misma serie se citan las siguientes especificaciones de la ISA:

X.200 Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 7498)

X.208 Especificación de la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8824)

X.209 Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8825)

X.217 Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 8649)

X.218 Transferencia fiable: modelo y definición de servicios (véase también la Norma ISO 9066-1)

X.219 Operaciones a distancia: modelo, notación y definición del servicio (véase también la Norma ISO 9072-1)

X.227 Especificación del protocolo de control de asociación para la interconexión de sistemas abiertos para aplicación del CCITT (véase también la Norma ISO 8650)

X.228 Transferencia fiable: especificación del protocolo (véase también la Norma ISO 9066-2)

X.229 Operaciones a distancia: especificación del protocolo (véase también la Norma ISO 9072-2)

2.2 *Sistemas de guía*

En esta Recomendación y en otras de la misma serie se citan las siguientes especificaciones de conceptos, modelos y servicios de sistemas de guía:

X.500 La guía – Visión de conjunto de conceptos, modelos y servicios (véase también la Norma ISO 9594-1)

X.501 La guía – Modelos (véase también la Norma ISO 9594-2)

X.509 La guía – Marco de autenticación (véase también la Norma ISO 9594-8)

X.511 La guía – Definición del servicio abstracto (véase también la Norma ISO 9594-3)

X.518 La guía – Procedimientos para operación distribuida (véase también la Norma ISO 9594-4)

X.519 La guía – Especificaciones de protocolos (véase la Norma ISO 9594-5)

X.520 La guía – Tipos de atributos seleccionados (véase también la Norma ISO 9594-6)

X.521 La guía – Clases de objetos seleccionadas (véase también la Norma ISO 9594-7)

2.3 *Sistemas de tratamiento de mensajes*

En esta Recomendación y en otras de la misma serie se citan las siguientes especificaciones de sistemas de tratamiento de mensajes:

T.330 Acceso telemático al servicio de mensajería interpersonal

X.400 Sistema de tratamiento de mensajes: Visión de conjunto del sistema y del servicio (véase también la Norma ISO 10021-1)

X.403 Sistemas de tratamiento de mensajes: Pruebas de conformidad

X.407 Sistemas de tratamiento de mensajes: Convenios para la definición del servicio abstracto (véase también la Norma ISO 10021-3)

X.408 Sistemas de tratamiento de mensajes: Reglas de conversión de tipos de información codificada

X.411 Sistemas de tratamiento de mensajes: Definición del servicio abstracto y procedimientos (véase también la Norma ISO 10021-4)

X.413 Sistemas de tratamiento de mensajes: Definición del servicio abstracto de almacenamiento de mensajes (véase también la Norma ISO 10021-5)

X.419 Sistemas de tratamiento de mensajes: Especificaciones de protocolo (véase también la Norma ISO 10021-6)

X.420 Sistemas de tratamiento de mensajes: Sistema de mensajería interpersonal (véase también la Norma ISO 10021-7)

3 Definiciones

Las definiciones que se indican a continuación se aplican a efectos de la presente Recomendación y de otras de la misma serie.

3.1 *Interconexión de sistemas abiertos*

3.1.1 En esta Recomendación y en otras de la misma serie se emplean los nombres de las siete capas del modelo de referencia así como los siguientes términos definidos en la Recomendación X.200:

a) sintaxis abstracta;
b) entidad de aplicación (EA);
c) proceso de aplicación;
d) unidad de datos de protocolo de aplicación (UDPA);
e) elemento de servicio de aplicación (ESA);
f) tarea de tratamiento de la información distribuida;
g) capa;
h) sistema abierto;
i) interconexión de sistemas abiertos (ISA);
j) par;
k) contexto de presentación;
l) protocolo;
m) modelo de referencia;
n) sintaxis de transferencia;
o) elemento de usuario (EU).

3.1.2 En esta Recomendación y en otras de la misma serie se emplean los nombres de los tipos y valores de datos NSA.1 así como los siguientes términos definidos en las Recomendaciones X.208 y X.209:

a) notación de sintaxis abstracta uno (NSA.1);
b) reglas básicas de codificación;
c) explícito;
d) exportación;
e) implícito;
f) importación;
g) macro;
h) módulo;
i) rótulo;
j) tipo;
k) valor.

3.1.3 En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Recomendación X.217:

a) asociación de aplicación; asociación;
b) contexto de aplicación (CA);
c) elemento de servicio control de asociación (ESCA);
d) iniciador;
e) respondedor.

3.1.4 En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Recomendación X.218:

a) transferencia fiable (TF);
b) elemento de servicio transferencia fiable (ESTF).

3.1.5 En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Recomendación X.219:

a) argumento;
b) asíncrono;
c) vinculado;
d) parámetro;
e) error distante;
f) operación distante;
g) operaciones distantes (OD);
h) elemento de servicio, operaciones distantes (ESOD);
i) resultado;
j) síncrono;
k) no vinculado.

3.2 *Sistemas de guía*

En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en las Recomendaciones de la serie X.500:

a) atributo;
b) certificado;
c) autoridad certificadora;
d) trayecto de la certificación;
e) inscripción en la guía;
f) agente de sistema de guía (ASG);
g) guía;
h) función confusión;
i) nombre;
j) clase de objeto;
k) objeto;
l) autenticación simple;
m) autenticación fuerte.

3.3 *Sistemas de tratamiento de mensajes*

A efectos de la presente Recomendación y de otras de la misma serie, son de aplicación las definiciones cuya relación figura en el anexo G.

4 Abreviaturas

A efectos de la presente Recomendación y de otras de la misma serie, son de aplicación las siglas cuya relación figura en el anexo G.

5 Convenios

En esta Recomendación se utilizan los convenios descriptivos indicados a continuación.

5.1 *NSA.1*

Esta Recomendación emplea, en sus anexos A y C, diversos convenios de descripción basados en la NSA.1, para definir información propia del tratamiento de mensajes, que pueda contener la guía. Utiliza, en particular, las macros OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE-SYNTAX de la Recomendación X.501, para definir las clases de objetos, los atributos y las sintaxis de atributo propias del tratamiento de mensajes.

La NSA.1 aparece en el anexo A como ayuda a la explicación y en el anexo C, innecesariamente en buena medida, como referencia. Cuando hay diferencias entre ambos, se indica una especificación de error.

Obsérvese que los rótulos de identificación de NSA.1 están implícitos en todo el módulo NSA.1 que se define en el anexo C; el módulo es definitivo a este respecto.

5.2 *Grado*

Cuando en esta Recomendación se describe una clase de estructura de datos (por ejemplo, direcciones O/D) que tiene componentes (por ejemplo, atributos), a cada componente se le asigna uno de los siguientes **grados**:

a) **obligatorio (O)**: un componente obligatorio estará presente en cada caso de la clase;

b) **facultativo (F)**: un componente facultativo estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que suministra ese caso. No hay valor por defecto;

c) **defectible (D)**: un componente defectible estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que ofrece ese caso. En su ausencia se aplica un valor por defecto especificado por esta Recomendación;

d) **condicional (C)**: un componente condicional estará presente en un caso de la clase, tal como exige esta Recomendación.

5.3 *Términos*

En el resto de la presente Recomendación, los términos se escriben en **negritas** al definirlos, en *bastardilla* cuando se hace referencia a los mismos antes de su definición y sin realce especial en otras ocasiones.

Los términos que son nombres propios se presentan en letras mayúsculas; no así los términos genéricos.

SECCIÓN 2 – MODELOS ABSTRACTOS

6 Visión de conjunto

En esta sección se presentan modelos abstractos de *tratamiento de mensajes*, que proporcionan la arquitectura básica para la elaboración de las especificaciones, más detalladas, que figuran en otras Recomendaciones de la serie.

El **tratamiento de mensajes** es una tarea distribuida del tratamiento de la información, que comprende las siguientes subtareas intrínsecamente relacionadas:

a) **transferencia de mensajes**: Transmisión diferida de objetos de información entre usuarios, empleando computadores como intermediarios.

b) **almacenamiento de mensajes**: Almacenamiento automático, para su posterior recuperación, de objetos de información, transportados mediante la transferencia de mensajes.

La sección 2 abarca los siguientes temas:

a) modelo funcional;

b) modelo de información;

c) modelo operacional;

d) modelo de seguridad.

Nota – El tratamiento de mensajes tiene una pluralidad de aplicaciones, una de las cuales es la mensajería interpersonal que se describe en la Recomendación X.420.

7 Modelo funcional

En este punto se da un modelo funcional de tratamiento de mensajes. De la realización concreta del modelo se ocupa otra Recomendación de la serie.

El **entorno del tratamiento de mensajes (ETM)** comprende objetos funcionales «primarios» de varios tipos: el *sistema de tratamiento de mensajes (STM)*, los *usuarios* y las *listas de distribución*. A su vez, el STM, puede descomponerse en objetos funcionales «secundarios», de menor nivel y de varios tipos: el *sistema de transferencia de mensajes (STRM)*, los *agentes de usuario*, las *memorias de mensajes* y las *unidades de acceso*. El *STRM*, en fin, puede descomponerse en objetos funcionales «terciarios», aun de menor nivel y de un solo tipo; los *agentes de transferencia de mensajes*.

Los tipos de objetos funcionales primarios, secundarios y terciarios y los tipos de *unidades de acceso* seleccionadas se definen y describen por separado en los puntos que siguen.

Tal como se precisa a continuación, los objetos funcionales se adaptan a veces a una o más aplicaciones del tratamiento de mensajes, por ejemplo la mensajería interpersonal (véanse las Recomendaciones X.420 y T.330). Un objeto funcional, que ha sido adaptado a una aplicación, comprende la sintaxis y la semántica del contenido de los mensajes intercambiados en esa aplicación.

Como asunto local, los objetos funcionales pueden tener capacidades superiores a las especificadas en esta Recomendación o en otras de la misma serie. En concreto, un *agente de usuario* típico tiene capacidades de preparación, reproducción y almacenamiento de mensajes que no están normalizadas.

7.1 *Objetos funcionales primarios*

El ETM comprende el *sistema de tratamiento de mensajes*, los *usuarios* y las *listas de distribución*. Entre estos objetos funcionales primarios se produce una interacción. A continuación se definen y describen los tipos de objetos.

En la figura 1/X.402 se representa de manera esquemática esa interacción.

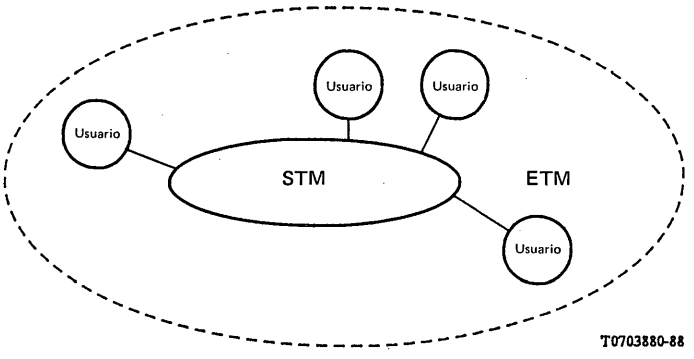


FIGURA 1/X.402

Entorno del tratamiento de mensajes

7.1.1 *Sistema de tratamiento de mensajes*

La finalidad principal del tratamiento de mensajes es transportar objetos de información de un usuario a otro. Al objeto funcional que lleva a cabo esta tarea se le denomina **sistema de tratamiento de mensajes (STM)**.

El ETM consta de un solo STM.

7.1.2 *Usuarios*

La finalidad principal del STM es transportar objetos de información entre *usuarios*. Al objeto funcional (por ejemplo, una persona) que más que proporcionar tratamiento de mensajes, participa en ese tratamiento, se le denomina **usuario**.

Cabe distinguir las siguientes clases de usuarios:

a) **usuario directo**: Usuario que participa en el tratamiento de mensajes utilizando directamente el STM.

b) **usuario indirecto**: Usuario que participa en el tratamiento de mensajes utilizando indirectamente el STM, es decir, a través de otro sistema de comunicaciones (por ejemplo, un sistema postal o una red télex) al que está enlazado el STM.

El ETM consta de un número cualquiera de usuarios.

7.1.3 *Lista de distribución*

Mediante el STM, un usuario puede hacer llegar objetos de información a grupos de usuarios previamente especificados, así como a usuarios individuales. Se llama **lista de distribución (LD)** al objeto funcional que representa a un grupo de usuarios previamente especificado y a otras LD.

Una LD representa cero o más usuarios y LD, a los que se les denomina sus **miembros**. De las LD (si es que hay alguna) se dice que están jerarquizadas. Pedir al STM que transporte un objeto de información (por ejemplo, un *mensaje*) a una LD equivale a pedirle que lo transporte a sus miembros. Téngase en cuenta que se trata de un proceso recurrente.

El derecho a transportar *mensajes* a una LD determinada, o el permiso para hacerlo, puede estar bajo control. A ese derecho, se le denomina **permiso de depósito**. Como asunto local, es posible restringir más aún el uso de una LD.

El ETM consta de un número cualquiera de LD.

Nota – Una LD podría estar más restringida, limitándola por ejemplo al transporte de *mensajes* con un determinado *tipo de contenido.*

7.2 *Objetos funcionales secundarios*

El STM comprende el *sistema de transferencia de mensajes*, los *agentes de usuarios*, las *memorias de mensajes* y las *unidades de acceso.* Entre estos objetos funcionales secundarios se produce una interacción. Más adelante se definen y describen los tipos de objetos.

En la figura 2/X.402 se representa de forma esquemática esa interacción.

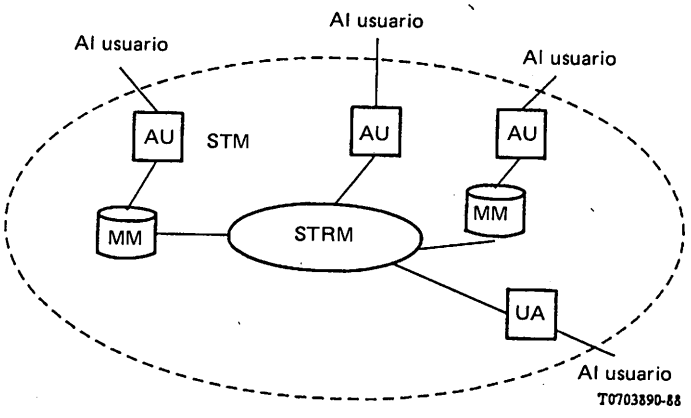


FIGURA 2/X.402

Sistema de tratamiento de mensajes

7.2.1 *Sistema de transferencia de mensajes*

En el STM se produce un transporte de objetos de información a usuarios individuales y a los miembros de las LD. El objeto funcional que realmente los transporta se llama **sistema de transferencia de mensajes (STRM).** El STRM es un sistema de comunicación de almacenamiento y retransmisión, del que se puede decir que es la columna vertebral del STM.

El STRM es de uso general y facilita toda clase de aplicaciones del tratamiento de mensajes. Además, el STRM puede adaptarse a una o más aplicaciones particulares, es decir, puede efectuar una *conversión.*

El STM consta de un solo STRM.

7.2.2 *Agentes de usuario*

El objeto funcional por medio del cual un usuario directo aislado participa en el tratamiento de mensajes se denomina **agente de usuario (AU).**

Un AU típico está adaptado a una o más aplicaciones particulares del tratamiento de mensajes.

El STM consta de un número cualquiera de AU.

Nota – En el caso de un AU que preste servicio a un usuario humano, lo típico es que la interacción entre agente y usuario se establezca a través de un dispositivo de entrada/salida (por ejemplo, un teclado, una pantalla, un dispositivo de barrido, una impresora o una combinación de algunos de estos dispositivos).

7.2.3 *Memorias de mensajes*

El usuario típico debe almacenar la información que recibe. El objeto funcional que proporciona a un usuario directo (aislado) la capacidad de almacenar mensajes se llama **memoria de mensajes (MM).** Cada MM está asociada a un AU, pero no todos los AU tienen MM asociada.

Las MM son de uso general y facilitan todas las aplicaciones de tratamiento de mensajes. Además, una MM puede adaptarse a una o más aplicaciones particulares, de tal modo que pueda, con mayor facilidad, *presentar* mensajes y permitir la *recuperación de mensajes* asociados a esa aplicación.

El STM consta de un número cualquiera de MM.

Nota – Como asunto local, un AU puede proporcionar capacidad de almacenamiento de objetos de información que complementa o sustituye la de una MM.

7.2.4 *Unidades de acceso*

El objeto funcional que enlaza al STRM con otro sistema de comunicaciones (por ejemplo, un sistema postal o la red télex) y, a través del cual, sus patronos participan en el tratamiento de mensajes como usuarios indirectos, se denomina **unidad de acceso (UA).**

Una UA típica está adaptada a un sistema de comunicaciones particular y a una o más aplicaciones particulares del tratamiento de mensajes.

El STM consta de un número cualquiera de UA.

7.3 *Objetos funcionales terciarios*

El STRM está formado por *agentes de transferencia de mensajes.* Entre estos objetos funcionales terciarios se produce una interacción. Más adelante se definen y describen los tipos de objetos terciarios.

En la figura 3/X.402 se representa de manera esquemática esa interacción.

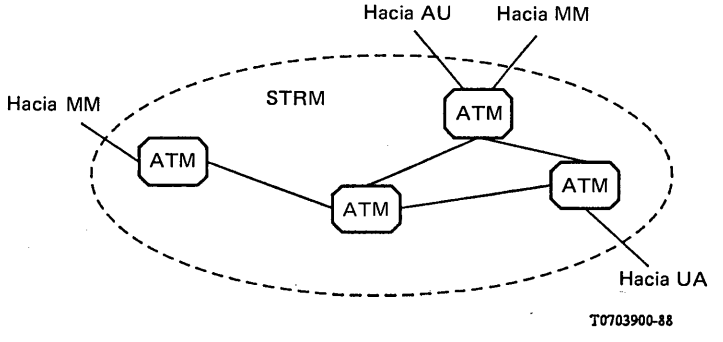


FIGURA 3/X.402

Sistema de transferencia de mensajes

7.3.1 *Agentes de transferencia de mensajes*

El STRM transporta objetos de información a usuarios y LD según el modo de almacenamiento y retransmisión. Al objeto funcional que proporciona el eslabón de la cadena de almacenamiento y retransmisión del STRM se le denomina **agente de transferencia de mensajes (ATM).**

Los ATM son de uso general y facilitan las aplicaciones del tratamiento de mensajes. Además, un ATM se puede adaptar a una o más aplicaciones particulares, es decir, puede efectuar una *conversión.*

El STR consta de un número cualquiera de ATM.

7.4 *Tipos de UA seleccionados*

Como se ha descrito anteriormente, entre el STM y otros tipos de sistemas de comunicaciones se produce un interfuncionamiento a través de las UA. En los párrafos que siguen se presentan varios tipos de UA seleccionados: de *entrega física,* de acceso telemático y por télex.

7.4.1 *Entrega física*

Una **unidad de acceso de entrega física (UAEF)** es una UA que somete los *mensajes* (pero no las *sondas* ni los *informes*) a *reproducción física,* y transporta los *mensajes físicos* resultantes a un *sistema de entrega física.*

A la transformación de un *mensaje* en un *mensaje físico* se le denomina **reproducción física**. Un **mensaje físico** es un objeto físico (por ejemplo, una carta y su sobre de papel) que contiene un *mensaje*.

Un **sistema de entrega física (SEF)** es un sistema que efectúa la *entrega física*. El sistema postal es un tipo importante de SEF. Se llama **entrega física** a la transferencia de un mensaje físico a un patrón de un SEF, uno de los usuarios indirectos a los que la UAEF proporciona capacidades de tratamiento de mensajes.

La mensajería interpersonal es una de las aplicaciones del tratamiento de mensajes proporcionadas por todas las UAEF (véase la Recomendación X.420).

7.4.2 *Telemática*

En la Recomendación X.420 se presentan las unidades de acceso telemático, que proporcionan, en exclusiva, la mensajería interpersonal.

7.4.3 *Télex*

En la Recomendación X.420 se presentan las unidades de acceso télex, que proporcionan, en exclusiva, la mensajería interpersonal.

8 Modelo de información

En este punto se presenta un modelo de información del tratamiento de mensajes. La realización concreta del modelo es objeto de otras Recomendaciones de la serie.

El STM y el STRM pueden transportar objetos de información de tres clases: *mensajes*, *sondas* e *informes*. En la primera columna del cuadro 4/X.402 figuran esas tres clases. Para cada una de ellas se indican, en la segunda columna, los tipos de objetos funcionales – usuario, AU, MM, ATM y UA – que son origen y destino final de tales objetos.

CUADRO 4/X.402

Objetos de información transportables

Objeto de información	Objeto funcional				
	Usuario	AU	MM	ATM	UA
Mensaje	OD	–	–	–	–
Sonda	O	–	–	D	–
Informe	D	–	–	O	–

O Último origen

D Último destino

En los puntos que siguen se definen y describen los objetos de información cuyo resumen figura en el cuadro 4/X.402.

8.1 *Mensajes*

La finalidad principal de la transferencia de mensajes es el transporte de objetos de información llamados **mensajes** de un usuario a otros. Un mensaje, como se muestra en la figura 4/X.402, consta de las siguientes partes:

a) **sobre**: Objeto de información cuya composición varía de un *paso de transmisión* a otro, y que identifica de manera diversa al *originador* del mensaje y a los *destinatarios potenciales*, informa sobre el transporte previo y dirige el siguiente por el STRM, y caracteriza el *contenido* del mensaje.

b) **contenido**: Objeto de información que el STRM ni examina ni modifica, si no es a efectos de *conversión*, mientras transporta el mensaje.

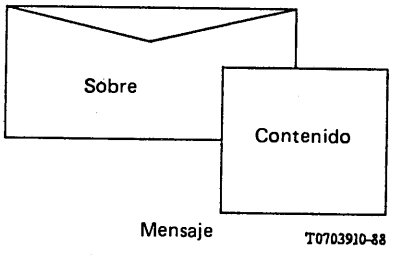


FIGURA 4/X.402

Sobre y contenido de un mensaje

Una parte de información, que figura en el sobre, identifica el tipo de contenido. El **tipo de contenido** es un identificador (un identificador de objeto o entero NSA.1) que indica la sintaxis y la semántica del contenido en su conjunto. Ese identificador permite al STRM determinar si el mensaje ha de *entregarse* o no a usuarios particulares, y permite a los AU y MM interpretar y tratar el contenido.

Otra parte de información, que figura asimismo en el sobre, identifica los tipos de información codificada representada en el contenido. Un **tipo de información codificada (TIC)** es un identificador (un identificador de objeto o entero NSA.1) que indica el soporte y el formato (por ejemplo, texto AI N.° 5 o facsímil del grupo 3) de partes individuales del contenido. Permite además al STRM determinar si el mensaje se ha de entregar o no a usuarios particulares, e identificar las oportunidades de *hacer* el mensaje entregable, convirtiendo una porción del contenido de un TIC a otro.

8.2 *Sondas*

Un segundo objetivo de la transferencia de mensajes es transportar objetos de información llamados **sondas** desde un usuario a otros (es decir, llevarlos hasta los ATM que prestan servicio a esos usuarios). Una sonda describe una clase de mensajes y se utiliza para determinar si deben *entregarse* o no dichos mensajes.

A un mensaje descrito por una sonda se le llama **mensaje descrito**.

La sonda consta de un solo sobre. El sobre contiene, en gran parte, la misma información que para un mensaje. Además del tipo de contenido y los tipos de información codificada del mensaje descrito, en el sobre figura la longitud de su contenido.

El *depósito* de una sonda da lugar a un comportamiento del STRM que es, en buena medida, el mismo que suscitaría el *depósito* de cualquier mensaje descrito, salvo que en el caso de la sonda, se prescinde de la *ampliación y de la entrega de la LD.* En concreto, y aparte de las consecuencias de la supresión de la *ampliación de la LD*, la sonda da lugar a los mismos *informes* a que daría lugar cualquier mensaje descrito. En esto reside la utilidad de las sondas.

8.3 *Informes*

Un tercer objetivo de la transferencia de mensajes es transportar a los usuarios unos objetos de información, llamados **informes**. Un informe, generado por el STRM, comunica el resultado o la marcha de la *transmisión* de un mensaje o de una sonda a uno o más destinatarios potenciales.

Al mensaje o a la sonda que sean objeto de un informe se les llama **mensaje objeto** o **sonda objeto**, respectivamente.

Un informe referido a un determinado *destinatario potencial* se lleva hasta el *originador* del mensaje o de la sonda objeto, a menos que el *destinatario potencial* sea un *destinatario miembro.* En este último caso, el informe es transportado a la LD a la que pertenezca el *destinatario miembro.* Como asunto local, (es decir, cuando exista una política establecida para esa LD particular), el transporte del informe puede proseguir hasta el propietario de la LD, a otro que contenga LD (en caso de jerarquización) o al originador del mensaje objeto (en su caso), o a ambos.

Los resultados a los que puede referirse un informe único son de las siguientes clases:

a) **informe de entrega**: *Entrega, exportación* o *afirmación* del mensaje objeto o de la sonda objeto, o bien *ampliación de la LD.*

b) **informe de no entrega**: *No entrega* o *no afirmación* del mensaje objeto o de la sonda objeto.

Un informe puede comprender uno o más informes de entrega y/o no entrega.

Un mensaje o una sonda puede dar lugar a varios informes de entrega y/o no entrega relativos a un determinado *destinatario potencial.* Cada uno de ellos marca el tránsito de un *paso* o *evento* de transmisión diferente.

9 Modelo operacional

En este punto se presenta un modelo operacional de tratamiento de mensajes. La realización concreta del modelo es objeto de otras Recomendaciones de la serie.

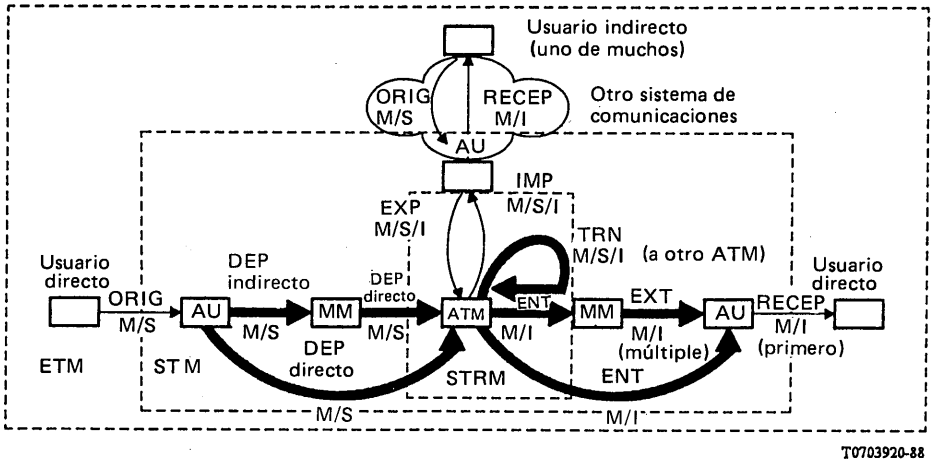
El STM puede transportar un objeto de información a usuarios individuales, LD o una combinación de ambos. El transporte se lleva a cabo por un proceso llamado *transmisión,* que comprende *pasos* y *eventos.* A continuación se definen y describen el proceso y sus subdivisiones, así como el papel que los usuarios y las LD desempeñan en éste.

9.1 *Transmisiôm*

Se llama **transmisión** al transporte o tentativa de transporte de un mensaje o de una sonda. La transmisión abarca el transporte del mensaje desde su *originador* a sus *destinatarios potenciales* y el transporte de la sonda desde su *originador* hasta los ATM, facultados para *afirmar* la *entregabilidad* o no del mensaje descrito a los *destinatarios potenciales* de aquélla. La transmisión comprende también el transporte o tentativa de transporte al *originador* de cuantos informes provoquen el mensaje o la sonda.

La transmisión se desarrolla a través de una secuencia de *pasos de transmisión* y *eventos.* Un **paso de transmisión** (o **paso**) consiste en el transporte de un mensaje, una sonda o un informe desde un objeto funcional a otro «adyacente» al primero. Un **evento de transmisión** (o **evento**) consiste en el tratamiento de un mensaje, una sonda o un informe en un objeto funcional, tratamiento que puede influir en la selección, por parte del objeto funcional, del siguiente paso o evento.

En la figura 5/X.402 se presenta de manera esquemática el flujo de información de la transmisión. Se muestran en ella los tipos de objetos funcionales – usuarios directos, usuarios indirectos, AU, MM, ATM y UA – que pueden tomar parte en una transmisión, los objetos de información – mensajes, sondas, e informes – que pueden ser transportados entre aquéllos y los nombres de los pasos de transmisión mediante los cuales se efectúan esos transportes.



Normalizado
No normalizado

M	Mensaje	ORIG	Origen	EXP	Exportación
S	Sonda	DEP	Depósito	ENT	Entrega
I	Informe	IMP	Importación	EXT	Extracción
		TRN	Transferencia	RECEP	Recepción

FIGURA 5/X.402

Flujo de información de la transmisión

La figura 5/X.402 destaca el hecho de que, un mensaje o informe, pueden ser extraídos repetidamente y que sólo el primer transporte de un objeto extraído desde el AU al usuario constituye *recepción.*

El evento tiene un papel destacado en la transmisión. La *división* duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus *destinatarios inmediatos.* Se llaman **destinatarios inmediatos** a los destinatarios potenciales asociados a un caso particular de un mensaje o sonda. Un ATM efectúa una división si el siguiente paso o evento, necesario para transportar un mensaje o sonda a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros. En cada una de las descripciones de pasos y eventos que a continuación se hacen, se supone que el paso o evento es adecuado para todos los destinatarios inmediatos, situación que puede crearse, si es preciso, por división.

9.2 *Funciones de la transmisión*

Los usuarios y las LD desempeñan una diversidad de papeles en la transmisión de un mensaje o una sonda. A esos papeles se les clasifica, de manera informal, en paquetes «origen», papeles «destino» y categorías a las que se pueden elevar los usuarios o las LD.

9.2.1 Un usuario puede desempeñar el siguiente papel «origen» en la transmisión de un mensaje o sonda:

a) **originador**: Usuario (no LD) que es origen último de un mensaje o sonda.

9.2.2 Un usuario o una LD pueden desempeñar alguno de los siguientes papales «destino» en la transmisión de un mensaje o sonda:

a) **destinatario deseado**: Uno de los usuarios o de las LD que el originador especifica como destinos de un mensaje o una sonda.

b) **destinatario alternativo especificado por el originador**: Usuario (o LD si hay alguna) al que el originador pide que sea transportado un mensaje o sonda, si no puede transportarse a un determinado destinatario deseado.

c) **destinatario miembro**: LD o usuario al cual se transporta un mensaje (pero no una sonda), como resultado de una *ampliación de LD.*

d) **destinatario alternativo designado por el destinatario**: Usuario (o LD si hay alguna) elegido por un destinatario miembro, o receptor deseado o alternativo al especificado por el originador, para que *redireccione* mensajes.

9.2.3 Un usuario o una LD pueden adquirir alguna de las siguientes categorías durante la transmisión de un mensaje o una sonda:

a) **destinatario potencial**: Cualquier LD o usuario hacia el cual se transporta un mensaje en cualquier momento durante la transmisión. Ha de tratarse necesariamente de un destinatario deseado o alternativo al especificado por el originador o al asignado.

b) **destinatario efectivo** (o **receptor**): Un destinatario potencial para el cual tiene lugar la *entrega* o la *afirmación.*

9.3 *Pasos de la transmisión*

En la primera columna del cuadro 5/X.402 figura una lista de los tipos de pasos que pueden producirse en una transmisión. Para cada tipo de la lista se indica, en la segunda columna, si ese paso está normalizado o no en la presente Recomendación o en otras de la misma serie; en la tercera columna, las clases de objetos de información – mensajes, sondas e informes – cuyo transporte está permitido en ese paso y en la cuarta columna, las clases de objetos funcionales – usuarios, AU, MM, ATM y UA – que pueden participar en ese paso como origen o destino del objeto.

El cuadro 5/X.402 está dividido en tres secciones. Los pasos de la primera sección corresponden a la «creación» de mensajes y sondas, los de la última a la «distribución» de mensajes e informes y los de la de en medio a la «remisión» de mensajes, sondas e informes.

En los puntos que siguen se definen y describen cada uno de los tipos de pasos de transmisión cuya relación figura en el cuadro 5/X.402.

CUADRO 5/X.402

Pasos de transmisión

Paso de transmisión	¿Normalizado?	Objetos de información			Objetos funcionales				
		M	S	I	Usuario	AU	MM	ATM	UA
Origen	No	X	X	–	O	D	–	–	–
Depósito	Sí	X	X	–	–	O	OD	D	–
Importación	No	X	X	X	–	–	–	D	O
Transferencia	Sí	X	X	X	–	–	–	OD	–
Exportación	No	X	X	X	–	–	–	O	D
Entrega	Sí	X	–	X	–	D	D	O	–
Recuperación	Sí	X	–	X	–	D	O	–	–
Recepción	No	X	–	X	D	O	–	–	–

M Mensaje
S Sonda
I Informe

O Origen
D Destino
X Permitido

9.3.1 *Origen*

En un paso de **origen**, un usuario directo transporta un mensaje o una sonda a su AU, o bien un usuario indirecto hace otro tanto al sistema de comunicaciones que le presta servicio. Este paso genera el mensaje o la sonda y constituye el primero de su transmisión.

El referido usuario es el originador del mensaje o de la sonda. Como tal originador identifica los destinatarios deseados de uno u otro objetos funcionales. Además, para cada destinatario deseado, puede identificar un destinatario alternativo, aunque no es preciso que lo haga.

9.3.2 *Depósito*

En un paso de **depósito** se transporta a un ATM, un mensaje o sonda que quedan a cargo del STRM. Cabe distinguir los dos tipos siguientes de depósito:

a) **depósito indirecto**: Paso de transmisión en el que el AU del originador transporta un mensaje o sonda a su MM y en el que la MM efectúa un *depósito directo*. Este paso sigue al de origen.

   Es un paso que sólo puede darse si el usuario dispone de una MM.

b) **depósito directo**: Paso de transmisión en el que el AU o la MM originador transportan un mensaje o sonda a un ATM. Este paso sigue al de origen o se produce como parte de un depósito indirecto.

   Es posible dar este paso tanto si el usuario está equipado con una MM como si no lo está.

El depósito indirecto y el directo son funcionalmente equivalentes, salvo en lo que se refiere a las capacidades adicionales de las que es posible disponer con el primero. El depósito indirecto puede diferir del directo en otros aspectos (por ejemplo, en el número de sistemas abiertos con los que debe establecer una interacción aquel que incorpore un AU) y ser por ello preferible al depósito directo.

Al AU o a la MM que participa en el depósito directo se le llama **agente de depósito**. Un agente de depósito se da a conocer al STRM mediante un proceso de registro, como resultado del cual el agente de depósito y el STRM quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.3 *Importación*

En un paso de **importación**, una UA transporta un mensaje, una sonda o un informe a un ATM. Este paso introduce en el STRM un objeto de información llevado en otro sistema de comunicaciones, y se produce a continuación de su transporte por dicho sistema.

Nota – El concepto de importación es un concepto genérico. La manera cómo se efectúe este paso varía, naturalmente, de una UA a otra.

9.3.4 *Transferencia*

En un paso de **transferencia**, un ATM transporta un mensaje, una sonda o un informe a otro ATM. En este paso, el transporte del objeto de información tiene lugar a lo largo de distancias físicas y, a veces, organizativas. Se produce a continuación del depósito directo o de la importación o de una transferencia previa.

Por supuesto, este paso sólo puede darse si el STRM consta de varios ATM.

Cabe distinguir, según sea el número de *DG* afectados, los siguientes tipos de transferencia:

a) **transferencia interna**: Transferencia que implica a varios ATM en un solo *DG*.

b) **transferencia externa**: Transferencia que implica a varios ATM en diferentes *DG*.

9.3.5 *Exportación*

En un paso de **exportación**, un ATM transporta un mensaje, una sonda o un informe a una UA. En este paso, se lanza un objeto de información desde el STRM hacia otro sistema de comunicaciones. El paso se produce a continuación del depósito directo, de la importación o de la transferencia.

El ATM puede generar, como parte de este paso, un informe de entrega.

Nota – El concepto de exportación es un concepto genérico. La manera cómo se efectúe este paso varía, naturalmente, de una UA a otra.

9.3.6 *Entrega*

En un paso de **entrega**, un ATM transporta un mensaje o un informe a una MM o a un AU. La MM y el AU corresponden a un destinatario potencial del mensaje o al originador del mensaje o sonda objeto del informe. En este paso se confía el objeto de información a un representante del usuario y se produce tras el depósito directo, la importación o la transferencia. Además, se eleva al usuario en cuestión a la categoría de destinatario efectivo.

En el caso de un mensaje el ATM puede generar, como parte de este paso, un informe de entrega.

Se llama **agente de entrega** a la MM o al AU que participan en la misma. Un agente de entrega se da a conocer al STRM mediante un proceso de registro, como resultado del cual el agente de entrega y el STRM quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.7 *Recuperación*

En un paso de **recuperación**, la MM de un usuario transporta un mensaje o un informe a su AU. El usuario en cuestión es un destinatario efectivo del mensaje o el originador del mensaje o de la sonda objeto. Este paso extrae del almacenamiento el objeto de información de manera no destructiva. Se produce tras el paso de entrega o de una recuperación previa.

El paso de recuperación sólo puede darse si el usuario está equipado con una MM.

9.3.8 *Recepción*

En un paso de **recepción**, un AU transporta un mensaje o informe a su usuario directo, o bien el sistema de comunicaciones que presta servicio a un usuario indirecto transporta ese objeto de información a dicho usuario. En cualquier caso, este paso transporta el objeto a su destino último.

Si se trata de un usuario directo, este paso sucede a la entrega del objeto o a la primera recuperación (solamente). Si se trata de un usuario indirecto, sucede al transporte de un objeto de información por el sistema de comunicaciones que sirve al usuario. En cualquiera de los dos casos, el usuario es un destinatario potencial (pero si es usuario directo, es destinatario no ya potencial sino efectivo) del mensaje objeto o la sonda objeto.

9.4 *Eventos de la transmisión*

En la primera columna del cuadro 6/X.402 se da una relación de los tipos de eventos que pueden producirse en una transmisión. Para cada tipo de evento se indica, en la segunda columna, los tipos de objetos de información, – mensajes, sondas e informes – para los que pueden desarrollarse tales eventos, y en la tercera columna, los tipos de objetos funcionales – usuarios, AU, MM, ATM y UA – a los que les está permitido desarrollarlos.

Todos los eventos se producen dentro del STRM.

CUADRO 6/X.402

Eventos de transmisión

Evento de transmisión	Objetos de información			Objetos funcionales				
	M	S	I	Usuario	UA	MM	ATM	AU
División	X	X	–	–	–	–	X	–
Combinación	X	X	X	–	–	–	X	–
Resolución de nombre	X	X	–	–	–	–	X	–
Ampliación de LD	X	–	–	–	–	–	X	–
Redireccionamiento	X	X	–	–	–	–	X	–
Conversión	X	X	–	–	–	–	X	–
No entrega	X	–	X	–	–	–	X	–
No afirmación	–	X	–	–	–	–	X	–
Afirmación	–	X	–	–	–	–	X	–
Encaminamiento	X	X	X	–	–	–	X	–

M Mensaje

S Sonda

I Informe

X Permitido

Los tipos de eventos de transmisión, resumidos en el cuadro 6/X.402 son definidos y descritos separadamente en los puntos que siguen.

9.4.1 *División*

En un evento de **división**, un ATM duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus destinatarios inmediatos. Este evento permite de manera efectiva a un ATM transportar independientemente un objeto a varios destinatarios potenciales.

Un ATM efectúa una división cuando el siguiente paso o evento, necesario para el transporte de una sonda o mensaje a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros.

9.4.2 *Combinación*

En un evento de **combinación**, un ATM combiña varios casos del mismo mensaje o sonda, o dos o más informes, de entrega y/o no entrega para el mismo mensaje o sonda objeto.

Un ATM puede, aunque no necesariamente, efectuar una combinación cuando determine que, para transportar a sus destinos varios objetos de información muy relacionados, hacen falta los mismos eventos y el mismo paso siguiente.

9.4.3 *Resolución de nombre*

En un evento de **resolución de nombre**, un ATM agrega la *dirección O/D* correspondiente al *nombre O/D* que identifica a uno de los destinatarios inmediatos de un mensaje o una sonda.

9.4.4 *Ampliación de LD*

En un evento de **ampliación de LD**, un ATM asigna una LD de entre los destinatarios de un mensaje (pero no de una sonda) a sus miembros, que de este modo se convierten en destinatarios miembros. Este evento elimina la falta de dirección de la especificación de los destinatarios inmediatos.

A una LD determinada se le somete a ampliación siempre en una localización preestablecida, dentro del STRM. Esta localización se llama **punto de ampliación** de la LD, y viene identificada por una *dirección O/D.*

El ATM puede generar, como parte de este evento, un informe de entrega.

La ampliación de la LD está sujeta al permiso de presentación. En el caso de una LD jerarquizada, ese permiso debe haber sido concedido a la LD de la que aquélla es miembro. De lo contrario, el permiso debe haber sido concedido al originador.

9.4.5 *Redireccionamiento*

En un evento de **redireccionamiento**, un ATM sustituye a un usuario o a una LD entre los destinatarios inmediatos de un mensaje o de una sonda, por un destinatario alternativo, especificado por el originador o asignado por el destinatario.

9.4.6 *Conversión*

En un evento de **conversión**, un ATM transforma partes del contenido de un mensaje de un TIC en otro, o altera una sonda de modo que parezca que los mensajes descritos fueron igualmente modificados. Este evento aumenta la probabilidad de que un objeto de información pueda ser entregado o afirmado, adaptándolo a sus destinatarios inmediatos.

Se distinguen los dos tipos de conversión que se indican a continuación, y que difieren en cómo se eligen el TIC de la información a convertir y el TIC resultante de la conversión:

a) **conversión explícita**: Conversión en la que el originador elige tanto el TIC inicial como el final.

b) **conversión implícita**: Conversión en la que el ATM elige los TIC finales, en función de los TIC iniciales y de las capacidades del AU.

9.4.7 *No entrega*

En un evento de **no entrega**, un ATM establece que el STRM no puede entregar un mensaje a sus destinatarios inmediatos, o no puede entregar un informe al originador de su mensaje o sonda objeto. Este evento detiene el transporte de un objeto al que el STRM considere intransportable.

En el caso de mensaje, el ATM genera, como parte de este evento, un informe de no entrega.

Un ATM efectúa una no entrega cuando, por ejemplo, determina que los destinatarios inmediatos no están especificados adecuadamente, que no aceptan la entrega de mensajes como el mensaje de que se trate, o que no se les ha entregado dentro de los límites de tiempo preestablecidos.

9.4.8 *No afirmación*

En un evento de **no afirmación**, un ATM establece que el STRM no puede entregar un mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda.

El ATM genera, como parte de ese evento, un informe de no entrega.

Un ATM produce una no afirmación cuando, por ejemplo, encuentra que los destinatarios inmediatos no están especificados adecuadamente o que no aceptarían la entrega de un mensaje descrito.

9.4.9 *Afirmación*

En un evento de **afirmación**, un ATM establece que el STRM puede entregar cualquier mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda y eleva a los destinatarios inmediatos a la categoría de destinatarios efectivos.

El ATM puede generar, como parte de este evento, un informe de entrega.

Un ATM produce una afirmación una vez que ha constatado que los destinatarios inmediatos están especificados adecuadamente y, si esos destinatarios son usuarios (pero no LD), que aceptarían la entrega de cualquier mensaje descrito. Si los destinatarios inmediatos son LD, el ATM producirá una afirmación si existe la LD y si el originador tiene el permiso de presentación pertinente.

9.4.10 *Encaminamiento*

En un evento de **encaminamiento**, un ATM selecciona el ATM «adyacente» al que transferirá un mensaje, sonda o informe. Este evento determina, de manera incremental, el camino de un objeto de información a través del STRM y, obviamente, sólo puede producir si el STRM consta de varios ATM.

Hay dos tipos de encaminamiento, que difieren entre sí por la clase de transferencia para la que preparan:

a) **encaminamiento interno**: Encaminamiento que prepara para una transferencia interna (es decir, una transferencia dentro de un *DG*).

b) **encaminamiento externo**: Encaminamiento que prepara para una transferencia externa (es decir, una transferencia entre distintos *DG*).

Un ATM realiza un encaminamiento cuando determina que no puede efectuar ningún otro evento ni dar ningún paso con respecto a un objeto.

10 Modelo de seguridad

En este punto se presenta un modelo de seguridad abstracto para la transferencia de mensajes. La realización concreta del modelo es tema de otras Recomendaciones de la serie. El modelo de seguridad proporciona un marco para la descripción de los servicios de seguridad que contrarrestan los riesgos potenciales (véase el anexo D) del STM, y de los elementos de seguridad que facilitan estos servicios.

Las características de seguridad constituyen una ampliación facultativa del STM, que pueden emplearse para minimizar el riesgo de exposición de bienes de capital y recursos a las infracciones de una política de seguridad (riesgos). Su objetivo es proporcionar seguridad con independencia de los servicios de comunicaciones proporcionados por otras entidades, de nivel superior o inferior. Los riesgos pueden combatirse mediante el recurso a la seguridad de tipo físico, la seguridad de los computadores (COMPUSEC) o los servicios de seguridad proporcionados por el STM. Según cuales sean los riesgos que se contemplen, se seleccionarán unos u otros servicios de seguridad de STM en combinación con adecuadas medidas de seguridad física y de COMPUSEC. Los servicios de seguridad facilitados por el STM se describen más adelante. La denominación y la estructuración de los servicios se basan en la norma ISO 7498-2.

Nota – A pesar de estas características de seguridad, pueden producirse ciertas agresiones contra las comunicaciones entre un usuario y el STM o contra las comunicaciones de usuario a usuario (por ejemplo, en el caso de usuarios que acceden al STM a través de una unidad de acceso, o de usuarios con acceso a distancia a sus AU). Para contrarrestar esas agresiones es preciso ampliar los servicios y modelos actuales de seguridad, lo que requiere *ulterior estudio.*

En muchos casos, la amplitud de los tipos de riesgos queda cubierta por varios de los servicios anotados.

Los servicios de seguridad se facilitan mediante el uso de elementos de servicio del sobre de mensajes del STRM. El sobre contiene argumentos propios de la seguridad, tal como se describe en la Recomendación X.411. La descripción de los servicios de seguridad que figura más adelante, se hace de la siguiente manera: en el § 10.2 se da una relación de los servicios con su definición e indicación, en cada caso, de cómo pueden ser proporcionados empleando los elementos de seguridad de la Recomendación X.411 y en el § 10.3 se describen uno a uno los elementos de seguridad con definición, en cada caso, del elemento de servicio, y referencias a sus argumentos constituyentes, según la Recomendación X.411.

Muchas de las técnicas empleadas se basan en mecanismos de cifrado. Los servicios de seguridad del STM permiten elegir los algoritmos con flexibilidad. Sin embargo, en algunos casos, sólo se ha definido totalmente en esta Recomendación la utilización del cifrado asimétrico. En una futura versión de la Recomendación se podrán utilizar mecanismos alternativos de cifrado simétrico.

Nota – Las expresiones «servicio de seguridad» y «elemento de seguridad» que se emplean en este punto no deben confundirse con las expresiones «elemento de servicio» y «servicio» empleadas en la Recomendación X.400. Las primeras expresiones se utilizan en este punto para mantener la armonía con ISO 7498-2.

10.1 *Políticas de seguridad*

Los servicios de seguridad del STM deben poder facilitar una amplia gama de políticas de seguridad, que va más allá de los límites del propio STM. Los servicios seleccionados y los riesgos contra los que se pretende asegurarse dependerán de la aplicación concreta y de los niveles de confianza que se tenga en las distintas partes del sistema.

La política de seguridad define cómo reducir a un nivel aceptable el riesgo de exposición al peligro de los bienes de capital.

Además será preciso el funcionamiento entre dominios diferentes, cada uno de ellos con su propia política de seguridad. Se deberán establecer acuerdos bilaterales sobre ese interfuncionamiento, ya que las políticas globales de seguridad, más amplias que la del mero STM, a que esos dominios estén sujetos, diferirán de todos modos entre sí. Debe definirse esto de tal manera que no se entre en conflicto con la política de seguridad de ninguno de los dos dominios y que el acuerdo llegue efectivamente a formar parte de la política de seguridad global de ambos.

10.2 *Servicio de seguridad*

Se definen en este punto los servicios de seguridad de la transferencia de mensajes. La denominación y la estructura de los mismos se basa en la norma ISO 7498-2.

Los servicios de seguridad de la transferencia de mensajes son de amplias y variadas clases. Esas clases, y los servicios correspondientes a cada una de ellas, aparecen relacionadas en el cuadro 7/X.402.

A lo largo de la serie de definiciones de servicios que viene a continuación se hace referencia a la figura 6/X.402, que representa el modelo funcional del STM de forma simplificada. En el texto se hace referencia en varias ocasiones a las etiquetas numeradas.

10.2.1 *Servicios de seguridad de autenticación de origen*

Estos servicios de seguridad facilitan la autenticación de la identidad de entidades pares comunicantes y de fuentes de datos.

10.2.2.1 *Servicios de seguridad de autenticación de origen de datos*

Estos servicios de seguridad permiten la confirmación del origen de un mensaje, una sonda o un informe a todas las entidades afectadas (es decir, los ATM o los usuarios del STRM destinatarios). No pueden proteger contra la duplicación de mensajes, sondas e informes.

10.2.1.1.1 *Servicio de seguridad de autenticación de origen de mensajes*

Este servicio de seguridad permite la confirmación del origen de un mensaje.

El servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de mensajes o el de integridad de argumento de mensajes. El primero se puede emplear para dar servicio de seguridad a cualquiera de las partes afectadas (1 a 5 inclusive, en la figura 6/X.402), mientras que el segundo sólo puede utilizarse para proporcionar servicio de seguridad a los usuarios del STRM (1 ó 5 en la figura 6/X.402). El elemento de seguridad elegido depende de la política de seguridad vigente.

10.2.1.1.2 *Servicio de seguridad de autenticación de origen de sondas*

El servicio de seguridad de autenticación de origen de sondas permite la confirmación del origen de una sonda.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de sondas. Puede emplearse el elemento de seguridad para dar el servicio a cualquiera de los ATM a través de los cuales se transfiere la sonda (2 a 4 inclusive, en la figura 6/X.402).

10.2.1.1.3 *Servicio de seguridad de autenticación de origen de informes*

El servicio de seguridad de autenticación de origen de informes permite la confirmación del origen de un informe.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de informes. El elemento de seguridad se emplea para dar servicio de seguridad al originador del mensaje o de la sonda objeto, así como a cualquiera de los ATM a través de los cuales se transfiere el informe (1 a 5 inclusive, en la figura 6/X.402).

CUADRO 7/X.402

Servicios de seguridad de la transferencia de mensajes

	Servicio							
	AU/ AU	AM/ ATM	ATM/ MM	ATM/ AU	AU/ MM	AU/ ATM	ATM/ ATM	MM/ AU
Autenticación de origen								
Autenticación de origen de mensajes	*	*	–	*	–	–	–	–
Autenticación de origen de sondas	–	–	*	*	–	–	–	–
Autenticación de origen de informes	–	–	–	–	*	*	*	–
Prueba de depósito	–	–	–	–	–	–	*	–
Prueba de entrega	*	–	–	–	–	–	–	a)
Gestión de acceso seguro								
Autenticación de entidades pares	–	*	*	*	*	*	*	*
Contexto de seguridad	–	*	*	*	*	*	*	*
Confidencialidad de datos								
Confidencialidad de conexiones	–	*	*	*	*	*	*	*
Confidencialidad de contenidos	*	–	–	–	–	–	–	–
Confidencialidad de flujo de mensajes	*	–	–	–	–	–	–	–
Servicios de integridad de datos								
Integridad de conexiones	–	*	*	*	*	*	*	*
Integridad de contenidos	*	–	–	–	–	–	–	–
Integridad de secuencia de mensajes	*	–	–	–	–	–	–	–
No rechazo								
No rechazo de origen	*	–	–	*	–	–	–	–
No rechazo de depósito	–	–	–	–	–	–	*	–
No rechazo de entrega	*	–	–	–	–	–	–	–
Etiquetado de mensajes de seguridad								
Etiquetado de mensajes de seguridad	*	*	*	*	*	*	*	*
Servicios de gestión de la seguridad								
Cambio de credenciales	–	*	–	*	*	*	*	–
Registros	–	*	–	*	–	–	–	–
Registros de la MM	–	*	–	–	–	–	–	–

* Un asterisco debajo de un encabezamiento del tipo *X/Y* significa que el servicio puede ser proporcionado desde un objeto funcional de tipo *X* a uno de tipo *Y*.

a) Este servicio lo proporciona la MM del destinatario al AU del originador.

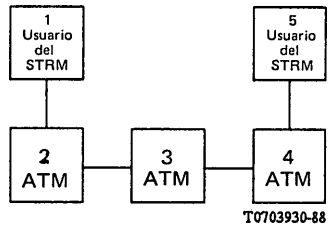


FIGURA 6/X.402

Modelo funcional de STM simplificado

10.2.1.2 *Servicio de seguridad de prueba de depósito*

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido recibido por el STRM para su entrega al destinatario o destinatarios especificados originalmente.

El servicio puede proporcionarse utilizando el elemento de seguridad de prueba de depósito.

10.2.1.3 *Servicio de seguridad de prueba de entrega*

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido entregado por el STRM al destinatario o destinatarios deseados.

El servicio puede proporcionarse utilizando el elemento de seguridad de prueba de entrega.

10.2.2 *Servicio de seguridad de gestión de acceso seguro*

El servicio de seguridad de gestión de acceso seguro se ocupa de la protección de los recursos contra su utilización no autorizada. Puede dividirse en dos componentes: servicio de autenticación de entidades pares y servicio de contexto de seguridad.

10.2.2.1 *Servicio de seguridad de autenticación de entidades pares*

Este servicio de seguridad se proporciona al establecer una conexión, para confirmar la identidad de la entidad que se conecta. Puede utilizarse en los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402 y asegura, al utilizarlo únicamente, contra los intentos de suplantación o de reactuación no autorizada de una conexión previa, por parte de una entidad.

El elemento de seguridad de intercambio de autenticación facilita este servicio. Téngase en cuenta que como consecuencia de la utilización de este elemento de seguridad, pueden liberarse otros datos, que en determinadas circunstancias podrían emplearse para facilitar un servicio de seguridad de confidencialidad de conexión y/o de integridad de conexión.

10.2.2.2 *Servicio de seguridad de contexto de seguridad*

Este servicio de seguridad se utiliza para limitar el alcance del paso de mensajes entre entidades, por referencia a las etiquetas de seguridad asociadas a los mensajes. Es un servicio que está, por tanto, en estrecha relación con el de seguridad de etiquetado de seguridad de mensajes, que permite la asociación de mensajes y etiquetas de seguridad.

Los elementos de seguridad de contexto de seguridad y registro facilitan el servicio de contexto de seguridad.

10.2.3 *Servicios de seguridad de confidencialidad de datos*

Estos servicios de seguridad protegen los datos contra su revelación no autorizada.

10.2.3.1 *Servicio de seguridad de confidencialidad de conexión*

El STM no presta un servicio de seguridad de confidencialidad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, como resultado del empleo del elemento de seguridad de intercambio de autenticación, para proporcionar el servicio de seguridad de autenticación de entidades pares. Este servicio de seguridad puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402.

10.2.3.2 *Servicio de seguridad de confidencialidad de contenido*

El servicio de seguridad de confidencialidad de contenido garantiza que el contenido de un mensaje sólo sea conocido por su emisor y su destinatario.

Es posible proporcionar este servicio mediante una combinación de los elementos de seguridad de confidencialidad de contenido y de confidencialidad de argumento de mensajes. Este último se puede emplear para transferir una clave secreta, utilizada con el primero en el cifrado del contenido del mensaje. Con estos elementos de seguridad, se proporciona el servicio desde el usuario 1 al usuario 5 del STRM, de la figura 6/X.402, siendo el mensaje ininteligible para los ATM.

10.2.3.3 *Servicio de seguridad de confidencialidad de flujo de mensajes*

Este servicio de seguridad protege contra la extracción de información que podría lograrse mediante la observación del flujo de mensajes. El STM proporciona este servicio sólo de forma limitada.

La técnica del sobre doble permite que un mensaje completo se convierta en contenido de otro mensaje. Esta técnica puede emplearse para ocultar la información de direccionamiento en determinados tramos del STRM. Junto con el rellano de tráfico (que queda fuera del objeto actual de esta Recomendación) podría utilizarse para lograr la confidencialidad del flujo de mensajes. Otros elementos de este servicio, tales como el control del encaminamiento o los pseudónimos, quedan también fuera del objeto de esta Recomendación.

10.2.4 *Servicios de seguridad de integridad de datos*

Estos servicios de seguridad se proporcionan para contrarrestar riesgos activos contra el STM.

10.2.4.1 *Servicio de seguridad de integridad de conexión*

El STM no presta un servicio de seguridad de integridad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, utilizando el elemento de seguridad de intercambio de autenticación en la prestación del servicio de seguridad de autenticación de entidades pares. El servicio puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402.

10.2.4.2 *Servicio de seguridad de integridad de contenido*

Este servicio de seguridad garantiza la integridad del contenido de un mensaje. Para ello, se habilita la determinación de si el contenido del mensaje ha sido o no modificado. El servicio no permite detectar reactuaciones de mensajes, lo que si es facilitado, en cambio, por el servicio de seguridad de integridad de secuencia de mensajes.

El servicio puede proporcionarse de dos modos diferentes, utilizando dos diferentes combinaciones de elementos de seguridad.

El elemento de seguridad de integridad de contenido junto con el de integridad de argumento de mensajes y, en algunos casos, el de confidencialidad de argumento de mensajes, pueden utilizarse para prestar servicio de seguridad a un destinatario de mensajes, es decir, para la comunicación del usuario 1 al usuario 5 del STRM, de la figura 6/X.402. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cual sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de argumento de mensajes se protege la verificación de integridad del contenido contra posibles cambios. La integridad de cualquier argumento de mensaje confidencial se garantiza utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

También puede emplearse el elemento de seguridad de autenticación de origen de mensajes para prestar este servicio de seguridad.

10.2.4.3 *Servicio de seguridad de integridad de secuencia de mensajes*

Este servicio de seguridad protege al originador y al destinatario de una secuencia de mensajes, contra el reordenamiento de la secuencia. Al mismo tiempo, protege contra la reactuación de mensajes.

Puede proporcionarse el servicio haciendo uso de una combinación de los elementos de seguridad de integridad de secuencia de mensajes y de integridad de argumento de mensajes. El primero da a cada mensaje un número de secuencia que puede protegerse contra posibles cambios mediante el segundo elemento. Es posible proporcionar simultáneamente confidencialidad e integridad del número de secuencia de mensajes, empleando el elemento de seguridad de confidencialidad de argumento de mensajes.

Estos elementos de seguridad facilitan el servicio para la comunicación del usuario 1 al usuario 5 del STRM, de la figura 6/X.402, y no a los ATM intermedios.

10.2.5 *Servicio de seguridad de no rechazo*

Estos servicios de seguridad dan garantía absoluta a un tercero, después de que el mensaje ha sido depositado, enviado o entregado, de que el depósito, el envío o la recepción se han producido tal como se dice. Téngase en cuenta que, para que esto funcione correctamente, la política de seguridad debe abarcar de manera explícita la gestión de claves asimétricas, a efectos de servicios de no rechazo, si se utilizan algoritmos asimétricos.

10.2.5.1 *Servicio de seguridad de no rehazo de origen*

Este servicio de seguridad da al destinatario o destinatarios de un mensaje garantía absoluta del origen del mismo, de su contenido y de su etiqueta de seguridad de mensaje asociada.

El servicio puede proporcionarse de dos modos diferentes, utilizando dos combinaciones distintas de elementos de seguridad. Téngase en cuenta que la prestación de este servicio es muy similar a la del servicio de seguridad de integridad de contenido (más débil).

El elemento de seguridad de integridad de contenido junto con el de integridad de argumento de mensajes y, en algunos casos, el de confidencialidad de argumento de mensajes, pueden utilizarse para prestar servicio de seguridad a un destinatario de mensajes, es decir, para la comunicación del usuario 1 al usuario 5 del STRM, de la figura 6/X.402. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cuál sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de mensajes se protege la verificación y, si hace falta, a la etiqueta de seguridad de mensajes, contra un posible cambio y/o rechazo. Cualquier argumento de mensaje confidencial queda protegido contra cambio y/o rechazo utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

Si no se requiere el servicio de seguridad de confidencialidad de contenido, también es posible emplear, como base de este servicio de seguridad, el elemento de seguridad de autenticación de origen de mensajes. En este caso puede proporcionarse el servicio de seguridad a todos los elementos del STM, es decir, a todos los usuarios del STRM y ATM de la figura 6/X.402.

10.2.5.2 *Servicio de seguridad de no rechazo de depósito*

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido depositado en el STRM para su entrega al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de depósito, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de depósito (más débil).

10.2.5.3 *Servicio de seguridad de no rechazo de entrega*

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido entregado al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de entrega, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de entrega (más débil).

10.2.6 *Servicio de seguridad del etiquetado de seguridad de mensajes*

Este servicio de seguridad permite asociar etiquetas de seguridad a todas las entidades del STM, es decir, los ATM y los usuarios del STRM. Conjuntamente con el servicio de seguridad de contexto de seguridad, facilita la ejecución de políticas de seguridad que precisen qué partes del STM pueden tratar mensajes, mediante las etiquetas de seguridad asociadas especificadas.

ARCHIVES U.I.T. GENÈVE

El servicio lo proporciona el elemento de seguridad de la etiqueta de seguridad de mensajes. Los elementos de seguridad de integridad de argumento de mensajes y de confidencialidad de argumento de mensajes aseguran la integridad y confidencialidad de la etiqueta.

10.2.7 *Servicio de gestión de la seguridad*

El STM necesita cierto número de servicios de gestión de seguridad. Los únicos servicios de gestión previstos en la Recomendación X.411 tratan del cambio de credenciales y del registro de etiquetas de seguridad de usuario del STRM.

10.2.7.1 *Servicio de seguridad de cambio de credenciales*

Este servicio de seguridad permite a una entidad del STM cambiar las credenciales que le afectan, contenidas en otra entidad del STM. Puede proporcionarse utilizando el elemento de seguridad de cambio de credenciales.

10.2.7.2 *Servicio de seguridad de registros*

Este servicio de seguridad permite el establecimiento en un ATM, de las etiquetas de seguridad autorizadas para un determinado usuario del STRM. Puede proporcionarse utilizando el elemento de seguridad de registros.

10.2.7.3 *Servicio de seguridad de registro de la MM*

Este servicio de seguridad permite el establecimiento de las etiquetas de seguridad que son admisibles para el usuario de la MM.

10.3 *Elementos de seguridad*

En los puntos que siguen se describen los elementos de seguridad, disponibles en los protocolos de la Recomendación X.411, para facilitar los servicios de seguridad en el STM. Esos elementos están relacionados directamente con los argumentos de varios servicios descritos en la Recomendación X.411. Este punto tiene por objeto extraer los elementos de las definiciones de servicios de la Recomendación X.411 que tienen relación con la seguridad, y definir la función de cada uno de esos elementos de seguridad identificados.

10.3.1 *Elementos de seguridad de autenticación*

Estos elementos de seguridad se definen para facilitar los servicios de seguridad de autenticación e integridad.

10.3.1.1 *Elementos de seguridad de intercambio de autenticación*

El elemento de seguridad de intercambio de autenticación está concebido para autenticar, posiblemente de manera mutua, la identidad de un usuario del STRM a un ATM, de un ATM a un ATM, de un ATM a un usuario del STRM de una MM a un AU o de un AU a una MM. Se basa en la utilización o el intercambio de datos secretos, tales como contraseñas o testigos cifrados asimétricamente o simétricamente. El resultado del intercambio es la confirmación de la identidad de la otra parte y, facultativamente, la transferencia de datos confidenciales que pueden utilizarse para la provisión del servicio de seguridad de confidencialidad de conexiones y/o de integridad de conexiones, en capas subyacentes. Dicha autenticación sólo es válida en el instante en que se produce, dependiendo la continuidad de la validez de la identidad autenticada de si se utiliza o no intercambio de datos confidenciales, o algún otro mecanismo, para establecer un trayecto de comunicación seguro. El establecimiento y uso de un trayecto de comunicación seguro está fuera del alcance de la presente Recomendación.

Este elemento de seguridad emplea el argumento de credenciales de iniciador y el resultado de credenciales de contestador de los servicios vinculados al STRM, a la MM y a un ATM. Las credenciales transferidas son contraseñas o testigos.

10.3.1.2 *Elementos de seguridad de autenticación de origen de datos*

Estos elementos de seguridad están concebidos de manera específica para facilitar los servicios de autenticación de origen de datos, aunque también se les puede emplear para proporcionar determinados servicios de integridad de datos.

10.3.1.2.1 *Elemento de seguridad de autenticación de origen de mensajes*

El elemento de seguridad de autenticación de origen de mensajes permite, a cualquiera que reciba o transfiera un mensaje, autenticar la identidad del usuario del STRM que originó el mensaje. Esto puede significar la prestación del servicio de seguridad de autenticación de origen de mensajes o del de no rechazo de origen.

El elemento de seguridad implica la transmisión, como parte de mensaje, de una verificación de autenticación de origen de mensajes, computada como una función del contenido del mensaje, del identificador de contenido de mensajes y de la etiqueta de seguridad de mensajes. Si también hace falta el servicio de seguridad de confidencialidad de contenido, el control de verificación se computa como una función del contenido del mensaje cifrado, en vez de una función del no cifrado. Actuando sobre el contenido del mensaje según es transportado en el mensaje global (es decir, después del elemento de seguridad facultativo de confidencialidad de contenido), cualquier entidad del STM puede verificar la integridad del mensaje global sin necesidad de ver el texto en claro del contenido del mensaje. No obstante, si se hace uso del servicio de seguridad de confidencialidad de contenido, no puede emplearse el elemento de seguridad de autenticación de origen de mensajes para proporcionar el servicio de seguridad de no rechazo de origen.

El elemento de seguridad utiliza la verificación de autenticación de origen de mensajes, que es uno de los argumentos de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.1.2.2 *Elemento de seguridad de autenticación de origen de sondas*

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de sondas permite a cualquier ATM autenticar la identidad del usuario del STRM que originó una determinada sonda.

Este elemento de seguridad utiliza la verificación de autenticación de origen de sondas, que es uno de los 5 argumentos del servicio de depósito de sondas.

10.3.1.2.3 *Elemento de seguridad de autenticación de origen de informes*

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de informes permite, a cualquier ATM o usuario del STRM que recibe un informe, autenticar la identidad del ATM que lo originó.

Este elemento de seguridad utiliza la verificación de autenticación de origen de informes, que es uno de los argumentos del servicio de entrega de informes.

10.3.1.3 *Elemento de seguridad de prueba de depósito*

Este elemento de seguridad proporciona al originador de un mensaje los medios para establecer que el mensaje fue aceptado por el STM para su transmisión.

El elemento de seguridad está constituido por dos argumentos: una petición de prueba de depósito enviada con un mensaje en el momento del depósio, y la prueba de depósito devuelta al usuario del STRM como parte de los resultados del depósito de mensajes. El STRM genera la prueba de depósito, que es computada como una función de todos los argumentos del mensaje depositado, del identificador de depósito de mensajes y del momento en que se produce el depósito de mensajes.

Puede utilizarse el argumento de prueba de depósito para facilitar el servicio de seguridad de prueba de depósitos. Dependiendo de cuál sea la política de seguridad en vigor, puede también facilitar el servicio de seguridad de no rechazo de depósito (más fuerte).

La petición de prueba de depósito es un argumento del servicio de depósito de mensajes. La prueba de depósito es uno de los resultados del servicio de depósito de mensajes.

10.3.1.4 *Elemento de seguridad de prueba de entrega*

Este elemento de seguridad proporciona al originador de un mensaje medios para establecer que el mensaje fue entregado en destino por el STM.

El elemento de seguridad está constituido por varios argumentos. El originador del mensaje incluye una petición de prueba de entrega en el mensaje depositado, y esta petición se entrega a cada destinatario con el mensaje. Un destinatario puede entonces computar la prueba de entrega como una función de un cierto número de argumentos asociados al mensaje. El STRM devuelve la prueba de entrega al originador del mensaje, como parte de un informe sobre los resultados del depósito de mensajes original.

Es posible utilizar la prueba de entrega para facilitar el servicio de seguridad de prueba de entrega. Dependiendo de cuál sea la política de seguridad en vigor, podría también facilitar el servicio de seguridad de no rechazo de entrega (más fuerte).

La petición de prueba de entrega es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes. La prueba de entrega es a la vez uno de los resultados del servicio de entrega de mensajes y uno de los argumentos de los servicios de transferencia de informes y de entrega de informes.

Nota – La no recepción de una prueba de entrega no implica la no entrega.

10.3.2 *Elementos de seguridad de gestión de acceso seguro*

Estos elementos de seguridad se definen para facilitar el servicio de seguridad de acceso seguro y los servicios de gestión de la seguridad.

10.3.2.1 *Elemento de seguridad de contexto de seguridad*

Cuando un usuario del STRM o un ATM se vincula a un ATM o a un usuario del STRM, la operación de vinculación especifica el contexto de seguridad de la conexión. Esto limita el alcance del paso de mensaje por referencia a las etiquetas asociadas a los mensajes. Además, el contexto de seguridad de la conexión puede ser alterado temporalmente para mensajes depositados o entregados.

El propio contexto de seguridad consta de una o más etiquetas de seguridad, que definen la sensibilidad de interacciones que pueden producirse, en línea con la política de seguridad en vigor.

El contexto de seguridad es un argumento de los servicios vinculados al STRM y a un ATM.

10.3.2.2 *Elemento de seguridad de registros*

El elemento de seguridad de registros permite el establecimiento en un ATM de etiquetas de seguridad autorizadas de un usuario del STRM.

El servicio de registros proporciona este elemento. Dicho servicio permite a un usuario del STRM cambiar los argumentos, contenidos en el STRM, relativos a la entrega de mensajes a ese usuario del STRM.

10.3.2.3 *Elemento de seguridad de registro de la MM*

El elemento de seguridad de registro de la MM permite el establecimiento de las etiquetas de seguridad admisibles del usuario de la MM.

El servicio de registro de la MM proporciona este elemento. Dicho servicio permite a un usuario de la MM cambiar los argumentos, contenidos en la MM, relativos a la recuperación de mensajes dirigidos a ese usuario de la MM.

10.3.3 *Elementos de seguridad de confidencialidad de datos*

A todos estos elementos de seguridad, basados en la utilización del cifrado, les afecta la provisión de la confidencialidad de los datos que pasan de una entidad del STM a otra.

10.3.3.1 *Elemento de seguridad de confidencialidad de contenidos*

El elemento de seguridad de confidencialidad de contenidos garantiza la protección del mensaje contra indiscreciones durante la transmisión, mediante un elemento de seguridad cifrado. El elemento de seguridad funciona de modo tal que solo el destinatario y el emisor del mensaje pueden conocer el texto en claro del contenido del mensaje.

La especificación del algoritmo de cifrado, la clave empleada y cualquier otro dato de inicialización, se transportan utilizando los elementos de seguridad de confidencialidad de argumento de mensajes y de integridad de argumento de mensajes. El algoritmo y la clave se emplean entonces para cifrar o descifrar los contenidos de los mensajes.

Este elemento de seguridad hace uso del identificador de algoritmo de confidencialidad de contenidos, que es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.3.2 *Elemento de seguridad de confidencialidad de argumento de mensajes*

El elemento de seguridad de confidencialidad de argumento de mensajes proporciona la confidencialidad, la integridad y, si hace falta, la irrevocabilidad de los datos de destinatario asociados a un mensaje. De manera específica, estos datos incluirán cuantas claves criptográficas y datos conexos hagan falta para el funcionamiento adecuado de los elementos de seguridad de confidencialidad e integridad, caso de que se invoquen esos elementos.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de confidencialidad de argumento de mensajes constituyen los datos cifrados, dentro del testigo de mensajes. Los datos cifrados del testigo de mensajes resultan ininteligibles para todos los ATM.

El testigo de mensajes es un argumento de los servicios de depósito de mensajes, de transferencia de mensajes y de entrega de mensajes.

10.3.4 *Elementos de seguridad de integridad de datos*

Estos elementos se proporcionan para facilitar la prestación de los servicios de integridad de datos, autenticación de datos y no rechazo.

10.3.4.1 *Elemento de seguridad de integridad de contenidos*

El elemento de seguridad de integridad de contenidos protege el contenido de un mensaje contra posibles modificaciones durante la transmisión.

Este elemento emplea uno o más algoritmos de criptografía. La especificación del algoritmo o algoritmos, la clave o claves utilizadas y cualquier otro dato de inicialización se transportan utilizando los elementos de seguridad de confidencialidad e integridad de argumento de mensajes. El resultado de la aplicación de los algoritmos y de la clave es la verificación de integridad de contenidos, que se envía en el sobre del mensaje. El elemento de seguridad sólo está disponible para el destinatario o destinatarios del mensaje, puesto que actúa en el texto en claro de los contenidos de los mensajes.

Si se protegiera el control de verificación de integridad de contenidos utilizando el elemento de seguridad de integridad de argumentos de mensajes, se le podría emplear, dependiendo de cuál fuese la política de seguridad en vigor, para facilitar la prestación del servicio de seguridad de no rechazo de origen.

El control de verificación de integridad de contenido es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.4.2 *Elemento de seguridad de integridad de argumento de mensajes*

El elemento de seguridad de integridad de argumento de mensajes proporciona la integridad y, si hace falta, la irrevocabilidad de determinados argumentos asociados a un mensaje. De manera específica, estos argumentos pueden comprender cualquier selección del identificador de algoritmo de confidencialidad de contenidos, del control de verificación de integridad de contenidos, de la etiqueta de seguridad de mensajes, de la petición de prueba de entrega y del número de secuencia de mensajes.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de integridad de argumento de mensajes constituyen los datos firmados, dentro del testigo de mensajes.

El testigo de mensajes es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.4.3 *Elemento de seguridad de integridad de secuencia de mensajes*

El elemento de seguridad de integridad de secuencia de mensajes protege al emisor y al destinatario de un mensaje contra la recepción de mensajes desordenados o duplicados.

Cada mensaje tiene asociado un número de secuencia de mensajes. Este número identifica la posición de un mensaje en una secuencia, desde el originador al destinatario. Así pues, cada pareja originador-destinatario que necesite utilizar este elemento de seguridad deberá mantener una secuencia precisa de números de mensajes. Este elemento de seguridad no facilita la inicialización o sincronización de números de secuencia de mensajes.

10.3.5 *Elementos de seguridad de no rechazo*

En la Recomendación X.411 no se definen, de manera específica, los elementos de seguridad de no rechazo. Los servicios de no rechazo pueden proporcionarse mediante una combinación de otros elementos de seguridad.

10.3.6 *Elementos de seguridad de la etiqueta de seguridad*

La finalidad de estos elementos de seguridad es facilitar el etiquetado de seguridad en el STM.

10.3.6.1 *Elemento de seguridad de etiqueta de seguridad de mensajes*

Se pueden etiquetar los mensajes con datos según se especifique en la política de seguridad vigente. La etiqueta de seguridad de mensajes está a disposición de los ATM intermedios, como parte de la política de seguridad global del sistema.

Es posible enviar una etiqueta de seguridad de mensajes como un argumento de mensajes y que sea protegida por el elemento de seguridad de integridad de argumento de mensajes o el de autenticación de origen de mensajes, del mismo modo que otros argumentos de mensajes.

Si son necesarias, tanto la confidencialidad como la integridad, se puede proteger la etiqueta de seguridad de mensajes, de manera alternativa, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. En este caso, la etiqueta así protegida es un argumento de originador-destinatario, y puede diferir de la etiqueta de seguridad de mensajes en la envolvente del mensaje.

10.3.7 *Elemento de seguridad de gestión de la seguridad*

10.3.7.1 *Elemento de seguridad de cambio de credenciales*

El elemento de seguridad de cambio de credenciales permite actualizar las credenciales de un usuario del STRM o de un ATM.

El elemento de seguridad lo proporciona el servicio de cambio de credenciales del STRM.

10.3.8 *Técnica del sobre doble*

Es posible dar protección adicional a un mensaje completo, incluidos los parámetros del sobre, especificando que el contenido de un mensaje es, en sí mismo, un mensaje completo, es decir, que se dispone de una técnica de doble sobre.

Se puede recurrir a esta técnica aunque se utilice el argumento del tipo de contenido, que permite especificar que el contenido de un mensaje es un sobre interno. Ese tipo de contenido significa que el contenido es, por sí mismo, un mensaje (sobre y contenido) que el destinatario indicado en el sobre externo debe reexpedir al destinatario indicado en el sobre interno.

El tipo de contenido es un argumento de los servicios de depósito, transferencia y entrega de mensajes.

SECCIÓN 3 – CONFIGURACIONES

11 Visión de conjunto

En esta sección se especifica cómo configurar el STM para satisfacer cualquiera de los diversos requisitos de tipo funcional, físico y organizativo.

La sección abarca los siguientes temas:

a) configuraciones funcionales;
b) configuraciones físicas;
c) configuraciones organizativas;
d) el *STM global.*

12 Configuraciones funcionales

Se especifican en este punto las posibles configuraciones funcionales del STM. La variedad de tales configuraciones está en relación directa con la presencia o ausencia de la guía y con la utilización o no, por parte de un usuario directo, de una MM.

12.1 *Respecto a la guía*

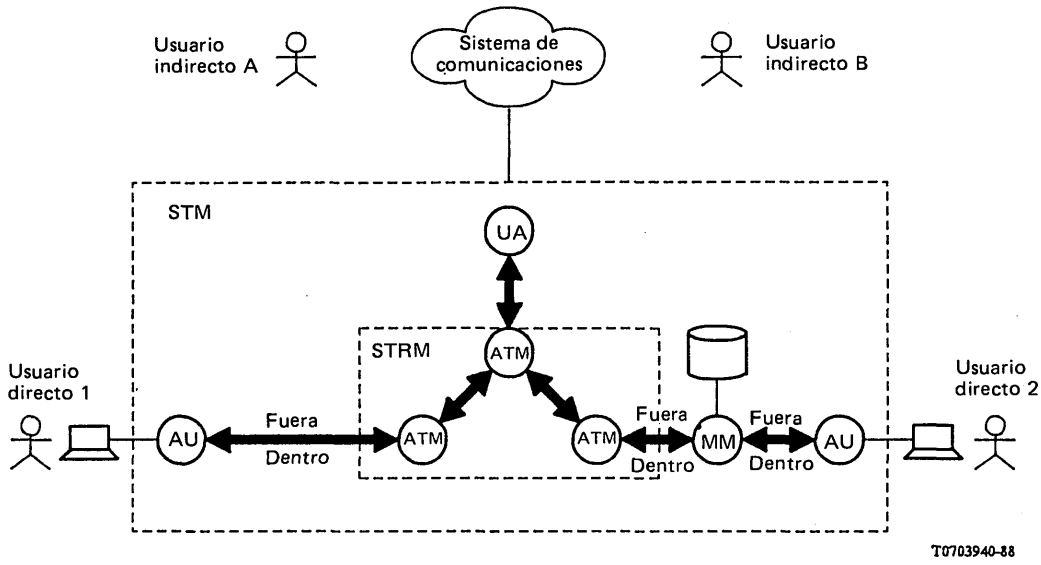
Con respecto a la guía, el STM puede configurarse para un usuario, o colectivo de usuarios (véase por ejemplo, el § 14.1), de dos maneras distintas: con la guía o sin ella. Un usuario sin acceso a la guía carecerá de las capacidades descritas en la sección cinco.

Nota – Es posible que durante un cierto periodo de tiempo exista una guía no plenamente interconectada, sino sólo parcialmente, mientras se elabora la guía (global) que hacen posible las Recomendaciones sobre guías.

12.2 *Respecto a la memoria de mensajes*

Con respecto a la MM, el STM puede configurarse, para un usuario directo particular, de dos maneras distintas: con MM o sin ella. Un usuario sin acceso a una MM no tiene capacidad de almacenar mensajes. En tal circunstancia, dependerá de su AU para el almacenamiento de objetos de información, con una capacidad que será un asunto local.

Las dos configuraciones funcionales identificadas anteriormente, se representan de manera esquemática en la figura 7/X.402, que ilustra además una posible configuración del STRM y su vinculación a otro sistema de comunicaciones a través de un AU. En esta figura, el usuario 2 está equipado con una MM, mientras que el usuario 1 no lo está.



Nota – Aunque los usuarios representados en esta figura son personas, ésta es aplicable con igual vigencia y validez a otras clases de usuarios.

FIGURA 7/X.402

Configuraciones funcionales respecto a la MM

13 Configuraciones físicas

En este punto se especifican las posibles configuraciones físicas del STM, es decir, cómo puede realizarse el STM como un conjunto de sistemas de computadores interconectados. Puesto que el número de configuraciones es ilimitado, los *sistemas de mensajería* se describen a partir de los cuales se construye el STM, y se identifican unas cuantas configuraciones representativas importantes.

13.1 *Sistemas de mensajería*

A las unidades elementales utilizadas en la construcción física del STM se les denomina *sistemas de mensajería.* Un **sistema de mesajería** es un sistema por computador (posiblemente, aunque no necesariamente, un sistema abierto) que contiene, o realiza, uno o más objetos funcionales.

Los sistemas de mensajería son de los tipos que se representan de manera esquemática en la figura 8/X.402.

En la primera columna del cuadro 8/X.402 se da una relación de los tipos de sistemas de mensajería representados en la figura 8/X.402. Para cada tipo de esa relación, la segunda columna indica las clases de objetos funcionales – AU, MM, ATM y UA – que pueden estar presentes en dicho sistema de mensajería, si su presencia es obligatoria o facultativa y si el sistema de mensajería consta simplemente de uno o posiblemente de múltiples objetos.

El cuadro 8/X.402 está dividido en dos secciones. Los sistemas de mensajería de los tipos de la primera sección prestan servicio a un solo usuario, mientras que los de la segunda pueden prestar servicio a un solo usuario o a varios usuarios.

Nota – Para la admisión de tipos de sistemas de mensajería se han tenido en cuenta los siguientes principios fundamentales:

a) Una UA y el ATM con el que interactúa se hallan típicamente ubicados en la misma posición, puesto que no se ha normalizado ningún protocolo que gobierne su interacción.

b) Un ATM se halla típicamente coubicado con múltiples AU o MM, porque, de los protocolos normalizados, sólo el de transferencia lleva un mensaje simultáneamente a destinatarios múltiples. La entrega en serie de un mensaje a destinatarios múltiples servidos por un sistema de mensajería, tal como exigiría el protocolo de entrega, resultaría ineficaz.

c) Nada se consigue ubicando varios ATM en el mismo emplazamiento, en un sistema de mensajería, puesto que un solo ATM presta servicio a múltiples usuarios, y la finalidad de un ATM es transportar objetos funcionales entre sistemas y no dentro de tales sistemas (con esto no se pretende excluir la posibilidad de que varios procesos relacionados con un ATM coexistan en un único sistema por computador).

d) La coubicación de una UA con un ATM no afecta al comportamiento del sistema con respecto al resto del STM. Un solo tipo de sistema de mensajería abarca, por tanto, la presencia y la ausencia de la UA.

Los tipos de sistemas de mensajería expuestos de manera resumida en el cuadro 8/X.402 se definen y describen en los puntos siguientes.

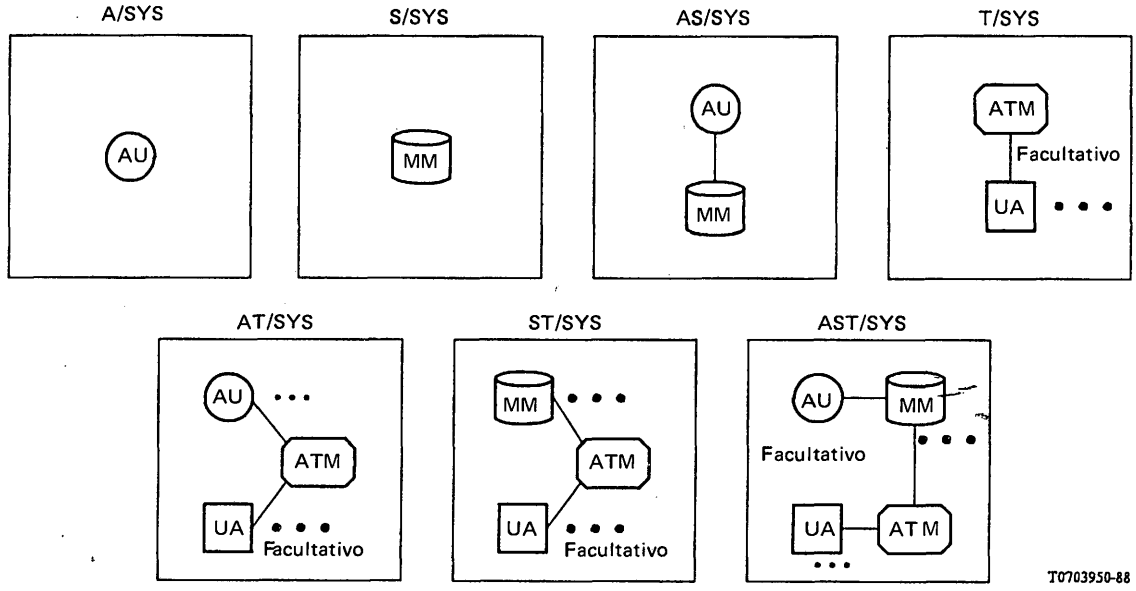


FIGURA 8/X.402

Tipos de sistemas de mensajería

CUADRO 8/X.402

Sistemas de mensajería

Sistema de mensajería	Objetos funcionales			
	AU	MM	ATM	UA
A/SYS	1	–	–	–
S/SYS	–	1	–	–
AS/SYS	1	1	–	–
T/SYS	–	–	1	[M]
AT/SYS	M	–	1	[M]
ST/SYS	–	M	1	[M]
AST/SYS	M	M	1	[M]

M Mútiple

[...] Facultativo

13.1.1 *Sistemas de acceso*

Un **sistema de acceso (A/SYS)** contiene un AU, pero no una MM ni un ATM ni una UA.

Un A/SYS se dedica a un único usuario.

13.1.2 *Sistemas de almacenamiento*

Un **sistema de almacenamiento (S/SYS)** contiene una MM, pero no un AU ni un ATM ni una UA.

Un S/SYS se dedica a un único usuario.

13.1.3 *Sistemas de acceso y almacenamiento*

Un **sistema de acceso y almacenamiento (AS/SYS)** contiene un AU, y una MM, pero no un ATM ni una UA.

Un AS/SYS se dedica a un único usuario.

13.1.4 *Sistemas de transferencia*

Un **sistema de transferencia (T/SYS)** contiene un ATM, facultativamente, una o más UA, pero no un AU ni una MM.

Un T/SYS puede prestar servicio a múltiples usuarios.

13.1.5 *Sistemas de acceso y transferencia*

Un **sistema de acceso y transferencia (AT/SYS)** contiene uno o más AU, un ATM y, facultativamente, una o más UA, pero no una MM.

Un AT/SYS puede prestar servicio a múltiples usuarios.

13.1.6 *Sistemas de almacenamiento y transferencia*

Un **sistema de almacenamiento y transferencia (ST/SYS)** contiene una o más MM, un ATM y facultativamente, una o más UA, pero no AU.

Un AST/SYS puede prestar servicio a múltiples usuarios.

13.1.7 *Sistema de acceso, almacenamiento y transferencia*

Un **sistema de acceso, almacenamiento y transferencia (AST/SYS)** contiene uno o más AU, una o más MM, un ATM y facultativamente, una o más UA.

Un AST/SYS puede prestar servicio a múltiples usuarios.

13.2 *Configuraciones representativas*

Los sistemas de mensajería pueden combinarse de diversas maneras para constituir el STM. Las configuraciones físicas posibles son ilimitadas, y por ello no pueden ser enumeradas. De todos modos, en la figura 9/X.402 y en los puntos que siguen, se describen varias configuraciones representativas importantes.

13.2.1 *Totalmente centralizada*

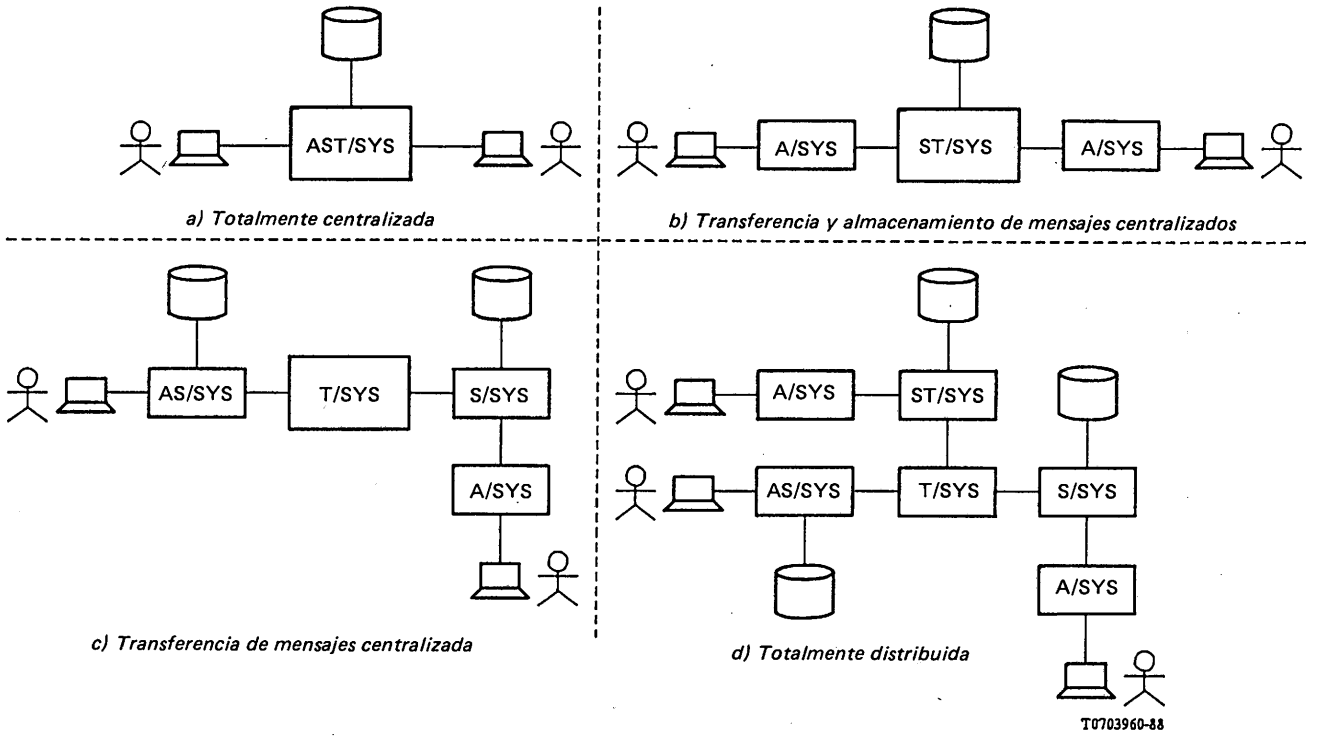
El STM puede estar totalmente centralizado [caso a) de la figura 9/X.402]. Este diseño se realiza mediante un único AST/SYS que contiene objetos funcionales de todas clases y que puede prestar servicio a múltiples usuarios.

13.2.2 *Transferencia y almacenamiento de mensajes centralizados*

El STM puede proporcionar transferencia y almacenamiento de mensajes centralmente, pero con acceso distribuido de los usuarios [caso b) de la figura 9/X.402]. Este diseño se realiza mediante un único ST/SYS y, por cada usuario, un A/SYS.

13.2.3 *Transferencia de mensajes centralizada*

El STM puede proporcionar transferencia de mensajes centralmente, pero con almacenamiento de mensajes y acceso de usuarios distribuidos [caso c) de la figura 9/X.402]. Este diseño se realiza mediante un único T/SYS y, por cada usuario, un A/SYS sólo o un S/SYS con un A/SYS asociado.



Nota 1 – Aunque los usuarios representados en esta figura son personas, ésta es aplicable con igual vigencia y validez a otras clases de usuarios.

Nota 2 – Además de las configuraciones físicas resultantes de los planteamientos «puros» que a continuación se indican, pueden construirse muchas configuraciones de carácter «híbrido».

FIGURA 9/X.402

Configuraciones físicas representativas

13.2.4 *Totalmente distribuida*

El STM puede proporcionar transferencia de mensajes incluso de manera distribuida [caso d) de la figura 9/X.402]. Este diseño implica múltiples ST/SYS o T/SYS.

14 Configuraciones organizativas

En este punto se especifican las configuraciones organizativas posibles del STM, es decir, cómo puede realizarse el STM en forma de conjuntos de sistemas de mensajería interconectados, pero gestionados independientemente (estando los propios sistemas conectados entre sí). Como el número de configuraciones es ilimitado, se describen los tipos de *dominios de gestión* a partir de los cuales se construye el STM, y se identifican unas cuantas configuraciones representativas importantes.

14.1 *Dominios de gestión*

A los bloques primarios, utilizados en la construcción de STM, se les denomina *dominios de gestión.* Un **dominio de gestión (DG)** (o **dominio**) es un conjunto de sistemas de mensajería – por lo menos uno, que contenga o realice un ATM – gestionado por una única organización.

Lo anterior no impide que una organización gestione un conjunto de sistemas de mensajería (por ejemplo, un solo A/SYS) que no tiene categoría de DG por falta de un ATM. Ese grupo de sistemas de mensajería, bloque secundario utilizado en la construcción del STM, son de la «incumbencia» de un DG.

Los DG son de varios tipos, cada uno de los cuales se define y describe en los puntos que siguen.

14.1.1 *Dominio de gestión de administración*

Un **dominio de gestión de administración (DGAD)** comprende varios sistemas de mensajería gestionados por una Administración. La distinción técnica principal entre un DGAD y un *DGPR* es que el primero se halla por encima del segundo en los regímenes jerárquicos de direccionamiento (véase el § 18) y encaminamiento (véase el § 19) del STM.

Nota – Un DGAD proporciona tratamiento de mensajes al público.

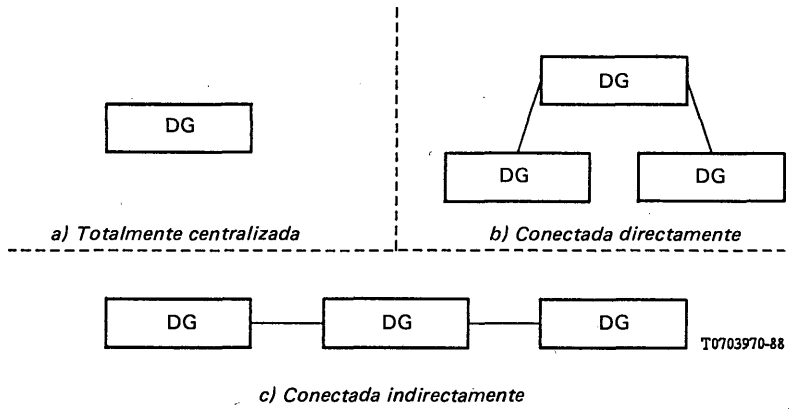
14.1.2 *Dominio de gestión privado*

Un **dominio de gestión privado (DGPR)** comprende sistemas de mensajería gestionados por una organización distinta de una Administración. La distinción técnica principal entre un DGPR y un DGAD es que el primero se halla por debajo del segundo en los regímenes jerárquicos de direccionamiento (véase el § 18) y encaminamiento (véase el § 19) del STM.

Nota – Un DGPR proporciona tratamiento de mensajes, por ejemplo, a los empleados de una compañía, o a esos empleados en un determinado emplazamiento de la compañía.

14.2 *Configuraciones representativas*

Los DG pueden combinarse de diversas maneras para constituir el STM. Las configuraciones organizativas posibles son ilimitadas, y por ello no pueden enumerarse. De todos modos, en la figura 10/X.402 y en los puntos que siguen se describen varias configuraciones representativas importantes.



Nota – Además de las configuraciones organizativas resultantes de los planteamientos «puros» que a continuación se indican, pueden construirse muchas otras organizaciones de carácter «híbrido».

FIGURA 10/X.402

Configuraciones organizativas representativas

14.2.1 *Totalmente centralizada*

Todo el STM puede ser gestionado por una organización [caso a) de la figura 10/X.402]. Este diseño se realiza mediante un único DG.

14.2.2 *Conectada directamente*

El STM puede ser gestionado por varias organizaciones, estando los sistemas de mensajería de cada una de ellas conectados a los sistemas de mensajería de todas las demás [caso b) de la figura 10/X.402]. Este diseño se realiza mediante múltiples DG interconectados por pares.

14.2.3 *Conectada indirectamente*

El STM puede ser gestionado por varias organizaciones, actuando los sistemas de mensajería de una como intermediarios entre los sistemas de mensajería de las otras [caso c) de la figura 10/X.402]. Este diseño se realiza mediante múltiples DG uno de los cuales está interconectado con todos los demás.

15 El STM global

Uno de los principales objetivos de esta Recomendación y de otras de la serie es facilitar la construcción del STM global, un STM que permita el tratamiento de mensajes intra e interorganizativo, y también intra e internacional, a escala mundial.

El STM global abarca, casi con toda seguridad, la gama completa de configuraciones funcionales especificadas en el § 12.

La configuración física del STM global es un híbrido de las configuraciones puras especificadas en el § 13, sumamente complejo y con un alto grado de distribución física.

La configuración organizativa del STM global es una combinación híbrida de las configuraciones puras especificadas en el § 14, sumamente compleja y con un alto grado de distribución organizativa.

En la figura 11/X.402 se da un ejemplo de posibles interconexiones, que no pretende identificar todas las configuraciones posibles. Tal como se indica en la figura 11/X.402 los DGAD juegan un papel central en el STM global. Mediante su interconexión internacional se constituye la columna vertebral de la transferencia de mensajes. Interconectándolos a nivel nacional, y dependiendo de cuáles sean los reglamentos nacionales, pueden también proporcionar entramados básicos, a ese mismo nivel, unidos al entramado internacional. Los DGAD sirven también como primera autoridad de denominación, en la *asignación de direcciones O/D* a usuarios y LD.

Los DGPR desempeñan un contenido más bien periférico en el STM global, estando conectados al eje central de los DGAD, que actúa de intermediario entre ellos.

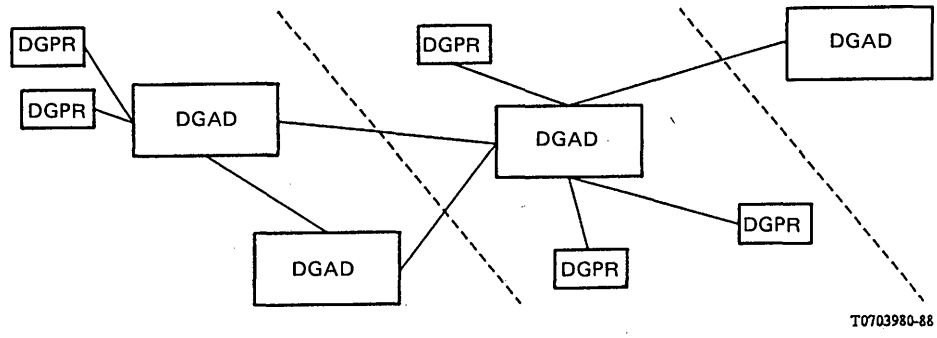


FIGURA 11/X.402

El STM global

SECCIÓN 4 – DENOMINACIÓN, DIRECCIONAMIENTO Y ENCAMINAMIENTO

16 Vision de conjunto

En esta sección se describen la denominación y el direccionamiento de usuarios y LD, y el encaminamiento hacia ellos de objetos de información.

La sección comprende los siguientes temas:

a) denominación;
b) direccionamiento;
c) encaminamiento.

17 Denominación

En este punto se especifica cómo se denomina a los usuarios y LD a efectos de tratamiento de mensajes en general y transferencia de mensajes en particular. Se definen los *nombres O/D* y se describe el papel que desempeñan en ellos los nombres de guía.

Cuando un AU o una MM depositan un mensaje o una sonda, identifican al STRM los destinatarios potenciales. Cuando el STRM entrega un mensaje, identifica el originador a cada AU o MM del destinatario potencial. Los *nombres O/D* son las estructuras de datos por medio de las cuales se realiza esa identificación.

17.1 *Nombres de guía*

Un nombre de guía es un componente de un *nombre O/D*. El nombre de guía identifica un objeto a la guía. Presentando ese nombre a la guía, el STM puede acceder la inscripción en la guía de un usuario o una LD. El STRM obtiene de esa inscripción, por ejemplo, la *dirección O/D* del usuario o de la LD.

No todos los usuarios o LD están inscritos en la guía y, por consiguiente, no todos ellos tienen un nombre de guía.

Nota 1 – Muchos usuarios y LD carecerán de nombre de guía mientras no se generalice la difusión de ésta, como elemento auxiliar del STM. Gran número de usuarios indirectos (por ejemplo, patrones postales) no tendrán tales nombres mientras no se disponga ampliamente de la guía, como un adjunto a otros sistemas de comunicación.

Nota 2 – A los usuarios y a las LD se les puede asignar nombres de guía incluso antes de que se ponga en marcha una guía interconectada y distribuida, preestableciendo las autoridades de denominación, de las que dependerá la guía en su momento.

Nota 3 – El nombre *de guía típico le resulta más cómodo y estable al usuario que la dirección O/D típica* porque la segunda está expresada necesariamente desde el punto de vista de la estructura organizativa o física del STM, mientras que el primero no lo está. Se pretende por ello que, con el tiempo, los nombres de guía se conviertan necesariamente en el principal medio de identificación de los usuarios y las LD fuera del STM (es decir, por otros usuarios), y que el empleo de las *direcciones O/D* se limite en gran medida al STRM (es decir, por los ATM).

17.2 *Nombres O/D*

Cada usuario o LD tiene uno o más *nombres O/D*. Un **nombre O/D** es un identificador por medio del cual puede un usuario ser designado como originador, o un usuario o una LD ser designados como destinatario potencial de un mensaje o sonda. El nombre O/D distingue a un usuario o una LD de otro, y puede identificar además su punto de acceso al STM.

Un nombre O/D incluye un nombre de guía, una *dirección O/D* o ambas cosas. Si está presente y es válido, el nombre de guía identifica de manera inequívoca al usuario o a la LD (aunque no es necesariamente el único que podrá hacerlo). La *dirección O/D*, cuando existe, hace eso mismo y más (véase el § 18.5).

En depósito directo, el AU o la MM del originador de un mensaje o sonda pueden incluir cualquiera de los dos componentes, o ambos, en cada nombre O/D que suministran. Si se omite la *dirección O/D*, el STRM la obtiene a partir de la guía, utilizando el nombre de guía. Si se omite el nombre de guía, el STRM prescinde de él. Si se incluyen ambos, el STRM confía en primer lugar en la *dirección O/D*. Si constatara que la *dirección O/D* era inválida (por ejemplo, porque se hubiera quedado obsoleta), procedería como si la *dirección O/D* hubiera sido omitida, confiando en el nombre de guía.

En entrega, el STRM incluye una *dirección O/D* y posiblemente un nombre de guía en cada nombre O/D que suministra al destinatario de un mensaje o al originador de un mensaje o sonda objeto de un informe. El nombre de guía se incluye si el originador lo ha suministrado, o si se identificó como miembro de una LD ampliada.

Nota – La redirección o la ampliación de LD pueden dar lugar a que el STRM lleve a un AU o a una MM en entrega, nombres O/D que el AU o la MM no suministraron en depósito directo.

18 Direccionamiento

En este punto se especifica la manera de direccionar a usuarios y LD. Se definen las *direcciones O/D*, se describe la estructura de las *listas de atributos* a partir de las que se elaboran, se examinan los conjuntos de caracteres con los que se componen los *atributos* individuales, se dan reglas para determinar si dos *listas de atributos* son equivalentes y para la inclusión de *atributos* condicionales en tales listas y se definen los *atributos normalizados* que pueden figurar en ellas.

Para transportar un mensaje, una sonda o un informe a un usuario, o para ampliar una LD especificada como destinatario potencial de un mensaje o una sonda, el STRM debe localizar el usuario o la LD relativos a sus propias estructuras física y organizativa. Las *direcciones O/D* son las estructuras de datos mediante las cuales se realizan todas estas localizaciones.

18.1 *Lista de atributos*

Las *direcciones O/D* de usuarios y LD son listas de atributos. Una **lista de atributos** es un conjunto ordenado de *atributos.*

Un **atributo** es un elemento de información que describe a un usuario o LD y que puede también ubicarlo en relación con la estructura física y organizativa del STM (o la red inherente al mismo).

Un atributo consta de las siguientes partes:

a) **tipo de atributo (o tipo)**: Identificador que indica una clase de información (por ejemplo, nombres personales).

b) **valor de atributo (o valor)**: Ejemplo de la clase de información indicada por el tipo de atributo (por ejemplo, un nombre personal).

Los atributos son de las dos clases siguientes:

a) **atributo normalizado**: Atributo cuyo tipo está vinculado a una clase de información por esta Recomendación.

El valor de cada atributo normalizado, excepto el del *tipo-terminal,* es una cadena o bien un grupo de cadenas.

b) **atributo definido por el dominio**: Atributo cuyo tipo está vinculado a una clase de información por un DG.

Tanto el tipo como el valor de cada atributo definido por el dominio son cadenas o grupos de cadenas.

Nota – El uso generalizado de atributos normalizados genera direcciones O/D más uniformes y por tanto más cómodas para el usuario. No obstante, es de prever que no todos los DG serán capaces de emplear tales atributos inmediatamente. La finalidad de los atributos definidos por el dominio es permitir a un DG que retenga durante cierto tiempo los convenios primitivos de direccionamiento existentes. Se pretende sin embargo, que todos los DG tiendan al empleo de atributos normalizados, y que los atributos definidos por el dominio se utilicen sólo con carácter provisional.

18.2 *Juegos de caracteres*

Los valores de atributos normalizados y los tipos y valores de atributos definidos por el dominio se elaboran a partir de cadenas numéricas, imprimibles y teletex, según los siguientes criterios:

a) El tipo o valor de un determinado atributo definido por el dominio puede ser una cadena imprimible, una cadena teletex o ambas. Se elegirá lo mismo para el tipo y para el valor.

b) Las clases de cadenas con las que pueden elaborarse valores de atributos normalizados y la manera de elaborarlos (por ejemplo, como una sola cadena o varias) difiere de un atributo a otro (véase el § 18.3).

El valor de un atributo consta de cadenas de una de las siguientes variedades, dependiendo de su tipo: numérico sólo, imprimible sólo, numérico e imprimible e imprimible y teletex. En relación con esto, las siguientes reglas gobiernan cada caso de comunicación:

a) Donde se permitan cadenas tanto numéricas como imprimibles, podrán suministrarse indiferentemente cadenas de una u otra variedad (pero no de ambas).

b) Donde se permitan cadenas tanto imprimibles como teletex, podrán suministrarse cadenas de una u otra variedad, o de ambas, pero las cadenas imprimibles se suministrarán lo menos posible cuando se transporten los atributos internacionalmente. Si se suministran cadenas tanto imprimibles como teletex, ambas deberán transportar la misma información, de tal modo que en la recepción pueda ignorarse una de las dos sin pérdida de seguridad.

La longitud de cada cadena y de cada secuencia de cadenas en un atributo se limitará tal como se indica en la especificación más detallada de atributos (por ejemplo, NSA.1) de la Recomendación X.411.

Nota 1 – Se permiten las cadenas teletex en valores de atributos para facilitar la inclusión, por ejemplo, de caracteres acentuados, utilizados normalmente en muchos países.

Nota 2 – No todos los dispositivos de entrada/salida permiten la introducción y visualización, por ejemplo, de caracteres acentuados. Las cadenas imprimibles son necesarias, a nivel internacional, para asegurar que esas limitaciones de los dispositivos no impiden la comunicación.

18.3 *Atributo normalizados*

En la primera columna del cuadro 9/X.402 figura la lista de tipos de atributos normalizados. Para cada tipo enumerado se indican en la segunda columna los conjuntos de caracteres – numéricos, imprimibles y teletex – con los que está permitido elaborar valores de atributos.

El cuadro 9/X.402 tiene tres secciones. Los tipos de atributos de la primera son de naturaleza general, los de la segunda están relacionados con el *encaminamiento a* un SEF y los de la tercera, con el *direccionamiento dentro de* un SEF.

CUADRO 9/X.402

Atributos normalizados

Tipo de atributo normalizado	Juego de caracteres		
	NUM	IMP	TTX
General			
Nombre-dominio-administración	×	×	–
Nombre-común	–	×	×
Nombre-país	×	×	–
Dirección-red	× [a]	–	–
Identificador-usuario-numérico	×	–	–
Nombre-organización	–	×	×
Nombre-unidades-organización	–	×	×
Nombre-personal	–	×	×
Nombre-dominio-privado	×	×	–
Identificador-terminal	–	×	–
Tipo-terminal	–	–	–
Encaminamiento postal			
Nombre-servicio-entrega-física	–	×	–
Nombre-país-entrega-física	×	×	–
Código-postal	×	×	–
Direccionamiento postal			
Componentes-ampliación-dirección-O/D postal	–	×	×
Componentes-ampliación-entrega-física	–	×	×
Atributos-postales-locales	–	×	×
Nombre-oficina-entrega-física	–	×	×
Número-oficina-entrega-física	–	×	×
Nombre-organización-entrega-física	–	×	×
Nombre-personal-entrega-física	–	×	×
Dirección-apartado-correos	–	×	×
Dirección-lista-correos	–	×	×
Dirección-calle	–	×	×
Dirección-postal-no-formatizada	–	×	×
Nombre-postal-exclusivo	–	×	×

NUM Numérico

IMP Imprimible

TTX Teletex

× Permitido

[a] En determinadas circunstancias, una secuencia de cadenas de octetos

Los tipos de atributos normalizados, resumidos en el cuadro 9/X.402, se definen y describen individualmente en los puntos que siguen.

18.3.1 *Nombre-dominio-administración*

Nombre-dominio-administración es un atributo normalizado que identifica un DGAD relativo al país indicado por un nombre-país.

El valor de este atributo es una cadena numérica o imprimible, elegida de entre un conjunto de tales cadenas administrado para este fin por el país aludido anteriormente.

Nota – El valor de atributo que consta de un único espacio (« ») se reservará para los siguientes fines. *Si lo permite* el país indicado por el atributo de nombre-país, un único espacio designará cualquiera (es decir, todos) los DGAD dentro del país. Esto afecta tanto a la identificación de usuarios dentro del país como al encaminamiento de mensajes, sondas e informaciones hacia y entre los DGAD de ese país. En relación con lo primero, es preciso que las direcciones O/D de los usuarios dentro del país se elijan de tal modo que se asegure su carácter inequívoco, incluso en ausencia de los nombres verdaderos de los DGAD de usuarios. En relación con lo segundo, ello permite que los DGPR de dentro y los DGAD de fuera del país encaminen mensajes, sondas e informes a cualquiera de DGAD de dentro del país indiscriminadamente, y exige que estos últimos se interconecten de manera tal que los mensajes, las sondas y los informes sean llevados a sus destinos.

18.3.2 *Nombre-común*

Nombre común es un atributo normalizado que identifica a una LD o a un usuario relativo a la entidad indicada por otro atributo (por ejemplo, un nombre-organización).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas. Sea imprimible o teletex, la cadena se elige de entre un conjunto de tales cadenas administrado para este fin (y quizá para otros) por la entidad aludida anteriormente.

Nota – Entre otras muchas posibilidades, un nombre-común podría identificar un cometido organizativo (por ejemplo, «Director de mercadotecnia»).

18.3.3 *Nombre-país*

Nombre-país es un atributo normalizado que identifica a un país.

El valor de este atributo es una cadena numérica que da uno de los números asignados al país por la Recomendación X.121, o una cadena imprimible que da el par de caracteres asignados al país por la norma ISO 3166.

18.3.4 *Componentes-ampliación-dirección-O/D-postal*

Componentes-ampliación-dirección-O/D-postal es un atributo normalizado que proporciona, en una dirección postal, información adicional necesaria para identificar al destinatario (por ejemplo, una unidad organizativa).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.5 *Componentes-ampliación-dirección-entrega-física*

Componentes-ampliación-dirección-entrega-física es un atributo normalizado que especifica, en una dirección postal, información adicional necesaria para identificar el punto exacto de entrega (por ejemplo, número de piso y despacho en un gran edificio).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.6 *Atributos-postales-locales*

Atributos-postales-locales es un atributo normalizado que especifica el lugar de distribución, distinto del indicado por un atributo de nombre-oficina-entrega-física (por ejemplo, una zona geográfica) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.7 *Dirección-red*

Dirección-red es un atributo normalizado que da la dirección de red de un terminal.

Este atributo tiene algunos de los siguientes valores:

a) una cadena numérica de conformidad con la Recomendación X.121;

b) dos cadenas numéricas tal como se especifican en las Recomendaciones E.163 y E.164;

c) una dirección de punto de acceso al servicio de presentación (PASP).

Nota – Entre las cadenas admitidas por la Recomendación X.121 se encuentra un número télex precedido por la cifra de escape télex (8).

18.3.8 *Identificador-usuario-numérico*

Identificador-usuario-numérico es un atributo normalizado que identifica numéricamente a un usuario relativo al DGAD, indicado por un nombre-dominio-administración.

El valor de este atributo es una cadena numérica elegida entre un conjunto de tales cadenas, administrado para este fin por el DGAD aludido anteriormente.

18.3.9 *Nombre-organización*

Nombre-organización es un atributo normalizado que identifica una organización. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre-organización identifique una única entidad dentro del país) o referirse al DG indentificado por un nombre-dominio-privado, por un nombre-dominio-administración, o por ambos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas. Sea imprimible o teletex, la cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por el país o el DG aludido anteriormente.

Nota – En los países en que cada atributo nombre-organización debe corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos atributos.

18.3.10 *Nombres-unidades-organizativas*

Nombre-unidades-organizativas es un atributo normalizado que identifica una o más unidades (por ejemplo, divisiones o departamentos) de la organización indicada por un nombre-organización, siendo cada unidad, excepto la primera, una subunidad de las unidades cuyos nombres le preceden en el atributo.

El valor de este atributo es una secuencia ordenada de cadenas imprimibles, una secuencia ordenada de cadenas teletex o ambas. Sea imprimible o teletex, cada cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por la organización (o unidad abarcadora) aludida anteriormente.

18.3.11 *Nombre-servicio-entrega-física*

Nombre-servicio-entrega-física es un atributo normalizado que identifica a un servicio de entrega física relativo al DGAD indicado por un nombre-dominio-administración.

El valor de este atributo es una cadena imprimible elegida de entre un conjunto de tales cadenas, administrado para este fin el DGAD aludido anteriormente.

18.3.12 *Nombre-personal*

Nombre-personal es un atributo normalizado que identifica una persona con respecto a la entidad indicada por otro atributo (por ejemplo, un nombre-organización).

El valor de este atributo comprende los siguientes cuatro elementos de información, de las que la primera es obligatoria y las otras facultativas:

a) el apellido de la persona;

b) el nombre de la persona;

c) las iniciales de todos sus apelativos, excepto la del apellido;

d) su generación (por ejemplo «hijo»).

La información anterior se proporciona en forma de cadenas imprimibles, cadenas teletex o ambas.

18.3.13 *Nombre-país-entrega-física*

Nombre-país-entrega-física es un atributo normalizado que identifica el país en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo está sometido a las mismas limitaciones que el de un nombre-país.

18.3.14 *Nombre-oficina-entrega-física*

Nombre-oficina-entrega-física es un atributo normalizado que identifica la ciudad, el pueblo, etc. en el que se halla la oficina postal a través de la cual un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.15 *Número-oficina-entrega-física*

Número-oficina-entrega-física es un atributo normalizado que distingue entre varias oficinas postales indicadas por un único nombre-oficina-entrega-física.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.16 *Nombre-organización-entrega-física*

Nombre-organización-entrega-física es un atributo normalizado que identifica una organización patrón postal.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.17 *Nombre-personal-entrega-física*

Nombre-personal-entrega-física es un atributo normalizado que identifica un patrón postal.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.18 *Dirección-apartado-correos*

Dirección-apartado-correos es un atributo normalizado que especifica el número del casillero de la oficina postal en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas, a elegir entre el conjunto de tales cadenas asignadas para este fin por la oficina postal indicada por un atributo de nombre-oficina-entrega-física.

18.3.19 *Código-postal*

Código-postal es un atributo normalizado que especifica el código postal para la zona geográfica en la que el usuario recibe la entrega de los mensajes físicos.

El valor de este atributo es una cadena imprimible o numérica, elegida de entre el conjunto de tales cadenas, mantenido y normalizado para este fin por la Administración del país identificado por un atributo de nombre-país-entrega-física.

18.3.20 *Dirección-lista-correos*

Dirección-lista-correos es un atributo normalizado que identifica el código que un usuario da a la oficina postal para que acopie los mensajes físicos que se le deben entregar.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas, elegida de entre el conjunto de tales cadenas asignadas a este fin por la oficina postal indicada por un atributo de nombre-oficina-entrega-física.

18.3.21 *Nombre-dominio-privado*

Nombre-dominio-privado es un atributo normalizado que identifica un DGPR relativo al DGAD. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre de DGPR identifique una única entidad dentro del país) o referirse al DGAD indentificado por un nombre-dominio-administración.

El valor de este atributo es una cadena numérica o imprimible elegida de entre un conjunto de tales cadenas administradas para este fin por el país o el DGAD aludido anteriormente.

Nota – En los países en que cada nombre de DGPR debe corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos nombres.

18.3.22 *Dirección-calle*

Dirección-calle es un atributo normalizado que especifica la dirección de calle [por ejemplo, número de la casa y nombre de la calle y tipo (por ejemplo, «camino»)] en la que el usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.23 *Identificador-terminal*

Identificador-terminal es un atributo normalizado que da el identificador terminal de un terminal (por ejemplo, un distintivo télex o un identificador de terminal de teletex).

El valor de este atributo es una cadena imprimible.

18.3.24 *Tipo-terminal*

Tipo-terminal es un atributo normalizado que da el tipo de un terminal.

El valor de este atributo es uno cualquiera de los siguientes: *télex*, *teletex*, *facsímil G3*, *facsímil G4*, *terminal A15* o *videotex*.

18.3.25 *Dirección-postal-no-formatizada*

Dirección-postal-no-formatizada es un atributo normalizado que especifica una dirección postal de usuario de forma libre.

El valor de este atributo es una secuencia de cadenas imprimibles, representando cada una una línea de texto, o bien una única cadena teletex, estando las líneas separadas tal como se especifica para tales cadenas, o bien ambas.

18.3.26 *Nombre-postal-exclusivo*

Nombre-postal-exclusivo es un atributo normalizado que identifica el punto de entrega, distinto del indicado por un dirección-calle, un dirección-apartado-correos o un dirección-lista-correos, (por ejemplo, un edificio o un caserío) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.4 *Equivalencia de listas de atributos*

Varias direcciones O/D, y por tanto varias listas de atributos, pueden indicar el mismo usuario o la misma LD. Esta multiplicidad de direcciones O/D se debe en parte (pero sólo en parte) a las siguientes reglas de equivalencia de listas de atributos:

a) El orden relativo de atributos normalizados es intrascendente.

b) Cuando el valor de un atributo normalizado pueda ser una cadena numérica o una cadena imprimible equivalente, la elección entre ellas se considerará intrascendente.

   Nota – Esta regla se aplica incluso al atributo normalizado nombre-país cuando la elección entre las formas Rec. X.121 o ISO 3166 se considere irrelevante. Cuando en la Rec. X.121 se asignen a un país más de un número, la relevancia del número utilizado no ha sido normalizada en esta Recomendación.

c) Cuando el valor de un atributo normalizado pueda ser una cadena imprimible, una cadena teletex equivalente o ambas, la elección entre las tres posibilidades se considerará intrascendente.

d) Cuando el valor de un atributo normalizado puede contener letras, los tipos de esas letras se considerarán intrascendentes.

e) En un tipo o valor de atributo definido por el dominio o en un valor de atributo normalizado, todos los espacios precedentes, todos los espacios subsiguientes y todos los intermedios consecutivos menos uno, se considerarán intrascendentes.

Nota 1 – Un DG puede imponer reglas de equivalencia adicionales a los atributos que asigna a sus propios usuarios y LD. Podría definir, por ejemplo, reglas relativas a los caracteres de puntuación en los valores de atributos, el tipo de las letras de tales atributos o el orden relativo de los atributos definidos por el dominio.

Nota 2 – En el plano nacional, los DG pueden imponer reglas de equivalencia adicionales respecto a los atributos normalizados cuyos valores se dan como cadenas teletex, en particular las reglas para la deducción de las cadenas imprimibles equivalentes.

18.5 *Formas de direcciones O/D*

Todo usuario o LD tiene asignadas una o más direcciones O/D. Una dirección O/D es una lista de atributos que distingue a un usuario de otro e identifica el punto de acceso del usuario al STM o al punto de ampliación de la LD.

Una dirección O/D puede tomar alguna de las formas que, de manera resumida, se indican en el cuadro 10/X.402. En la primera columna del cuadro se da una relación de los atributos disponibles para la elaboración de direcciones O/D. Para cada forma de dirección O/D, la segunda columna indica los atributos que pueden aparecer en estas direcciones O/D y sus grados (véase también el § 18.6).

El cuadro 10/X.402 tiene cuatro secciones. Los tipos de atributos de la primera son los de carácter general, los de la segunda y la tercera son específicos de la entrega física. La cuarta sección comprende los atributos definidos por el dominio.

Las formas de direcciones O/D, expuestas de manera resumida en el cuadro 10/X.402, se definen y describen individualmente en los puntos que siguen.

18.5.1 *Dirección O/D nemotécnica*

Dirección O/D nemotécnica es una dirección que identifica nemotécnicamente a un usuario o una LD. Identifica a un DGAD y a un usuario o una LD relativos a éste.

Una dirección O/D nemotécnica consta de los siguientes atributos:

a) un nombre-país y un nombre-dominio-administración, que juntos identifican a un DGAD;

b) un nombre-dominio-privado, un nombre-organización, un nombres-unidades-organizativas, un nombre-personal o nombre-común o una combinación de los anteriores; y facultativamente uno o más atributos definidos por el dominio, que, conjuntamente, identifican a un usuario o una LD relativos al DGAD mencionado en a).

18.5.2 *Dirección O/D numérica*

Dirección O/D numérica es una dirección que identifica numéricamente a un usuario. Identifica a un DGAD y a un usuario relativo a él.

Una dirección O/D numérica consta de los siguientes atributos:

a) un nombre-país y un nombre-dominio-administración, que conjuntamente identifican a un DGAD;

b) un identificador-usuario-numérico y, de manera condicional, un nombre-dominio-privado, que juntos identifican al usuario relativo al DGAD mencionado en a);

c) de manera condicional, uno o más atributos definidos por el dominio que proporcionan información adicional a la de identificación del usuario.

18.5.3 *Dirección O/D postal*

Dirección O/D postal es una dirección que identifica a un usuario por su dirección postal. Identifica al servicio de entrega física a través del cual ha de accederse al usuario y da la dirección postal del mismo.

Se distinguen las siguientes clases de direcciones O/D postales:

a) **formatizada**: Dirección O/D postal que especifica la dirección postal de un usuario mediante varios atributos. Para esta forma de dirección O/D postal, la presente Recomendación prescribe, con cierto detalle, la estructura de direcciones postales.

b) **no formatizada**: Dirección O/D postal que especifica una dirección postal de un usuario en un solo atributo. Para esta forma de dirección O/D postal, la presente Recomendación no prescribe mayormente la estructura de las direcciones postales.

CUADRO 10/X.402

Formas de direcciones O/D

Tipos de atributos	Formas de direcciones O/D				
	NEM	NUM	Postal		TERM
			F	NF	
General					
Nombre-dominio-administración	O	O	O	O	C
Nombre-común	C	–	–	–	–
Nombre-país	O	O	O	O	C
Dirección-red	–	–	–	–	O
Identificador-usuario-numérico	–	O	–	–	–
Nombre-organización	C	–	–	–	–
Nombre-unidades-organizativas	C	–	–	–	–
Nombre-personal	C	–	–	–	–
Nombre-dominio-privado	C	C	C	C	C
Identificador	–	–	–	–	C
Tipo-terminal	–	–	–	–	C
Encaminamiento postal					
Nombre-servicio-entrega-física	–	–	C	C	–
Nombre-país-entrega-física	–	–	O	O	–
Código-postal	–	–	O	O	–
Direccionamiento postal					
Componentes-ampliación-dirección-O/D postal	–	–	C	–	–
Componentes-ampliación-entrega-física	–	–	C	–	–
Atributos-postales-locales	–	–	C	–	–
Nombre-oficina-entrega-física	–	–	C	–	–
Número-oficina-entrega-física	–	–	C	–	–
Nombre-organización-entrega-física	–	–	C	–	–
Nombre-personal-entrega-física	–	–	C	–	–
Dirección-apartado-correos	–	–	C	–	–
Dirección-lista-correos	–	–	C	–	–
Dirección-calle	–	–	C	–	–
Dirección-postal-no-formatizada	–	–	–	O	–
Nombre-postal-exclusivo	–	–	C	–	–
Definido por el dominio					
Definido por el dominio (uno o más)	C	C	–	–	C

NEM	Nemotécnica	NF	No formatizada
NUM	Numérica	O	Obligatoria
TERM	Terminal	C	Condicional
F	Formatizada		

Una dirección O/D postal, tanto si es formalizada como si no lo es, consta de los siguientes atributos:

a) un nombre-país y un nombre-país-administración, que juntos identifican a un DGAD;

b) de manera condicional, un nombre-dominio-privado, un nombre-servicio-entrega-física o ambos, que juntos identifican al servicio de entrega física mediante el cual se accede al usuario;

c) un nombre-país-entrega-física y un código-postal que juntos identifican la zona geográfica en la que el usuario recibe la entrega de mensajes físicos.

Una dirección O/D postal formatizada comprende, además, uno de cada uno de los atributos de direccionamiento postal (véase el cuadro 9/X.402) excepto el de dirección-postal-no-formatizada, que necesita el SEF para identificar el patrón postal.

Una dirección O/D postal no formatizada incluye, adicionalmente, un atributo de dirección-postal-no-formatizada.

Nota – El número total de caracteres de los valores de todos los atributos, excepto nombre-país, nombre-dominio-administración y nombre-servicio-entrega-física, en una dirección O/D postal, deberá ser lo bastante reducido para permitir su reproducción en 6 líneas de 30 caracteres, que es el tamaño de una ventanilla de sobre típica. El algoritmo de reproducción es específico de la UAEF, pero es probable que incluya delimitadores de inserción (por ejemplo, espacios) entre algunos de los valores de atributos.

18.5.4 *Dirección O/D terminal*

Dirección O/D terminal es una dirección que identifica un usuario mediante el número de red y, si es preciso, el tipo de su terminal. También puede identificar el DGAD a través del cual se accede a ese terminal. En el caso de un terminal telemático, da la dirección de red del terminal y, posiblemente, su identificador y tipo de terminal. En el caso de un terminal télex, da su número de télex.

Una dirección O/D terminal consta de los siguientes atributos:

a) una dirección-red;

b) de manera condicional, un identificador-terminal;

c) de manera condicional, un tipo-terminal;

d) de manera condicional, un nombre-país y un nombre-dominio-administración que juntos identifican un DGAD;

e) de manera condicional, un nombre-dominio-privado y, condicionalmente asimismo, uno o más atributos definidos por el dominio, todos los cuales proporcionan información adicional a la que identifica al usuario.

Los atributos de nombre-dominio-privado y definido por el dominio sólo estarán presentes si también lo están los de nombre-dominio-administración y nombre-país.

18.6 *Atributos condicionales*

La presencia o ausencia en una dirección O/D particular, de los atributos señalados como condicionales en el cuadro 10/X.402, se determina según los criterios que a continuación se exponen.

Si se accede a un usuario o LD a través de un DGPR, los atributos utilizados para encaminar mensajes al DGPR están presentes en la dirección O/D, a discreción del DGAD indicado por los atributos nombre-país y nombre-dominio-administración de la dirección O/D y de acuerdo con las reglas establecidas por él. El DGAD no impone más limitaciones a los atributos de la dirección O/D. Si no se accede a un usuario a través de un DGPR, todos los atributos condicionales, excepto los específicos de las direcciones O/D postales, figuran en una dirección O/D a discreción del DGAD indicado por los atributos nombre-país y nombre-dominio-administración y de acuerdo con las reglas establecidas por él.

Todos los atributos condicionales específicos de las direcciones O/D postales están presentes o ausentes en tales direcciones O/D, de modo que se satisfagan las exigencias de direccionamiento postal de los usuarios a los que identifican.

19 Encaminamiento

Para transportar un mensaje, sonda o informe a un usuario o al punto de ampliación de una LD, un ATM debe, no sólo localizar el usuario o la LD (es decir obtener su dirección O/D), sino también seleccionar un encaminamiento hacia esa ubicación.

El encaminamiento externo es un proceso incremental y sólo vagamente normalizado. A continuación se sugieren algunos principios para el encaminamiento externo. El interno queda fuera del alcance de esta Recomendación.

Estos principios son ilustrativos, y no son definitivos.

a) En un STM que conste de un único DG, la cuestión del encaminamiento, naturalmente, no se plantea.

b) Un DGPR puede estar conectado a un único DGAD. Cuando esto ocurre, el encaminamiento implica necesariamente al DGAD.

c) Un DGAD puede estar conectado a múltiples DGPR. Si este es el caso, el encaminamiento puede basarse en atributos de dirección O/D condicionales, incluyendo el de nombre-dominio-privado, pero sin limitarse a él.

d) Un DG puede estar conectado directamente a algunos otros DG, pero no a todos. Cuando la dirección O/D identifica a un DG con el que no existe conexión directa, el encaminamiento se puede basar en *acuerdos bilaterales* con los DG con los que sí existen conexiones directas, y en otras reglas locales.

e) Cuando el DG está conectado directamente al DG identificado por la dirección O/D, el objeto es encaminado, por sistema, directamente a ese DG.

f) Por *acuerdo bilateral*, un DG podría encaminar un objeto a otro DG a efectos de, por ejemplo, conversión.

g) Un DG puede encaminar a una dirección O/D mal formada siempre que, naturalmente, contenga por lo menos los atributos requeridos para ello.

Nota – Los acuerdos bilaterales y las reglas locales a que se ha aludido anteriormente, quedan fuera del alcance de esta Recomendación, y pueden estar basados en consideraciones de tipo técnico, político o económico, o de otra clase.

SECCIÓN 5 – USO DE LA GUÍA

20 Visión de conjunto

En esta sección se describen los usos que el STM puede hacer de la guía, cuando se dispone de ella. Si el STM no dispone de guía, la manera según la cual realiza las mismas tareas, si es que las realiza, es un asunto local.

La sección comprende los siguientes temas:

a) autenticación;

b) resolución de nombres;

c) ampliación de LD;

d) evaluación de capacidades.

21 Autenticación

Un objeto funcional puede efectuar la autenticación utilizando información almacenada en la guía.

22 Resolución de nombres

Un objeto funcional puede llevar a cabo la resolución de nombres utilizando la guía.

Un objeto que posee el nombre de guía de un usuario o de una LD y cuya dirección o direcciones O/D desea obtener, presenta ese nombre a la guía y pide los siguientes atributos de la inscripción en la guía del objeto:

a) *Direcciones O/D del STM*;

b) *Métodos de entrega preferidos del STM.*

Para hacerlo de manera satisfactoria, el objeto debe primero autenticarse él mismo a la guía, y tener derechos de acceso a la información solicitada.

23 Ampliación de LD

Un objeto funcional puede llevar a cabo la ampliación de una LD utilizando la guía, previa verificación de que existen los permisos de depósitos necesarios.

Para obtener los miembros de una LD cuyo nombre de guía posee, el objeto presenta ese nombre a la guía y pide los siguientes atributos de la inscripción en la guía del objeto:

a) *miembros de LD del STM*;

b) *permisos de depósito de LD del STM*;

c) *métodos de entrega preferidos del STM.*

Para hacerlo de manera satisfactoria, el ATM debe primero autenticarse él mismo a la guía, y tener derechos de acceso a la información solicitada.

24 Evaluación de capacidades

Un objeto funcional puede evaluar las capacidades de un usuario o LD utilizando la guía.

Los atributos de guía siguientes representan capacidades de usuario de posible importancia en el tratamiento de mensajes:

a) *longitud de contenido entregable del STM*;

b) *tipos de contenido entregables del STM*;

c) *TIC entregables del STM*

d) *métodos de entrega preferidos del STM.*

Los atributos de guía siguientes representan capacidades de MM de posible importancia en el tratamiento de mensajes:

a) *acciones automáticas facilitadas por el STM*;

b) *tipos de contenido facilitados por el STM*;

c) *atributos facultativos facilitados por el STM.*

Para evaluar determinada capacidad de un usuario o MM cuyo nombre de guía posee, el objeto presenta ese nombre a la guía y pide los atributos asociados a esa capacidad, que figuran en la inscripción en la guía del objeto.

Para hacerlo de manera satisfactoria, el ATM debe primero autenticarse él mismo a la guía y tener derechos de acceso a la información solicitada.

SECCIÓN 6 – REALIZACIÓN POR ISA

25 Visión de conjunto

En esta sección se describe cómo se realiza el STM por medio de la ISA.

La sección comprende los siguientes temas:

a) elementos de servicio de aplicación;

b) contextos de aplicación.

26 Elementos de servicio de aplicación

En este punto se identifican los elementos de servicio de aplicación (ESA) que figuran en la realización mediante ISA del tratamiento de mensajes.

En la ISA, las capacidades de comunicación de sistemas abiertos se organizan en grupos de capacidades relacionadas, llamados ESA. En la presente sección, se examina este concepto, a partir del modelo de referencia ISA, se establece una distinción entre ESA *simétricos* y *asimétricos* y se presentan los ESA definidos para el tratamiento de mensajes o que le sirven de apoyo.

Nota – El STM depende no sólo de los ESA examinados, sino también del elemento de servicio de acceso a la guía, definido en la Recomendación X.519. Sin embargo, como este ESA no figura en los *CA* para tratamiento de mensajes (véase la Recomendación X.419), no se analiza aquí.

26.1 *El concepto de ESA*

La figura 12/X.402 ilustra el concepto de ESA. En ella se representan de manera esquemática dos sistemas abiertos en comunicación. Sólo se muestran las partes de los sistemas abiertos relacionados con la ISA, a las que se llama entidades de aplicación (EA). Cada EA consta de un EU y de uno o más ESA. El EU representa la parte organizativa o de control de una EA, que define el cometido del sistema abierto (por ejemplo, el de un ATM). Por su parte, un ESA representa uno de los conjuntos de capacidad de comunicaciones, o servicios (por ejemplo, depósito o transferencia de mensajes), que el EU necesita para desempeñar su cometido.

A la relación entre dos EA en sistemas abiertos diferentes se le llama asociación de aplicación. Los ESA de un sistema abierto se comunican con sus ESA pares del otro a través de una conexión de presentación entre ellos. Esa comunicación es la que crea y mantiene la relación inherente a la asociación de aplicación. Para que varios ESA se combinen de manera satisfactoria en una única EA, deben estar diseñados de manera que coordinen su utilización de la asociación de aplicación.

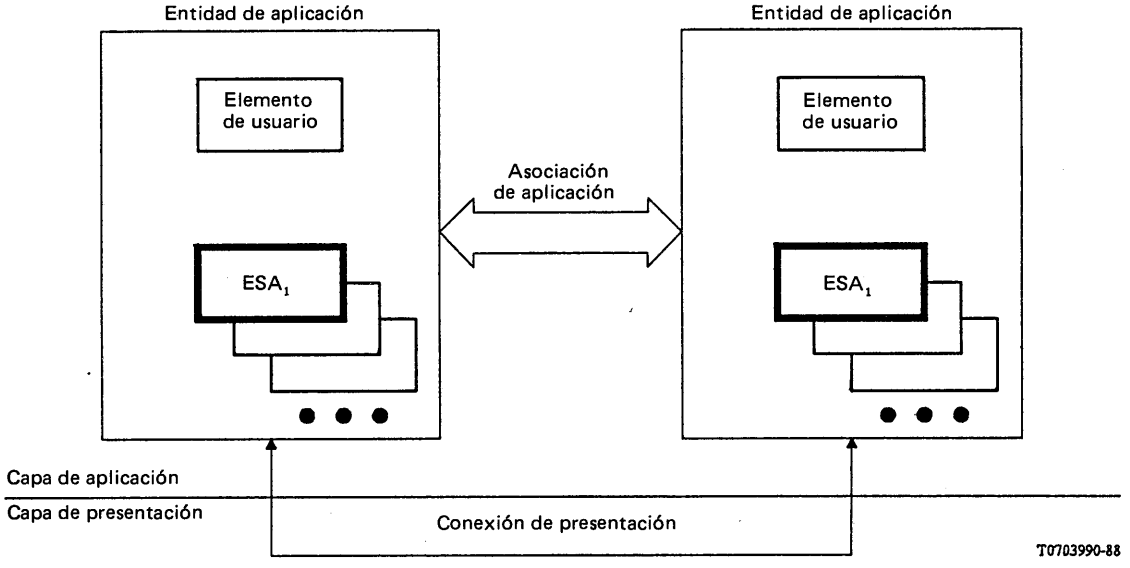


FIGURA 12/X.402

El concepto de ESA

Un ESA desempeña el papel, en gran medida mecánico, de trasladar las peticiones formuladas por su EU, y las respuestas, a y desde la forma dictada por el protocolo de aplicación que gobierna la interacción del ESA con su ESA par del sistema abierto al que la asociación le conecta. El ESA efectúa un servicio, o una parte del mismo, abstracto, a efectos de comunicación de la ISA (véase la Recomendación X.407).

Nota – En sentido estricto, el papel de un sistema abierto viene determinado por el comportamiento de sus procesos de aplicación. En el contexto del tratamiento de mensajes, un proceso de aplicación realiza un objeto funcional de uno de los tipos definidos en el § 7. A su vez, un EU es una parte de un proceso de aplicación.

26.2 *ESA simétricos y asimétricos*

Cabe distinguir los siguientes dos tipos de ESA, ilustrados en la figura 13/X.402:

a) **simétrico**: ESA por medio del cual un EU suministra y consume un servicio. El ESA para transferencia de mensajes, por ejemplo, es simétrico, porque ambos sistemas abiertos, cada uno de los cuales incorpora un ATM, ofrece y puede consumir por medio de él el servicio de transferencia de mensajes.

a) **asimétrico**: ESA por medio del cual un EU suministra y consume un servicio, pero no ambas cosas; dependiendo de cómo esté configurado el ESA. El ESA para entrega de mensajes, por ejemplo, es asimétrico, porque sólo el sistema abierto que incorpora un ATM ofrece el servicio asociado, y sólo el otro sistema abierto, que incorpora un AU o una MM, lo consume.

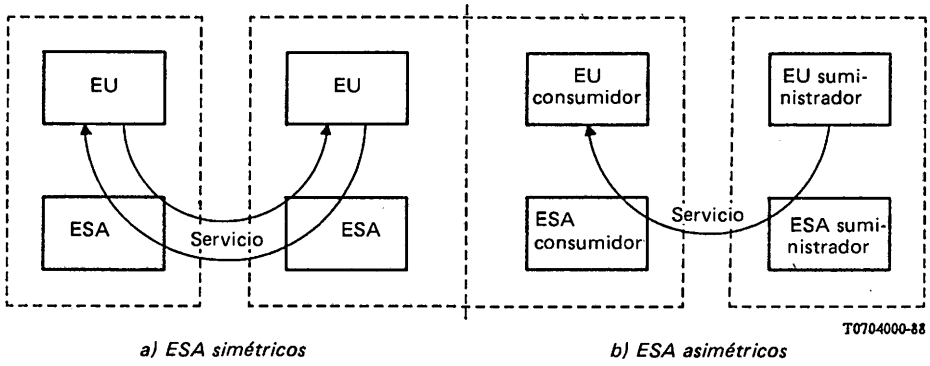


FIGURA 13/X.402

ESA simétricos y asimétricos

Con respecto a un determinado ESA asimétrico, un EU suministra un servicio que el otro consume. Los ESA, coubicados con los EU, ayudan en el suministro y consumo del servicio. Los cuatro papeles resultantes se muestran en la figura 14/X.402, con la siguiente terminología:

a) **EU suministrador de x**: Proceso de aplicación que suministra el servicio representado por el ESA asimétrico *x*.

b) **ESA suministrador de x**: ESA asimétrico *x* configurado para coubicación con un EU suministrador de *x*.

c) **EU consumidor de x**: Proceso de aplicación que consume el servicio representado por el ESA asimétrico *x*.

d) **ESA consumidor de x**: ESA asimétrico *x* configurado para coubicación con un EU consumidor de *x*.

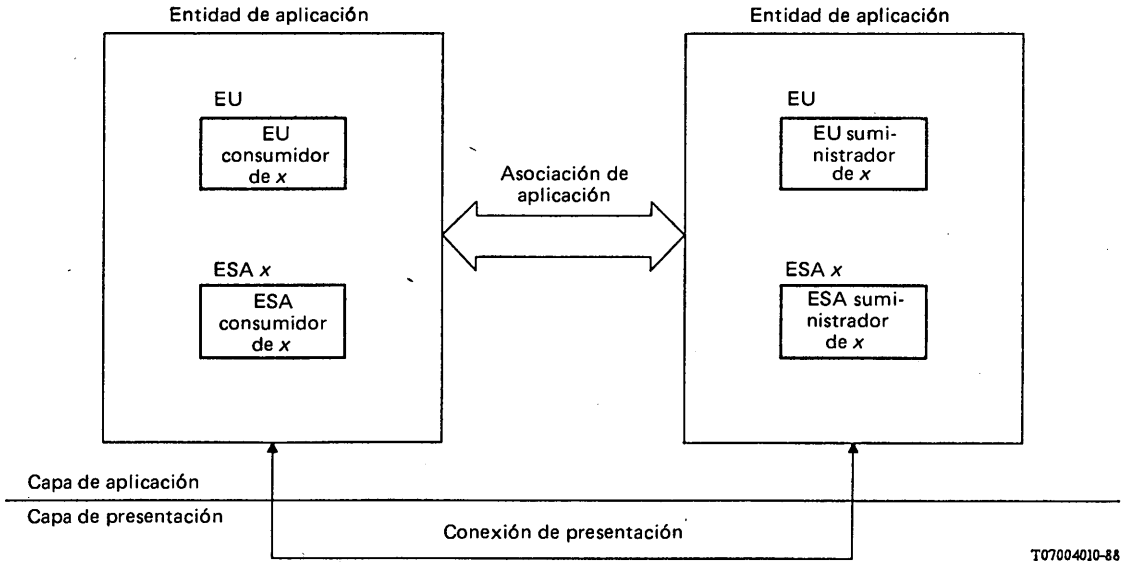


FIGURA 14/X.402

Terminología para ESA asimétricos

Como se ha indicado, los cuatro papeles descritos anteriormente están definidos en relación con un determinado ESA. Cuando una EA consta de varios ESA asimétricos, estos papeles se asignan independientemente a cada ESA. Así, tal como se muestra en la figura 15/X.402, un único EU podría servir como consumidor con respecto a un ESA y como suministrador con respecto a otro.

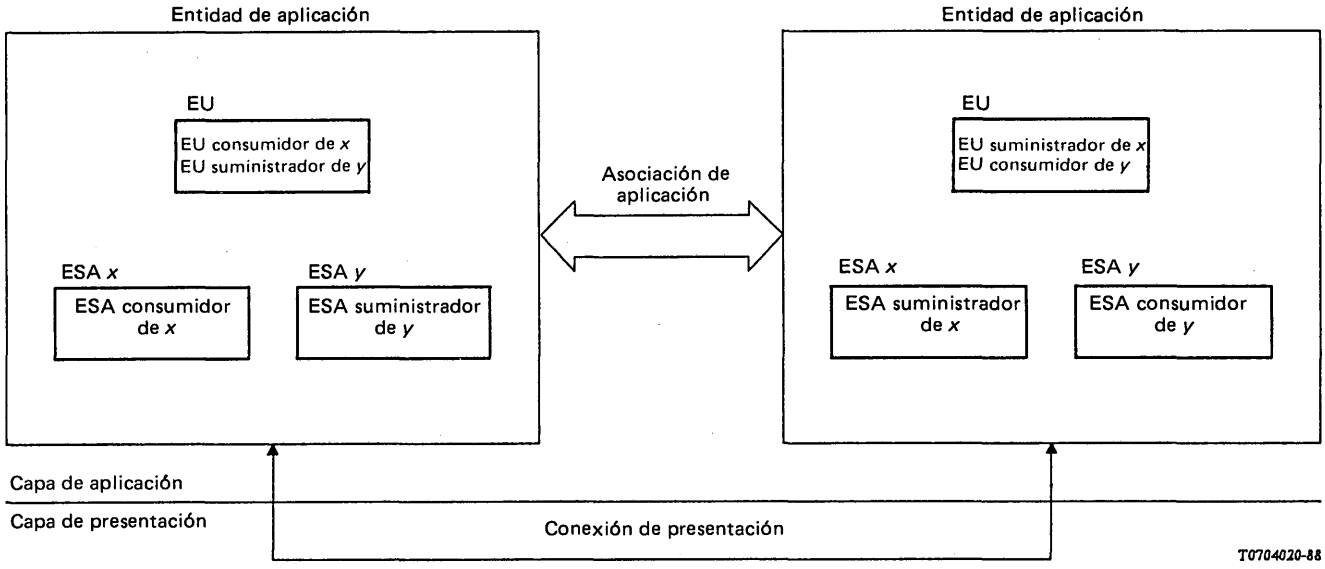


FIGURA 15/X.402

ESA asimétricos múltiples

26.3 *ESA de tratamiento de mensajes*

En la primera columna del cuadro 11/X.402 figura la lista de los ESA que proporcionan los diversos servicios del tratamiento de mensajes. Para cada ESA de la primera columna, se indica en la segunda si es simétrico o asimétrico. La tercera columna identifica los objetos funcionales – AU, MM, ATM y UA – que están asociados al ESA, como consumidores o como suministradores.

CUADRO 11/X.402

ESA de tratamiento de mensajes

ESA	Forma	Objetos funcionales			
		AU	MM	ATM	UA
ESTM	SIM	–	–	CS	–
ESDM	ASIM	C	CS	S	–
ESEM	ASIM	C	C	S	–
ESRM	ASIM	C	S	–	–
ESAM	ASIM	C	CS	S	–

SIM Simétrico

ASIM Asimétrico

C Consumidor

S Suministrador

Los ESA de tratamiento de mensajes, resumidos en el cuadro 11/X.402, se presentan por separado en los puntos que siguen. En la Recomendación X.419 figuran sus definiciones.

26.3.1 *Transferencia de mensajes*

El elemento de servicio transferencia de mensajes (ESTM) es el medio por el cual se efectúa el paso de transmisión de transferencia.

26.3.2 *Depósito de mensajes*

El elemento de servicio depósito de mensajes (ESDM) es el medio por el cual se efectúa el paso de transmisión de depósito.

26.3.3 *Entrega de mensajes*

El elemento de servicio entrega de mensajes (ESEM) es el medio por el cual se efectúa el paso de transmisión de entrega.

26.3.4 *Recuperación de mensajes*

El elemento de servicio recuperación de mensajes (ESRM) es el medio por el cual se efectúa el paso de transmisión de extracción.

26.3.5 *Administración de mensajes*

El elemento de servicio de administración de mensajes (ESAM) es el medio por el cual un AU, una MM o ATM archiva, en cada uno de los otros dos la información que facilita y controla su interacción subsiguiente, mediante el ESDM, ESM, el ESRM y el ESAM.

26.4 *ESA de apoyo*

En la primera columna del cuadro 12/X.402 figura la lista de los ESA de uso general, de los que dependen los ESA de tratamiento de mensajes. Para cada ESA de la primera columna, se indica en la segunda si es simétrico o asimétrico.

CUADRO 12/X.402

ESA de apoyo

ESA	Forma
ESOD	SIM
ESTF	SIM
ESCA	SIM

SIM Simétrico

Los ESA de apoyo, resumidos en el cuadro 12/X.402 se presentan por separado en los puntos que siguen.

26.4.1 *Operaciones distantes*

El elemento de servicio operaciones distantes (ESOD) es el medio por el cual, los ESA asimétricos de tratamiento de mensajes, estructuran sus interacciones de petición-respuesta, entre sistemas abiertos consumidores y suministradores.

El ESOD se define en la Recomendación X.219.

26.4.2 *Transferencia fiable*

El elemento de servicio transferencia fiable (ESTF) es el medio por el cual diversos ESA de tratamiento de mensajes, simétricos y asimétricos, transportan objetos de información – especialmente grandes, (por ejemplo, mensajes facsímil) – entre sistemas abiertos, de modo que se garantice su almacenamiento seguro en sus destinos.

El ESTF se define en la Recomendación X.218.

26.4.3 *Control de asociación*

El elemento de servicio control de asociación (ESCA) es el medio por el cual se establecen, se liberan y, en otros aspectos, se gestionan todas las asociaciones de aplicación entre sistemas abiertos.

El ESCA se define en la Recomendación X.217.

27 Contextos de aplicación

En la ISA, las capacidades de comunicación (es decir, los ESA) de dos sistemas abiertos son dirigidos, para un fin determinado, mediante contextos de aplicación (CA). Un CA es una especificación detallada del empleo de una asociación entre dos sistemas abiertos, es decir, un protocolo.

Un CA especifica cómo debe establecerse la asociación (por ejemplo, qué parámetros de inicialización se deben intercambiar), qué ESA deben participar en una comunicación entre pares a través de la asociación, qué limitaciones han de imponerse (si es que se impone alguna) a su utilización individual de la asociación, si el consumidor de cada ESA asimétrico es el iniciador o el contestador y cómo puede liberarse la asociación (por ejemplo, qué parámetros de finalización se deben intercambiar).

Todo CA tiene asignado un nombre (un identificador de objeto NSA.1). El iniciador de una asociación indica al contestador cuál es el CA que dirigirá el uso de la asociación, haciéndole llegar el nombre del CA por medio del ESCA.

Un CA identifica también con un nombre (un identificador de objeto NSA.1) las sintaxis abstractas de las UDPA que puede llevar una asociación, como resultado de su utilización por los ESA del CA. De manera convencional, se asigna un nombre bien al conjunto de las UDPA asociadas a cada ESA individual o bien al CA como un todo. El iniciador de una asociación indica al contestador la o las sintaxis abstractas, enviándole sus nombres por medio del ESCA.

Las sintaxis abstractas de una UDPA es su estructura como objeto de información (por ejemplo, un conjunto NSA.1 que comprenda un código de instrucción entero y un argumento de instrucción cadena AI5). Se diferencia de la sintaxis de transferencia de la UDPA, que es como se representa el objeto de información para transmisión entre dos sistemas abiertos (por ejemplo, un octeto indicando un conjunto NSA.1, seguido por un octeto que dé la longitud del conjunto, etc.).

Los CA, por medio de los cuales se proporcionan los diversos servicios de tratamiento de mensajes, se especifican en la Recomendación X.419. A estos protocolos se les conoce por P1, P3 y P7.

Nota – La naturaleza del contenido de un mensaje no entra en la definición del CA de tratamiento de mensajes, porque el contenido queda englobado (como una cadena de octetos) en los protocolos que lo transportan.

ANEXO A

(a la Recomendación R.402)

Clases de objetos de guía y atributos

Este anexo forma parte integrante de la presente Recomendación.

Varias clases de objetos de guía, atributos y sintaxis de atributos son específicos del tratamiento de mensajes. Se definen en el presente anexo utilizando los macros OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE-SYNTAX respectivamente, de la Recomendación X.501.

A.1 *Clases de objetos*

A continuación se especifican las clases de objetos del tratamiento de mensajes.

Nota – Las clases de objetos de guía descritos en este anexo pueden combinarse con otras clases de objetos, por ejemplo, los definidos en la Recomendación X.521. En el § 9 de la Recomendación X.501 figura una explicación del modo en que pueden combinarse las clases de objetos de guía en una inscripción de guía. El anexo B de la Recomendación X.521 da más información sobre las formas de nombres de guía y posibles estructuras de árboles de informaciones de guía.

A.1.1 *Lista de distribución del STM*

Un objeto **lista de distribución del STM** es una LD. Los atributos de su inscripción identifican su nombre común, permisos de depósito y direcciones O/D y, en la medida en que estén presentes los atributos pertinentes, describen la LD, identifican su organización, sus unidades organizativas y su propietario, mencionan objetos relacionados e identifican sus tipos de contenido entregable, TIC entregables, miembros y métodos de entrega preferidos.

```
mhs-distribution-list OBJECT-CLASS
        SUBCLASS OF top
        MUST CONTAIN {
                commonName,
                mhs-dl-submit-permissions,
                mhs-or-addresses }
        MAY CONTAIN {
                description,
                organization,
                organizationalUnitName,
                owner
                seeAlso,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-dl-members,
                mhs-preferred-delivery-methods }
        ::= id-oc-mhn-distribution-list
```

A.1.2 *Memoria de mensajes del STM*

Un objeto **memoria de mensajes del STM** es una EA que realiza una MM. Los atributos de su inscripción, en la medida en que estén presentes, describen la MM, identifican a su propietario y enumeran los atributos facultativos, las acciones automáticas y los tipos de contenido que facilita.

```
mhs-message-store OBJECT-CLASS
        SUBCLASS OF aplicationEntity
        MAY CONTAIN {
                description,
                owner,
                mhs-supported-optional-atributes,
                mhs-supported-automatic-actions,
                mhs-supported-content-types }
        ::= id-oc-mhs-message-store
```

A.1.3 *Agente de transferencia de mensajes del STM*

Un objeto **agente de transferencia de mensajes del STM** es una EA que pone en ejecución un ATM. Los atributos de su inscripción, en la medida que estén presentes, describen el ATM e identifican a su propietario y la longitud de su contenido entregable.

```
mhs-message-transfer-agent OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
                description,
                owner,
                mhs-deliverable-content-length }
        ::= id-oc-mhs-message-transfer-agent
```

A.1.4 *Usuario del STM*

Un objeto **usuario del STM** es un usuario genérico del STM (el usuario genérico del STM puede tener, por ejemplo, una dirección comercial, o una dirección privada, o ambas). Los atributos de su inscripción identifican la dirección O/D del usuario y, en la medida en que estén presentes, los atributos pertinentes identifican la longitud del contenido entregable del usuario, tipos de contenido y TIC, su MM y sus métodos de entrega preferidos.

```
mhs-user OBJECT-CLASS
        SUBCLASS OF top
        MUST CONTAIN {
              mhs-or-adresses },
        MAY CONTAIN {
              mhs-deliverable-content-length,
              mhs-deliverable-content-types,
              mhs-deliverable-eits,
              mhs-message-store,
              mhs-preferred-delivery-methods }
        ::= id-oc-mhs-user
```

A.1.5 *Agente de usuario del STM*

Un objeto **agente de usuario del STM** es una EA que realiza un AU. Los atributos de su inscripción, en la medida en que estén presentes, identifican al propietario del AU, la longitud de su contenido entregable, tipos de contenido y TIC, y su dirección O/D.

```
mhs-user-agent OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
              owner,
              mhs-deliverable-content-length,
              mhs-deliverable-content-types,
              mhs-deliverable-eits,
              mhs-or-addresses}
        ::= id-oc-mhs-user-agent
```

A.2 *Atributos*

Los atributos específicos del tratamiento de mensajes son los que se indican a continuación.

A.2.1 *Longitud de contenido entregable del STM*

El atributo **longitud del contenido entregable del STM** identifica la longitud máxima del contenido de los mensajes cuya entrega aceptará un usuario.

Un valor de este atributo es un entero.

```
mhs-deliverable-content-length ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX integerSyntax
        SINGLE VALUE
        ::= id-at-mhs-deliverable-content-length
```

A.2.2 *Tipos de contenido entregable del STM*

El atributo **tipos de contenido entregable del STM** identifica los tipos de contenido de los mensajes cuya entrega aceptará el usuario.

Un valor de este atributo es un identificador de objeto.

```
mhs-deliverable-content-types ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-deliverable-content-types
```

A.2.3 *TIC entregables del STM*

El atributo**TIC entregables del STM** identifica los TIC de los mensajes cuya entrega aceptará el usuario.

Un valor de este atributo es un identificador de objeto.

```
mhs-deliverable-eits ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentfierSyntax
        MULTI VALUE
        ::= id-at-mhs-deliverable-eits
```

A.2.4 *Miembros de LD del STM*

El atributo **miembros de LD del STM** identifica los miembros de una LD.

Un valor de este atributo es un nombre O/D.

```
mhs-dl-members ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
        MULTI VALUE
        ::= id-at-mhs-dl-members
```

A.2.5 *Permisos de depósito de LD del STM*

El atributo **permisos de depósito de LD del STM** identifica los usuarios y las LD que pueden depositar mensajes a una LD.

Un valor de este atributo es un permiso de depósito de LD.

```
mhs-dl-submit-permissions ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
        MULTI VALUE
        ::= id-at-mhs-dl-submit-permissions
```

A.2.6 *Memoria de mensajes del STM*

El atributo **memoria de mensajes del STM** identifica una MM de usuario por un nombre.

El valor de este atributo es un nombre distinguido de guía.

```
mhs-message-store ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
        SINGLE VALUE
        ::= id-at-mhs-message-store
```

A.2.7 *Direcciones O/D del STM*

El atributo **direcciones O/D del STM** especifica las direcciones O/D de un usuario o de una LD.

Un valor de este atributo es una dirección O/D.

```
mhs-or-addresses ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
        MULTI VALUE
        ::= id-at-mhs-or-addresses
```

A.2.8 *Métodos de entrega preferidos del STM*

El atributo **métodos de entrega preferidos del STM** identifica, en orden decreciente de preferencias, los métodos de entrega que prefiere un usuario.

Un valor de este atributo es un método de entrega preferido.

```
mhs-preferred-delivery-methods ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-at-mhs-preferred-delivery-methods
```

A.2.9 *Acciones automáticas permitidas por el STM*

El atributo **acciones automáticas permitidas por el STM** identifica las acciones automáticas que un AM admite totalmente.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-automatic-actions ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-supported-automatic-actions
```

A.2.10 *Tipos de contenido permitidos por el STM*

El atributo **tipos de contenido permitidos por el STM** identifica los tipos de contenido de los mensajes cuya sintaxis semántica permite totalmente una MM.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-content-types ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-supported-content-types
```

A.2.11 *Atributos facultativos permitidos por el STM*

El atributo **atributos facultativos permitidos por el STM** identifica los atributos facultativos que permite totalmente una MM.

Un valor de este atributo es un identificador de objeto.

```
mhs-supported-optional-attributes ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-supported-optional-attributes
```

A.3 *Sintaxis de atributos*

Las sintaxis de atributos específicos del tratamiento de mensajes son las que se indican a continuación.

A.3.1 *Permiso de depósito de LD del STM*

La sintaxis de atributo **permiso de depósito de LD del STM** caracteriza un atributo, cada uno de cuyos valores es un permiso de depósito.

```
mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
        SYNTAX DLSubmitPermission
        MATCHES FOR EQUALITY
        ::= id-as-mhs-dl-submit-permission

DLSubmitPermission ::= CHOICE {
        individual          [0] ORName,
        member-of-dl        [1] ORName,
        pattern-match       [2] ORNamePattern,
        member-of-group     [3] Name }
```

El valor de un permiso de depósito de LD presentado será del tipo *individual.*

Un permiso de depósito de LD concede, dependiendo de su tipo, acceso de presentación a los cero o más usuarios o listas de distribución siguientes:

a) *Individual*: Usuario o LD (no ampliada) alguno de cuyos nombres O/D es igual al nombre O/D especificado.

b) *Miembro-de-ld*: Cada miembro de la LD, o de cada LD jerarquizada de manera recurrente, alguno de cuyos nombres O/D es igual al nombre O/D especificado.

c) *Concordancia-de-esquemas*: Cada usuario o LD (no ampliada) alguno de cuyos nombres O/D satisface el esquema de nombres O/D especificado.

```
ORNamePattern ::= ORName
```

d) *Miembro-de-grupo*: Cada miembro de grupo-de-nombres, o de cada grupo-de-nombres jerarquizado, de manera recurrente, cuyo nombre está especificado.

Se considera que un valor presentado es igual a un valor objetivo de este tipo si los dos son idénticos, atributo por atributo. Además, se puede declarar igualado en otras condiciones, que son asunto local.

A.3.2 *Dirección O/D del STM*

La sintaxis del atributo **dirección O/D del STM** caracteriza a un atributo cada uno de cuyos valores es una dirección O/D.

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX
        SYNTAX ORAddress
        MATCHES FOR EQUALITY
        ::= id-as-mhs-or-address
```

Un valor de dirección O/D presentado es igual a un valor de dirección O/D objetivo en las condiciones especificadas en el § 18.4.

A.3.3 *Nombre O/D del STM*

La sintaxis del atributo **nombre O/D del STM** caracteriza a un atributo cada uno de cuyos valores es un nombre O/D.

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX
        SYNTAX ORName
        MATCHES FOR EQUALITY
        ::= id-as-mhs-or-name
```

Un valor de nombre O/D presentado es igual a un valor de nombre O/D objetivo si los dos son idénticos, atributo por atributo. Puede además declararse igualdad bajo otras condiciones, que son asunto local.

ANEXO B

(a la Recomendación X.402)

Definiciones de referencia de identificadores de objetos

Este anexo forma parte integrante de la presente Recomendación.

En él se definen, a efectos de referencia, diversos identificadores de objetos mencionados en el módulo NSA.1 del anexo C. Se utiliza NSA.1.

Todos los identificadores de objetos asignados por esta Recomendación lo son en el presente anexo. El anexo B es definitivo para todos, excepto para los de los módulos del NSA.1 y del propio STM. Las asignaciones definitivas para el primero se producen en los mismos módulos; en los párrafos IMPORT aparecen otras referencias a los mismos. El segundo es fijo.

```
MHSObjectIdentifiers {joint-iso-ccitt
        mhs-motis(6) arch(5) modules(0) object-identifiers(0)}
        DEFINITIONS IMPLICIT TAGS ::=
        BEGIN
        -- Prólogo
        -- Exporta todo.

IMPORTS -- nada -- ;

ID ::= OBJECT IDENTIFIER

-- Aspectos del STM

id-mhsac ID ::= { joint-iso-ccitt mhs-motis(6) mhsac(0) }
        -- Contexto de aplicación del STM
        -- Véase la Recomendación X.419
```

```
id-ipms     ID ::= { joint-iso-ccitt mhs-motis(6) ipms(1) }
            -- Mensajería interpersonal
            -- Véase la Recomendación X.420

id-asdc     ID ::= { joint-iso-ccitt mhs-motis(6) asdc (2) }
            -- Convenios de definición de servicio abstracto
            -- Véase la Recomendación X.407

id-mts      ID ::= { joint-iso-ccitt mhs-motis(6) mts (3) }
            -- Sistema de transferencia de mensajes
            -- Véase la Recomendación X.411

id-ms       ID ::= { joint-iso-ccitt mhs-motis(6) ms (4) }
            -- Memoria de mensajes
            -- Véase la Recomendación X.413

id-arch     ID ::= { joint-iso-ccitt mhs-motis(6) arch (5) }
            -- Arquitectura global
            -- Véase esta Recomendación

id-group    ID ::= { joint-iso-ccitt mhs-motis(6) group(6) }
            -- Reservado


-- Categorías

id-mod      ID ::= { id-arch 0} -- módulos, no definitivo
id-oc       ID ::= { id-arch 1} -- clases de objetos
id-at       ID ::= { id-arch 2} -- tipos de atributos
id-as       ID ::= { id-arch 3} -- sintaxis de atributos


-- Módulos

id-object-identifiers                   ID ::= {id-mod 0} -- no definitivo
id-directory-objects-and-attributes;    ID ::= {id-mod 1}
                --no definitivo


-- Clases de objetos

id-oc-mhs-distribution-list             ID ::= {id-oc 0 }
id-oc-mhs-message-store                 ID ::= {id-oc 1 }
id-oc-mhs-message-transfer-agent        ID ::= { id-oc 2 }
id-oc-mhs-user                          ID ::= { id-oc 3 }
id-oc-mhs-user-agent                    ID ::= { id-oc 4 }


-- Atributos

id-at-mhs-deliverable-content-length    ID ::= { id-at 0 }
id-at-mhs-deliverable-content-types     ID ::= { id-at 1 }
id-at-mhs-deliverable-eits              ID ::= { id-at 2 }
id-at-mhs-dl-members                    ID ::= { id-at 3 }
id-at-mhs-dl-submit-permissions         ID ::= { id-at 4 }
id-at-mhs-message-store                 ID ::= { id-at 5 }
id-at-mhs-or-addresses                  ID ::= { id-at 6 }
id-at-mhs-preferred-delivery-methods    ID ::= { id-at 7 }
id-at-mhs-supported-automatic-actions   ID ::= { id-at 8 }
id-at-mhs-supported-content-types       ID ::= { id-at 9 }
id-at-mhs-supported-optional-attributes ID ::= { id-at 10 }


-- Sintaxis de atributos

id-as-mhs-dl-submit-permission          ID ::= { id-as 0 }
id-as-mhs-or-address                    ID ::= { id-as 1 }
id-as-mhs-or-name                       ID ::= { id-as 2 }

END -- final de los identificadores de objetos de STM
```

ANEXO C

(a la Recomendación R.402)

Definición de referencia de clases de objetos de guía y atributos

Este anexo forma parte integrante de la presente Recomendación.

Este anexo, que complementa el anexo A define a efectos de referencia las clases de objetos, los atributos y las sintaxis de atributos específicos del tratamiento de mensajes. Para ello, se hace uso de las macro OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE SYNTAX de la Recomendación X.501.

```
MHSDirectoryObjectsAndAttributes { joint-iso-ccitt
    mhs-motis(6) arch(5) modules(0) directory(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
    -- Prólogo
    -- Exporta todo

IMPORTS
    -- Identificadores de objetos del STM
        id-as-mhs-dl-submit-permission, id-as-mhs-or-address,
        id-as-mhs-or-name-, id-at-mhs-deliverable-content-length,
        id-at-mhs-deliverable-content-types,
        id-at-mhs-deliverable-eits, id-at-mhs-dl-members,
        id-at-mhs-dl-submit-permissions, id-at-mhs-message-store,
        id-at-mhs-or-addresses, id-at-mhs-preferred-delivery-methods,
        id-at-mhs-supported-automatic-actions,
        id-at-mhs-supported-content-types,
        id-at-mhs-supported-optional-attributes,
        id-oc-mhs-distribution-list, id-oc-mhs-message-store,
        id-oc-mhs-message-transfer-agent,
        id-oc-mhs-user,
        id-oc-mhs-user-agent
        ----
        FROM MHSObjectIdentifiers { joint-iso-ccitt
            mhs-motis(6) arch(5) modules(0) object-identifiers(0) }
    -- Servico abstracto del STM
        ORAddress, ORName, RequestedDeliveryMethod
        ----
        FROM MTSAbstractService { joint-iso-ccitt
            mhs-motis(6) mts(3) modules(0) mTS-abstract-service(3)}
    -- Marco de información
        ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS
        ----
        FROM InformationFramework { joint-iso-ccitt
            ds(5) modules(1) informationFramework(a) }
    -- Clases de objeto seleccionadas
        applicationEntity
        top
        ----
        FROM SelectedObjectClasses { joint-iso-ccitt
            ds(5) modules(1) selectedObjectClasses(6) }
    -- Tipos de atributo seleccionados
        commonName, description, distinguishedNameSyntax,
        integerSyntax, objectIdentifierSyntax, organization,
        organizationalUnitName, owner, seeAlso
        ----
        FROM SelectedAttributeTypes { joint-iso-ccitt
            ds(5) modules(1) selectedAttributeTypes(5) };
```

```
-- CLASES DE OBJETOS

-- Lista de distribución del STM
        mhs-distribution-list OBJECT-CLASS
                SUBCLASS OF top
                MUST CONTAIN {
                        commonName,
                        mhs-dl-submit-permissions,
                        mhs-or-addresses }
                MAY CONTAIN {
                        description,
                        organization,
                        organizationalUnitName,
                        ower,
                        seeAlso,
                        mhs-deliverable-content-types,
                        mhs-deliverable-eits,
                        mhs-dl-members,
                        mhs-preferred-delivery-methods }
                ::= id-oc-mhs-distribution-list

-- Memoria de mensajes del STM
        mhs-message-store OBJECT-CLASS
                SUBCLASS OF applicationEntity
                MAY CONTAIN {
                        description,
                        owner,
                        mhs-supported-optional-attributes,
                        mhs-supported-automatic-actions,
                        mhs-supported-content-types }
                ::= id-oc-mhs-message-store

-- Agente de transferencia de mensajes del STM
        mhs-message-transfer-agent OBJECT-CLASS
                SUBCLASS OF applicationEntity
                MAY CONTAIN {
                        description,
                        owner,
                        mhs-deliverable-content-length }
                ::= id-oc-mhs-message-transfer-agent

-- Usuario del STM
        mhs-user OBJECT-CLASS
                SUBCLASS OF TOP
                MUST CONTAIN {
                        mhs-or-addresses }
                MAY CONTAIN {
                        mhs-deliverable-content-length,
                        mhs-deliverable-content-types,
                        mhs-deliverable-eits,
                        mhs-message-store,
                        mhs-preferred-delivery-methods }
                ::= id-oc-mhs-user

-- Agente de usuario del STM
        mhs-user-agent OBJECT-CLASS
                SUBCLASS OF applicationEntity
                MAY CONTAIN {
                        owner,
                        mhs-deliverable-content-length,
                        mhs-deliverable-content-types,
                        mhs-deliverable-eits,
                        mhs-or-addresses }
                ::= id-oc-mhs-user-agent
```

```
-- ATRIBUTOS

    -- Longitud de contenido entregable del STM
        mhs-deliverable-content-length ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX integerSyntax
            SINGLE VALUE
            ::= id-at-mhs-deliverable-content-length

    -- Tipos de contenido entregable del STM
        mhs-deliverable-content-types ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-content-types

    -- TIC entregables del STM
        mhs-deliverable-eits ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-deliverable-eits

    -- Miembros de LD del STM
        mhs-dl-members ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
            MULTI VALUE
            ::= id-at-mhs-dl-members

    -- Permisos de depósito de LD del STM
        mhs-dl-submit-permissions ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
            MULTI VALUE
            ::= id-at-mhs-dl-submit-permissions

    -- Direcciones O/D del STM
        mhs-or-addresses ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
            MULTI VALUE
            ::= id-at-mhs-or-addresses

    -- Memoria de mensajes del STM
        mhs-message-store ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
            SINGLE VALUE
            ::= id-at-mhs-message-store

    -- Métodos de entrega preferidos del STM
        mhs-preferred-delivery-methods ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
            MATCHES FOR EQUALITY
            SINGLE VALUE
            ::= id-at-mhs-preferred-delivery-methods

    -- Acciones automáticas admitidas por el STM
        mhs-supported-automatic-actions ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-automatic-actions

    -- Tipos de contenido admitidos por el STM
        mhs-suppported-content-types ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-content-types

    -- Atributos facultativos admitidos por el STM
        mhs-supported-optional-attributes ATTRIBUTE
            WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
            MULTI VALUE
            ::= id-at-mhs-supported-optional-attributes
```

```
-- SINTAXIS DE ATRIBUTO

    -- Permiso de presentación de LD de STM
        mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
            SYNTAX DLSubmitPermission
            MATCHES FOR EQUALITY
            ::= id-as-mhs-dl-submit-permission
        DLSubmitPermission ::= CHOICE {
            individual          [0] ORName,
            member-of-dl        [1] ORName,
            pattern-match       [2] ORNamePattern,
            member-of-group     [3] Name }
        ORNamePattern ::= ORName

    -- Dirección O/D del STM
        mhs-or-address-syntax ATTRIBUTE-SYNTAX
            SYNTAX ORAddress
            MATCHES FOR EQUALITY
            ::= id-as-mhs-or-address

    -- Nombre O/D del STM
        mhs-or-syntax ATTRIBUTE-SYNTAX
            SYNTAX ORName
            MATCHES FOR EQUALITY
            ::= id-as-mhs-or-name

END -- final de la guía del STM
```

ANEXO D

Amenazas contra la seguridad

Este anexo no forma parte de la presente Recomendación.

En el § 15.1 de la Recomendación X.400 se da una visión general de las amenazas contra la seguridad del STM. En esta Recomendación se consideran las amenazas tal como se plantean en el STM: amenazas en el acceso, amenazas entre mensajes, amenazas en los propios mensajes y amenazas en su almacenamiento. Todas estas amenazas pueden aparecer en las diversas formas siguientes:

a) suplantación;

b) secuenciamiento de mensajes;

c) modificación de información

d) denegación de servicio;

e) fuga de información;

f) rechazo;

g) otras amenazas del STM.

Además, las amenazas pueden surgir por accidente o intento doloroso, y pueden tener un carácter activo o pasivo. Las agresiones al STM se dirigirán hacia sus debilidades potenciales, y pueden comprender un cierto número de amenazas. Este anexo se ocupa de amenazas individuales, examinándose varios tipos amplios de amenazas, que de todos modos no constituyen una relación exhaustiva de las mismas.

En el cuadro D-1/X.402 se indica cómo hacer frente a esas amenazas utilizando los servicios de seguridad del STM. La lista de amenazas que aquí se da es indicativa, no definitiva.

CUADRO D-1/X.402

Utilización de los servicios de seguridad del STM

Amenaza	Servicios
Suplantación	
Simulación y mal uso del STRM	Autenticación de origen de mensajes Autenticación de origen de sondas Gestión de acceso seguro
Falso acuse de recibo	Prueba de entrega
Falsa originación de un mensaje	Autenticación de origen de mensajes
Simulación de un ATM a un usuario del STRM	Prueba de depósito Autenticación de origen de informes Gestión de acceso seguro
Simulación de un ATM a otro ATM	Autenticación de origen de informes Gestión de acceso seguro
Secuenciación de mensajes	
Reactuación de mensajes	Integridad de secuencia de mensajes
Reordenación de mensajes	Integridad de secuencia de mensajes
Adelanto de mensajes	
Retraso de mensajes	
Modificación de información	
Modificación de mensajes	Integridad de conexión Integridad de contenido
Destrucción de mensajes	Integridad de secuencia de mensajes
Degradación del encaminamiento y de otra información de gestión	
Denegación de servicio	
Denegación de comunicaciones	
Saturación de ATM	
Saturación del STRM	
Rechazo	
Denegación de origen	No rechazo de origen
Denegación de depósito	No rechazo de depósito
Denegación de entrega	No rechazo de entrega
Fuga de información	
Pérdida de confidencialidad	Confidencialidad de conexión Confidencialidad de contenido
Pérdida de anonimato	Confidencialidad de flujo de mensajes
Apropiación indebida de mensajes	Gestión de acceso seguro
Análisis del tráfico	Confidencialidad de flujo de mensajes
Otras amenazas	
Originador no autorizado para etiqueta de seguridad de mensajes	Gestión de acceso seguro Etiquetado de seguridad de mensajes
Usuario ATM/STRM no autorizado para el contexto de seguridad	Gestión de acceso seguro
Encaminamiento erróneo	Gestión de acceso seguro Etiquetado de seguridad de mensajes
Procedimientos de etiquetado diferentes	

D.1 *Suplantación*

El fenómeno llamado suplantación ocurre cuando una entidad finge, con éxito, ser una entidad distinta de la que es, y puede tener lugar de diferentes maneras. Un usuario no autorizado del STRM puede simular a otro para acceder sin permiso a las facilidades del STRM, o actuar en detrimento de un usuario válido, por ejemplo, desechando sus mensajes. Un usuario del STRM puede suplantar a otro y acusar recibo, falsamente, de un mensaje en nombre del receptor «válido». Un mensaje puede ser introducido en el STRM por un usuario que utilice falsamente la identidad de otro. Un usuario del STRM, un AM o un ATM se pueden enmascarar como si fuesen un usuario, un AM o un ATM distintos.

Entre las amenazas de tipo suplantación figuran las siguientes:

a) simulación y mal uso del STRM;

b) falso acuse de recibo;

c) falsa originación de un mensaje;

d) simulación de un ATM a un usuario del STRM;

e) simulación de un ATM a otro ATM.

Una suplantación incluye normalmente otras formas de agresión y, en un sistema seguro, puede implicar series de autenticaciones de usuarios válidos, por ejemplo, en la reactuación o modificación de mensajes.

D.2 *Secuenciamiento de mensajes*

Las amenazas contra la secuenciación de mensajes se producen cuando un mensaje se repite, entero o en parte, se le desplaza en el tiempo o se reordena. Puede recurrirse a esto para aprovecharse de la información de autenticación de un mensaje válido o reordenar o desplazar en el tiempo mensajes válidos. Si bien con los servicios de seguridad del STM es imposible evitar la reactuación de mensajes, sí cabe detectarlas y eliminar los efectos de esa amenaza.

Entre las amenazas a la secuenciación de mensajes figuran las siguientes:

a) reactuación de mensajes;

b) reordenación de mensajes;

c) adelanto de mensajes;

d) retraso de mensajes.

D.3 *Modificación de información*

La información para un destinatario deseado, la información de encaminamiento y otros datos relativos a la gestión pueden perderse o modificarse sin que ello se detecte. Es algo que puede ocurrir con cualquier elemento del mensaje, por ejemplo, su etiquetado, el contenido, los atributos, el destinatario o el originador. La degradación de la información de encaminamiento o de otro tipo de información de la gestión, almacenada en los ATM o utilizada por ellos, puede dar lugar a que el STRM pierda mensajes o bien a que funcione de manera incorrecta.

Entre las amenazas de tipo modificación de información figuran las siguientes:

a) modificación de mensajes;

b) destrucción de mensajes;

c) degradación del encaminamiento y de otra información de gestión.

D.4 *Denegación de servicio*

La denegación de servicio se produce cuando una entidad deja de realizar su cometido o evita que otras realicen los suyos. Puede tratarse de una denegación de acceso o de comunicaciones (que da lugar a otros problemas, como los de sobrecarga), una eliminación deliberada de mensajes dirigidos a un determinado destinatario, o una invención de tráfico extra. Se denegará el STRM si se provoca el fallo o el funcionamiento incorrecto de un ATM. Además, un usuario del STRM puede dar lugar a que dicho servicio se deniegue a otro usuario, saturándolo con mensajes que podrían sobrecargar la capacidad de conmutación de un ATM o llenar el espacio de almacenajes de mensajes de que se disponga.

Entre las amenazas de denegación de servicio figuran las siguientes:

a) denegación de comunicaciones;

b) fallo del ATM;

c) saturación del STRM.

D.5 *Rechazo*

El rechazo tiene lugar cuando un usuario del STRM o el propio STRM pueden negar a posteriori el depósito, la recepción o la originación de un mensaje.

Entre las amenazas de rechazo figuran las siguientes:

a) denegación de origen;

b) denegación de depósito;

c) denegación de entrega.

D.6 *Fuga de información*

Un ente no autorizado puede captar información vigilando las transmisiones o accediendo sin permiso a la información almacenada en alguna entidad del STM o por suplantación. En algunos casos, la presencia en el sistema de un usuario del STRM puede ser un asunto delicado y debe preservarse su anonimato. También es posible que un usuario del STRM distinto del destinatario deseado se haga con un mensaje enviado al segundo. Este podría ser el resultado de la simulación y del mal uso del STRM, o de haber provocado el funcionamiento incorrecto de un ATM. Además, observando el tráfico se pueden obtener otros detalles sobre la información que fluye por un STRM.

Entre las amenazas de fuga de información, figuran las siguientes:

a) pérdida de confidencialidad;

b) pérdida de anonimato;

c) apropiación indebida de mensajes;

d) análisis de tráfico.

D.7 *Otras amenazas*

En un sistema de seguridad de nivel único o de nivel múltiple, puede haber cierto número de amenazas relativas al etiquetado de seguridad, por ejemplo, el encaminamiento a través de un nodo al que no se le puede confiar información particularmente valiosa o en donde los sistemas utilizan procedimiento de etiquetado diferentes. Pueden existir amenazas a la implantación de una política de seguridad basada en la separación lógica utilizando etiquetas de seguridad. Es posible que un usuario del STRM origine un mensaje y le asigne una etiqueta para la que no está autorizado. Cabe también que un usuario del STRM o un ATM establezcan o acepten una asociación con un contexto de seguridad, para el que no tienen autorización.

Entre las «otras amenazas» aludidas en el epígrafe, figuran las siguientes:

a) originador no autorizado para etiqueta de seguridad de mensajes (depósito inadecuado);

b) usuario del STRM/ATM no autorizado para el contexto;

c) encaminamiento erróneo;

d) procedimientos de etiquetado diferentes.

ANEXO E

(a la Recomendación R.402)

Provisión de servicios de seguridad en la Recomendación X.411

Este anexo forma parte de la presente Recomendación.

En el cuadro E-1/X.402 se indica qué elementos de servicio de la Recomendación X.411 pueden utilizarse para facilitar los servicios de seguridad descritos en el § 10.2.

CUADRO E-1/X.402

Provisión de servicios de seguridad del STM

Servicio	Argumentos/servicios del STRM
Servicios de seguridad de autenticación de origen	
Autenticación de origen de mensajes	Verificación de autorización de origen de mensajes Testigo de mensajes
Autenticación de origen de sondas	Verificación de autenticación de origen de sondas
Autenticación de origen de informes	Verificación de autenticación de origen de informes
Prueba de depósito	Petición de prueba de depósito Prueba de depósito
Prueba de entrega	Petición de prueba de entrega Prueba de entrega
Servicios de seguridad de gestión de acceso seguro	
Autenticación de entidades pares	Credenciales de iniciador Credenciales de respondedor
Contexto de seguridad	Contexto de seguridad
Servicios de seguridad de confidencialidad de datos	
Confidencialidad de conexiones	No proporcionado
Confidencialidad de contenidos	Identificador del algoritmo de confidencialidad de contenidos Testigo de mensajes
Confidencialidad del flujo de mensajes	Tipo de contenido
Servicios de seguridad de integridad de datos	
Integridad de conexiones	No proporcionado
Integridad de contenidos	Verificación de integridad de contenidos Testigo de mensajes Verificación de autenticación de origen de mensajes
Integridad de secuencia de mensajes	Número de secuencia de mensajes Testigo de mensajes
Servicios de seguridad de no rechazo	
No rechazo de origen	Verificación de integridad de contenido Testigo de mensajes Verificación de autenticación de origen de mensajes
No rechazo de depósito	Petición de prueba de depósito Prueba de depósito
No rechazo de entrega	Petición de prueba de entrega Prueba de entrega
Etiquetado de mensajes	Etiqueta de seguridad de mensajes Testigo de mensajes Verificación de autenticación de origen de mensajes
Servicios de seguridad de gestión de la seguridad	
Cambio de credenciales	Cambio de credenciales
Registros	Registros

ANEXO F

Diferencias entre la Recomendación del CCITT y la norma ISO

Este anexo no forma parte de la presente Recomendación.

En él se da una relación de todas las diferencias, excepto las puramente estilísticas, entre esta Recomendación y la correspondiente norma internacional de la ISO.

Entre ambas especificaciones hay las diferencias siguientes:

a) La Norma Internacional de la ISO que corresponde a esta Recomendación muestra la conexión directa de dos DGPR situados en el mismo país, la de dos DGPR situados en países diferentes, y la de un solo DGPR conectado a dos DGAD, lo que no hace esta Recomendación (véase la figura 11/X.402).

b) La Norma Internacional de la ISO que corresponde a esta Recomendación no requiere que los DGAD y los DGPR estén relacionados jerárquicamente para direccionamiento y encaminamiento; mientras que esta Recomendación sí lo requiere (véanse los § 14.1.1, 14.1.2, 15 y 19).

c) Cuando un atributo de dirección O/D admite cadenas imprimibles y teletex, la Norma Internacional de la ISO que corresponde a esta Recomendación, no requiere que se proporcione la cadena imprimible, como mínimo, cuando los atributos se estén transportando internacionalmente, mientras que esta Recomendación sí lo requiere (véase el § 18.2).

ANEXO G

Índice

Este anexo no forma parte de la presente Recomendación.

Este anexo constituye el índice de esta Recomendación. Proporciona los números de los puntos donde se definen los elementos de cada categoría. El tratamiento de cada categoría es exhaustivo.

Este anexo presenta un índice de los elementos (si los hay) en las siguientes categorías:

a) abreviaturas;

b) términos;

c) elementos de información;

d) módulos NSA.1;

e) macros NSA.1;

f) tipos NSA.1;

g) valores NSA.1;

h) *acuerdos bilaterales*

i) **elementos que requieren ulterior estudio**;

j) **elementos a preparar.**

G.1 *Abreviaturas*

A/SYS 13.1.1
AS/SYS 13.1.3
ASG 3.2
AST/SYS 13.1.7
AT/SYS 13.1.5
ATM 7.3.1
AU 7.2.2
C 5.2
CA 3.1.3, 27
COMPUSEC 10
D 5.2
DG 14.1
DGAD 14.1.1
DGPR 14.1.2
EA 3.1.1
ESA 3.1.1, 26
ESAM 26.3.5
ESCA 3.13, 26.4.3
ESDM 26.3.2
ESEM 26.3.3
ESOD 3.1.5, 26.4.1
ESRM 26.3.4
ESTF 3.1.4, 26.4.2
ESTM 26.3.1
ETM 7
EU 3.1.1
F 5.2
IS
ISA 3.1.1
LD 7.1.3
MM 7.2.3
NSA.1 13.1.2
O 5.2
OD 3.1.5
P1 27
P3 27
P7 27
S/SYS 13.1.2
SEF 7.4.1
ST/SYS 13.1.6
STM 7.1.1
STRM 7.2.1
T/SYS 13.1.4
TF 3.1.4
TIC 8.1
UA 7.2.4
UDPA 3.1.1
UAEF 7.4.1

G.2 *Términos*

afirmación 9.4.9
agente de depósito 9.3.2
agente de entrega 9.3.6
agente de transferencia de mensajes 7.3.1
agente de usuario 7.2.2
almacenamiento de mensajes 6
ampliación de LD 9.4.4
asimétrico 26.2
atributo 18.1
atributo definido por el dominio 18.1
atributo normalizado 18.1
atributos-postales-locales 18.3.6
código postal 18.3.19
combinación 9.4.2
componentes-ampliación-dirección-entrega física 18.3.5
componentes-ampliación-dirección-O/D postal 18.3.4
condicional 5.2
contenido 8.1
conversión 9.4.6
conversión explícita 9.4.6
conversión implícita 9.4.6
defectible 5.2
depósito 9.3.2
depósito directo 9.3.2
depósito indirecto 9.3.2
destinatario 9.2
destinatario alternativo al destinatario asignado 9.2
destinatario alternativo especificado por el originador 9.2
destinatario deseado 9.2
destinatario efectivo 9.2
destinatario indirecto 9.2
destinatario inmediato 9.1
destinatario miembro 9.2
destinatario potencial 9.2
dirección-apartado-correos 18.3.18
dirección-calle 18.3.22
dirección-lista-correos 18.3.20
dirección-postal-no-formatizada 18.3.25
dirección O/D 18.5
dirección O/D numérica 18.3.2
dirección O/D nemotécnica 18.5.1
dirección O/D postal 18.5.3
dirección O/D terminal 18.5.4
dirección-red 18.3.7
división 9.4.1
dominio 14.1
dominio de gestión 14.1
dominio de gestión de administración 14.1.1
dominio de gestión privado 14.1.2
encaminamiento 9.4.10
encaminamiento externo 9.4.10
encanamiento interno 9.4.10
entorno de tratamiento de mensajes 7
entrega 9.3.6
entrega física 7.4.1
ESA consumidor 26.2
ESA suministrador 26.2
EU consumidor 26.2
EU suministrador 26.2

evento 9.1
evento de transmisión 9.1
exportación 9.3.5
recuperación 9.3.7
facultativo 5.2
formatizado 18.5.3
grado 5.2
indentificador terminal 18.3.23
identificador-usuario-numérico 18.3.8
importación 9.3.3
informe 8.3
informe de entrega 8.3
informe de no entrega 8.3
jerarquizado 7.1.3
lista de atributos 18.1
lista de distribución 7.1.3
memoria de mensajes 7.2.3
mensaje 8.1
mensaje descrito 8.2
mensaje físico 7.4.1
mensaje objeto 8.3
miembros 7.1.3
no entrega 9.4.7
no formatizado 18.5.3
no afirmación 9.4.8
nombre-común 18.3.2
nombre-dominio-administración 18.3.1
nombre-dominio-privado 18.3.21
nombre O/D 17.2
nombre-organización 18.3.9
nombre-organización-entrega-física 18.3.16
nombre-país 18.3.3
nombre-país-entrega-física 18.3.13
nombre-personal 18.3.12
nombre-personal-entrega-física 18.3.17
nombre-postal-exclusivo 18.3.26
nombre-servicio-entrega-física 18.3.11
nombre-unidades-organizativas 18.3.10
número-oficina-entrega-física 18.3.14
obligatorio 5.2
origen 9.3.1
originador 9.2
paso 9.1
paso de transmisión 9.1
permiso de depósito 7.1.3
punto de ampliación 9.4.4
recepción 9.3.8
redirección 9.4.5
reproducción física 7.4.1
resolución de nombre 9.4.3
simétrico 26.2
sistema de acceso 13.1.1
sistema de acceso y almacenamiento 13.1.3
sistema de acceso, almacenamiento y transferencia 13.1.7
sistema de acceso y transferencia 13.1.5
sistema de almacenamiento 13.1.2
sistema de almacenamiento y transferencia 13.1.6
sistema de entrega física 7.4.1
sistema de mensajería 13.1
sistema de transferencia 13.1.4
sistema de transferencia de mensajes 7.2.1
sistema de tratamiento de mensajes 7.1.1
sonda
sonda objeto 8.3
STM global 15
tipo 18.1
tipo de atributo 18.1
tipo de contenido 8.1
tipo de información codificada 18.1
tipo-terminal 18.3.24
transferencia 9.3.4
transferencia externa 9.3.4
transferencia interna 9.3.4
transferencia de mensajes 6
transmisión 9.1
tratamiento de mensajes 6
unidad de acceso 7.2.4
unidad de acceso de entrega física 7.4.1
usuario 7.1.2
usuario directo 7.1.2
usuario indirecto 7.1.2
valor 18.1
valor de atributo 18.1

Recomendación X.403

SISTEMAS DE TRATAMIENTO DE MENSAJES: PRUEBAS DE CONFORMIDAD

(Melbourne, 1988)

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) la necesidad de asegurar la interoperabilidad de los sistemas de tratamiento de mensajes;

(c) la necesidad de especificaciones de pruebas de conformidad para los sistemas de tratamiento de mensajes;

(d) que las Recomendaciones de la serie X.400 especifican los sistemas de tratamiento de mensajes;

(e) el estado actual de la metodología de pruebas de ISA y la notación dentro de CCITT-ISO,

recomienda por unanimidad

(1) que la metodología de pruebas para los sistemas de tratamiento de mensajes sea la descrita en esta Recomendación;

(2) que la notación utilizada para definir las especificaciones de pruebas para sistemas de tratamiento de mensajes sea la descrita en esta Recomendación;

(3) que el alcance y contenido de los manuales de especificación de pruebas de conformidad del CCITT para sistemas de tratamiento de mensajes sean los descritos en esta Recomendación.

ÍNDICE

0 *Introducción*

1 *Objeto y campo de aplicación*

2 *Referencias*

3 *Definiciones*

4 *Abreviaturas*

5 *Convenios*

6 *Visión de conjunto*

7 *Requisitos de conformidad*

8 *Metodología de pruebas*

9 *Estructura de las series de pruebas*

10 *Información que deben suministrar los realizadores*

11 *Notación de pruebas*

12 *Procedimientos de evaluación de la conformidad*

Anexo A – Notación de pruebas

Anexo B – Proformas ECRP de SMIP (P2)

Anexo C – Proformas ECRP de STRM (P1)

Anexo D – Proformas ECRP de STF

0 Introducción

Esta Recomendación describe los métodos de prueba, criterios de prueba y notación de prueba que deben utilizarse para las pruebas de conformidad de los sistemas de tratamiento de mensajes basados en las Recomendaciones de la serie X.400 de 1984, complementadas por la guía del realizador de la serie X.400 (versión 5).

1 Objeto y campo de aplicación

Los protocolos de tratamiento de mensajes, en el contexto de la presente Recomendación, se encuentran en las Recomendaciones de la serie X.400 (1984) y en la guía del realizador de la serie X.400 (versión 5).

Sus especificaciones de pruebas abstractas se encuentran en los manuales de especificación de pruebas de conformidad del CCITT asociados con la presente Recomendación:

- Manual de especificación de pruebas de conformidad para SMIP (P2)
- Manual de especificación de pruebas de conformidad para STRM (P1)
- Manual de especificación de pruebas de conformidad para SPF.

Aunque estos manuales se mencionan en la presente Recomendación, no forman parte de ella.

Si bien para el interfuncionamiento es necesario contar con la operación correcta y completa de los protocolos de sesión, transporte y otras capas inferiores, la prueba de estas capas está fuera del alcance de esta Recomendación. Además, las pruebas de conformidad de las Recomendaciones de la serie X.400 deben verificar que el servidor de transferencia fiable (STF) utiliza debidamente las capas inferiores a él.

Las pruebas definidas en este documento se aplican al trabajo entre varios dominios (DGAD a DGAD y DGAD a DGPR). Se relacionan con cualquier ATM o AU en un dominio que acepta comunicaciones con otros dominios.

Las pruebas de conformidad de la semántica y sintaxis de la información de la parte de cuerpo real transmitida en una PARTE DE CUERPO (BODY PART) está fuera del alcance de este documento.

La finalidad de esta Recomendación es reducir al mínimo el tiempo y costo que los fabricantes de realizaciones X.400 y proveedores de servicios X.400 deban emplear para garantizar un alto grado de interoperabilidad de sus equipos. Este propósito se logra con un conjunto de especificaciones de pruebas de conformidad de las Recomendaciones de la serie X.400. El éxito en la ejecución conjunta de las especificaciones de pruebas por dos realizaciones pueden ser aceptado como una evidencia concluyente de la operación completa y correcta de esas realizaciones.

El objeto y finalidad de esta Recomendación es diferente de otras Recomendaciones del CCITT que definen protocolos y servicios de comunicación, tales como las Recomendaciones de la serie X.400 (1984). La finalidad de las Recomendaciones de la serie X.400 es la definición de un sistema de forma inequívoca. Sin embargo, una Recomendación sobre pruebas de conformidad proporciona un subconjunto de pruebas, bien elegidas, de entre un número virtualmente infinito de pruebas, necesarias para garantizar el cumplimiento total de una norma de protocolo. El subconjunto se elige de tal manera que proporcione un alto grado de confianza en que las realizaciones probadas interfuncionarán, a la vez que se toman en cuenta las consideraciones pragmáticas como el tiempo requerido para realizar las pruebas.

Las pruebas de conformidad de normas funcionales están fuera del alcance de la presente Recomendación. Sin embargo, se reconoce que las pruebas de conformidad con las normas funcionales pueden derivarse de estas Recomendaciones y de los manuales de especificación de prueba asociados.

Debe señalarse que la prueba de conformidad de los sistemas de tratamiento de mensajes puede corresponder al marco de los reglamentos nacionales y puede estar sujeta a políticas de prueba de las Administraciones que están fuera del alcance de este documento.

2 Referencias (versión 1984)

Recomendación X.210 Convenios relativos a la definición del servicio de capa en la interconexión de sistemas abiertos (ISA).

Recomendación X.400 Sistemas de tratamiento de mensajes: modelo de sistemas y elementos de servicio.

Recomendación X.401 Sistemas de tratamiento de mensajes: elementos de servicio básicos y facilidades de usuario facultativas.

Recomendación X.408 Sistemas de tratamiento de mensajes: reglas de conversión de tipos de información codificada.

Recomendación X.409	Sistemas de tratamiento de mensajes: sintaxis y notación de la transferencia de presentación.
Recomendación X.410	Sistema de tratamiento de mensajes: operaciones distantes y servidor de transferencia fiable.
Recomendación X.411	Sistema de tratamiento de mensajes: capa de transferencia de mensajes.
Recomendación X.420	Sistemas de tratamiento de mensajes: capa de agente de usuario del servicio de mensajería interpersonal.
Serie X.400	Guía del realizador versión 5

3 Definiciones

3.1 *Definiciones de convenios de servicio*

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.210, versión 1984:

a) primitiva;
b) petición (primitiva);
c) indicación (primitiva);
d) respuesta (primitiva);
e) confirmación (primitiva).

3.2 *Definiciones de tratamiento de mensajes*

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.400, versión 1984:

a) dominio de gestión de administración;
b) mensaje interpersonal (Recomendación X.420);
c) mensaje;
d) transferencia de mensajes (Recomendación X.411);
e) originador;
f) dominio de gestión privada;
g) destinatario;
h) usuario.

4 Abreviaturas

En la presente Recomendación se utilizan las siguientes abreviaturas.

DGAD	Dominio de gestión de administración
PSA	Primitiva de servicio abstracto
IDU	Método de prueba insertada distribuida en una sola capa
STM	Sistema de tratamiento de mensajes
SMIP	Sistema de mensajería interpersonal
RSP	Realización sujeta a pruebas
UDPM	Unidad de datos del protocolo de mensajes
TRM	Transferencia de mensajes
ATM	Agente de transferencia de mensajes
STRM	Sistema de transferencia de mensajes
P1	Protocolo de transferencia de mensajes (Recomendación X.411)
P2	Protocolo de mensajería interpersonal (Recomendación X.420)
PCO	Punto de control y observación
ECRP	Enunciado de conformidad de realización de protocolo

ISRP	Información suplementaria de realización de protocolo para pruebas
UDP	Unidad de datos del protocolo
DGPR	Dominio de gestión privado
STF	Servidor de transferencia fiable
PAS	Punto de acceso al servicio
PSP	Parámetro de serie de pruebas
NCAT	Notación combinada tabular y de árbol
AU	Agente de usuario

5 Convenios

No se define ningún convenio para la presente Recomendación.

6 Visión de conjunto

Hay dos tipos de documentos del CCITT relacionados con la prueba de conformidad X.400:

a) la presente Recomendación X.403, titulada «sistemas de tratamiento de mensajes: pruebas de conformidad»;

b) tres manuales de especificaciones de pruebas de conformidad del CCITT conexos, titulados:
   - Manual de especificaciones de pruebas de conformidad para SMIP (P2)
   - Manual de especificaciones de pruebas de conformidad para STRM (P1)
   - Manual de especificaciones de pruebas de conformidad para STF.

La presente Recomendación está destinada a un amplio público. Los manuales están destinados a los realizadores de pruebas y contienen las especificaciones de pruebas detalladas.

6.1 *Recomendaciones sobre pruebas de conformidad X.400*

Esta Recomendación proporciona la siguiente información:

a) los requisitos de conformidad para las realizaciones X.400;

b) la metodología de prueba;

c) la estructura de las especificaciones de prueba;

d) la información que deben proporcionar los realizadores como prerequisitos de las pruebas de conformidad;

e) la notación de prueba;

f) los procedimientos de evaluación de la conformidad.

6.2 *Manuales de especificación de pruebas de conformidad X.400*

Los tres manuales de especificaciones de pruebas de conformidad del CCITT contienen las especificaciones de prueba para SMIP (P2), STRM (P1), STF. Las especificaciones de prueba están escritas en una notación que se expone en términos generales en el § 11. Los manuales de especificaciones de pruebas de conformidad se mencionan en esta Recomendación, pero no forman parte de ella.

Puesto que los manuales contienen especificaciones de prueba detalladas e inequívocas, los usuarios de los manuales deben estar familiarizados con las Recomendaciones de la serie X.400, así como con la metodología de prueba utilizada.

7 Requisitos de conformidad

La finalidad de las especificaciones de prueba de que trata la presente Recomendación es definir pruebas que establezcan un alto grado de confianza en que las diversas capas de protocolo de una realización sometida a prueba son conformes a los requisitos de las Recomendaciones de la serie X.400 (1984).

7.1 Un sistema que pretende ser conforme con el servicio MIP de las Recomendaciones de la serie X.400 tiene que satisfacer correctamente:

- los elementos de servicio MIP básicos definidos en el cuadro 2/X.400;
- las facilidades facultativas de usuario MIP definidas como esenciales en los cuadros 1/X.401 y 2/X.401 (cuando se deba considerar la categorización para generación y recepción);
- las facilidades facultativas de usuario MIP definidas como adicionales en los cuadros 1/X.401 y 2/X.401, que el sistema declare aceptar;
- los requisitos relacionados con el servicio MIP definidos en la versión 5 de la guía del realizador de la serie X.400.

7.2 Un sistema que pretenda ser conforme con el servicio TRM de las Recomendaciones de la serie X.400 debe satisfacer correctamente:

- los elementos de servicio TRM básicos definidos en el cuadro 1/X.400, relacionados con el protocolo STRM (P1);
- las facilidades facultativas de usuario TRM definidas como esenciales en los cuadros 3/X.401 y 4/X.401 y relacionadas con el protocolo STRM (P1);
- las facilidades facultativas de usuario definidas como adicionales en los cuadros 3/X.401 y 4/X.401 y relacionadas con el protocolo STRM (P1), que el sistema declare aceptar;
- los requisitos relacionados con el servicio TRM P1 definidos en la versión 5 de la guía del realizador de la serie X.400.

7.3 El sistema que pretenda ser conforme con el servicio STF de las Recomendaciones de la serie X.400 debe satisfacer correctamente:

- los servicios STF definidos en la Recomendación X.410;
- los requisitos relacionados al servicio STF definidos en la versión 5 de la guía del realizador de la serie X.400.

7.4 La presunta conformidad de una realización con las Recomendaciones de la serie X.400 puede verificarse utilizando los manuales de especificación de pruebas de conformidad de esta Recomendación, para garantizar que:

a) La realización no actúa o reacciona en forma diferente a la descrita en las Recomendaciones.

b) La realización es capaz de tratar los errores de protocolo.

La reacción de una realización al recibir errores de protocolo no está definida en las Recomendaciones de la serie X.400. A los efectos de las pruebas de conformidad, se establece el requisito adicional mínimo de que, en tales casos, la realización continúe operando normalmente.

La ausencia de un elemento de protocolo obligatorio en P2 o P1 se considera como un error de protocolo. Hay que señalar que en un STM realizado, un dominio destinatario puede decidir entregar una UDPM incorrecta. Esto debe ser considerado por el vendedor de equipo como un diseño patentado, y las acciones específicas que se efectúan en estas situaciones son definidas por el vendedor y no están sujetas a conformidad.

c) La realización satisface correctamente los requisitos definidos en la guía del realizador de la serie X.400 en su versión 5.

Las longitudes máximas y el número máximo de apariciones se interpretan de la siguiente manera:

- En el origen: la realización puede admitir sus valores máximos hasta, pero sin exceder, el valor impuesto.
- En el destino: la realización debe admitir los valores máximos impuestos. Puede aceptar valores superiores a los establecidos, pero los requisitos de conformidad exigidos a la realización en caso de recepción de una longitud/ocurrencia que sobrepasa el valor impuesto son los mismos que para los errores de protocolo.

La conformidad a las Recomendaciones de la serie X.400 no puede verificarse en el caso de las realizaciones para las cuales no es posible efectuar todas las pruebas necesarias con respecto a las características clasificadas como obligatorias, básicas o esenciales facultativas.

ARCHIVES U.I.T. GENÈVE

8 Metodología de pruebas

8.1 *Configuraciones de prueba*

Se utilizan dos configuraciones de pruebas. La primera se muestra en la figura 1/X.403 y se utiliza para probar SMIP (P2), STRM (P1) y STF.

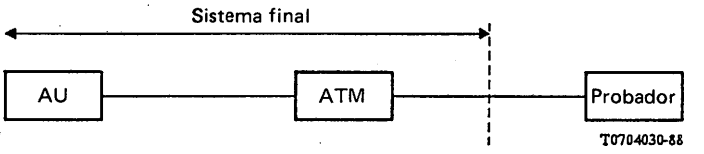


FIGURA 1/X.403

Configuración del sistema final

La segunda configuración se muestra en la figura 2/X.403 y se utiliza para probar los aspectos del relevador de protocolo STRM (P1).

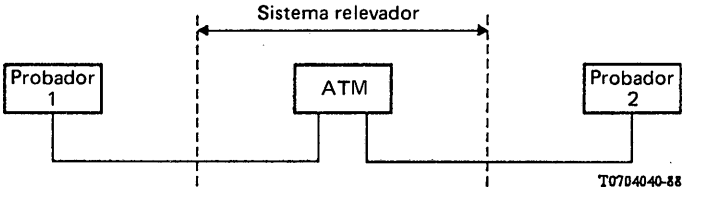


FIGURA 2/X.403

Configuración de prueba del ATM relevador

8.2 *Puntos de control y observación*

Los casos de prueba se describen en forma abstracta en términos de sucesos en los puntos de control y observación (PCO), tanto en el probador como en la realización sometida a prueba (RSP). Generalmente, estos PCO son puntos de acceso al servicio (PAS) y los sucesos generalmente son primitivas de servicio abstracto (PSA). Esto no significa que los fabricantes deban tener PAS a las que se pueda tener acceso, o realizar PSA dentro de sus sistemas. Durante la ejecución de la prueba se puede acceder a los PCO de una RSP en forma indirecta a través de un interfaz de usuario. Cuando la prueba se realiza a través de un interfaz de usuario, la relación de correspondencia de los sucesos entre el PAS y el interfaz de usuario es proporcionada por el proveedor de la RSP, como se describe en el § 10.2.

8.2.1 *PCO para SMIP (P2)*

Los casos de prueba SMIP (P2) se describen utilizando los puntos de control y observación (PCO) que aparecen en la figura 3/X.403.

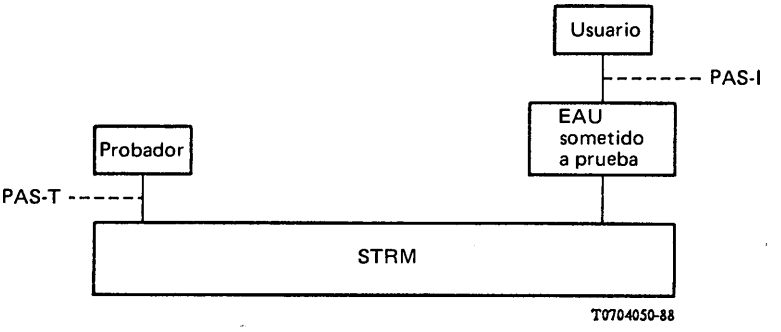


FIGURA 3/X.403

Puntos de control y observación para SMIP(P2)

Para el probador, el punto de control y de observación es el punto de acceso de servicio (PAS) definido en el límite entre la capa de agente de usuario y la capa de transferencia de mensaje. Este PCO utiliza las primitivas del servicio de capa de transferencia de mensaje definidas en la Recomendación X.411.

Para la RSP, el PCO es el PAS definido en el límite superior de la capa de agente de usuario. Sin embargo, la Recomendación X.420 no incluye una definición de primitivas de servicio y por lo tanto ha sido necesario establecer primitivas de servicio ficticias para el envío y recepción de mensajes IP, a fin de poder describir formalmente los casos de prueba.

8.2.2 *PCO para STRM (P1)*

Los casos de prueba STRM (P1) se describen utilizando los PCO que aparecen en la figura 4/X.403.

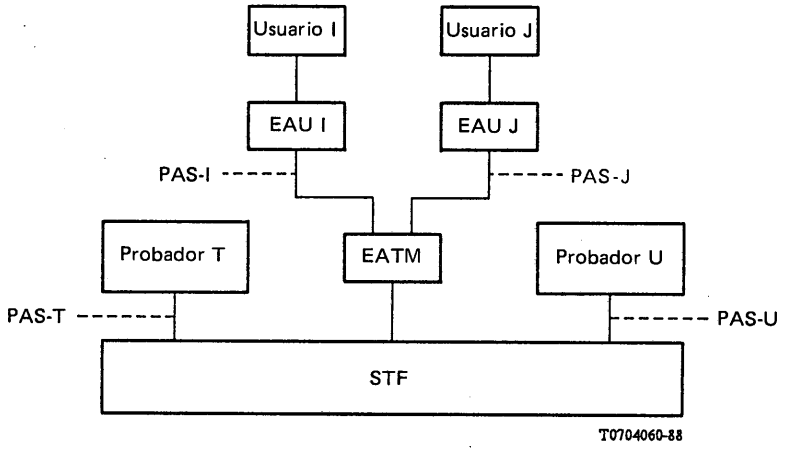


FIGURA 4/X.403

Puntos de control y observación para STRM(P1)

Para el probador, el PCO es el PAS definido en el límite entre la capa TRM y el STF. Este PCO utiliza las primitivas STF definidas en la Recomendación X.410.

Para las RSP, el PCO es el PAS definido en el límite entre la capa AU y la capa TRM. Este PCO utiliza las primitivas de servicio TRM definidas en la Recomendación X.411.

La prueba de las funciones de relevo requiere más de un PAS probador. Igualmente la prueba de la entrega a destinos múltiples requiere más de un AU en la RSP.

8.2.3 *PCO para STF*

Los casos de prueba STF se describen utilizando los PCO que aparecen en la figura 5/X.403.

Para el probador, el PCO es el PAS definido en el límite entre el STF y la capa de sesión. Este PCO utiliza las primitivas de servicio de sesión definidas en la Recomendación X.215.

Para la RSP, el PCO es el PAS definido en el límite superior de la capa de agente de usuario. Este PCO utiliza las mismas primitivas de servicio ficticias definidas para SMIP (P2) (§ 8.2.1).

La descripción de los casos de prueba STF incluye sucesos en un tercer PAS en la RSP (PAS-I) entre la capa TRM y el STF. Los sucesos de este PAS se utilizan únicamente para aclaración y el mismo no sirve de PCO.

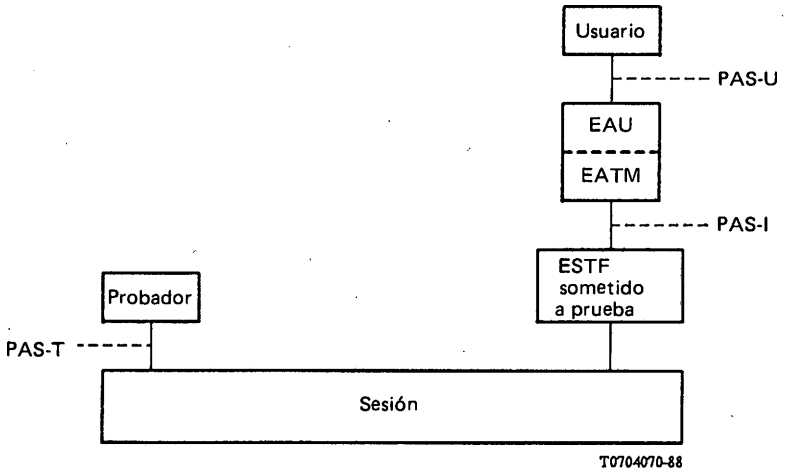


FIGURA 5/X.403

Puntos de control y observación para STF

8.3 *Estrategia de diseño de pruebas*

Las especificaciones de prueba STM están diseñadas con arreglo a los siguientes conceptos:

a) Una especificación de prueba se define como una serie de pruebas compuestas de un número de casos de prueba, tal como se definen en el § 11.1.

b) Los casos de pruebas se definen en términos de:
   - eventos PSA de capa inferior en el probador;
   - eventos PSA capa superior en la RSP.

c) Los casos de prueba definen la secuencia de estos sucesos PSA y los parámetros asociados, en especial las UDP.

d) Los casos de prueba para comportamiento válido especifican secuencias de sucesos PSA y UDP que concuerdan con las Recomendaciones de la serie X.400.

e) Los casos de prueba para comportamiento no válido se caracterizan por:
   - un evento o UDP correcto iniciado por el probador en un estado de protocolo donde no está permitido (un suceso inoportuno), o
   - una UDP correcta que incorpora un elemento sintácticamente correcto y dentro de la gama, pero que está en conflicto con el valor negociado, o
   - una UDP enviada por el probador y sintácticamente incorrecta (por ejemplo, falta el elemento de protocolo obligatorio, un valor fuera de gama o un indicador de longitud codificado en forma incorrecta), o
   - para un STF un evento PSA de capa inferior emitido por el probador utilizado, con parámetros no permitidos o no adecuados (ejemplo: SPSN en SConnect) según las restricciones de la Recomendación X.400.

f) La extensión de la prueba se limita a un número razonable de casos de prueba aplicando los siguientes principios:
   1) Para comportamiento válido:
      - Si hay un número pequeño de valores de elemento de protocolo válidos, hay que probarlos todos.
      - Si hay una gama de valores, hay que probar los extremos y algunos de los valores comunes.
      - Si no hay límites, hay que probar un valor extremo más allá de los valores comunes.
   2) Para no válido:
      - El número de casos de prueba para un tipo de error especial se reduce a uno o a unos cuantos comunes.

8.3.1 *Estrategia de las pruebas X.409*

Los casos de prueba de la Recomendación X.409 definidos en los manuales de especificaciones de pruebas de conformidad del CCITT asociados con esta Recomendación son aplicables únicamente a los sistemas de tratamiento de mensajes de las Recomendaciones de la serie X.400. La prueba de X.409 se realiza como parte de las pruebas de STRM (P1), SMIP (P2), y STF. Las características sometidas a prueba son los tipos de datos definidos en la Recomendación X.409, las diversas formas de codificación de longitud y el uso de primitivas y elementos de datos constructores. Para aumentar la posibilidad de realizar las pruebas, los casos de prueba, siempre que sea posible, han sido elegidos utilizando los elementos de protocolo asociados con elementos de servicio obligatorio.

Se identifican dos categorías de pruebas X.409:

- *Pruebas de decodificación*

  Estas pruebas se establecen identificando las características de la Recomendación X.409 que deben aplicarse y fijando conjuntos de UDP de prueba codificados correcta e incorrectamente y que tengan dichas características. Las pruebas se realizan transmitiendo los UDP de prueba a la RSP y observando la reacción local de la realización y/o cualquier UDP resultante devuelta al probador.

- *Pruebas de codificación*

  Estas pruebas se establecen identificando un conjunto de peticiones de servicio de usuario que puedan generar UDP cuya codificación aplique las principales características de la Recomendación X.409. El probador debe verificar la validez de los códigos de las UDP resultantes generadas por la RSP.

  Las pruebas de decodificación permiten que las características de decodificación de una realización según la Recomendación X.409 se ejerzan plenamente utilizando UDP de prueba válidas e inválidas. Las pruebas de codificación permiten únicamente la verificación de la conducta válida de la codificación de acuerdo con la Recomendación X.409.

8.3.2 *Estrategia para la prueba de SMIP (P2)*

Se identifica dos categorías de pruebas:

- RSP como originador;
- RSP como destinatario.

Con la RSP como originador, para cada elemento de servicio aceptado por la realización se realizan pruebas:

- invocando el servicio;
- haciendo que el probador verifique la validez de las UDP resultantes;
- haciendo que el probador, según el caso, retorne UDP de respuesta válidas e inválidas al originador.

Con la RSP como destinatario, para cada elemento de servicio se realizan pruebas:

- haciendo que el probador envíe UDP válidas e inválidas para dicho servicio;
- observando la reacción local del AU;
- verificando la validez de cualquier UDP adicional generada por el AU.

Para evitar una duplicación innecesaria de casos de prueba, los elementos del servicio MIP que también sean elementos de servicio TRM (por ejemplo la notificación de entrega) se enumeran dentro de la serie de pruebas STRM (P1) conjuntamente con los elementos de servicio TRM correspondientes, y no dentro de la serie de pruebas SMIP (P2).

Se supone que la prueba de la capa TRM se realiza a través de un agente de usuario.

8.3.3 *Estrategia para la prueba de STRM (P1)*

Cuando se prueba el funcionamiento de una realización STRM (P1) se identifican cinco categorías de pruebas:

- RSP como originador;
- RSP como destinatario;
- RSP como relevador;
- RSP como destinatario de relevador;
- RSP como destinatario/originador.

Con la RSP como originador, para cada elemento del servicio aceptado por la realización, se realizan las pruebas:

- invocando el servicio;
- verificando la validez de las UDP resultantes.

Con la RSP como destinatario, para cada elemento de servicio admitido por la realización, se realizan las pruebas:

- haciendo que el probador envíe UDP válidas e inválidas a dicho servicio;
- observando la reacción local del AU;
- verificando la validez de cualquier UDP adicional generada por el AU.

Con la RSP como relevador, para cada elemento de servicio se realizan las pruebas:

- haciendo que el probador envíe UDP válidas e inválidas para relevo;
- verificando la validez de la reacción de la RSP.

Con la RSP como destinatario de relevador, para cada elemento de servicio se realizan las pruebas:

- enviando un conjunto de UDP válidas e inválidas dirigidas a más de un destinatario. Al menos, uno de estos destinatarios estará unido a la RSP y los destinatarios adicionales estarán unidos a un ATM a distancia, de tal menera que la RSP pueda enviar el mensaje por relevo;
- verificando la validez de la reacción de la RSP como destinatario;
- verificando que las UDP que son transmitidas por relevo no estén adulteradas y que sean modificadas en forma adecuada.

Con la RSP como destinatario/originador, para cada elemento de servicio aceptado por la realización, se realizan las pruebas:

- invocando a la RSP para que envíe un mensaje a múltiples destinatarios. Al menos, uno de los destinatarios estará unido a la RSP y un destinatario adicional estará unido a un ATM a distancia;
- verificando la validez de la reacción de la RSP como destinatario;
- verificando la validez de las UDP transmitidas por la RSP.

8.3.4 *Estrategia para la prueba de STF*

Se utilizan las siguientes fases de prueba:

a) *Fase de negociación y establecimiento de conexión/asociación*

La Recomendación X.410 permite diferentes opciones negociables y la fase de negociación se prueba en forma exhaustiva utilizando elementos válidos e inválidos.

b) *Liberación ordenada de la conexión/asociación*

Sólo se requieren unas cuentas pruebas para verificar la realización correcta de las características de liberación del STF.

c) *Fase de transferencia de datos con intercambio de testigos*

Las pruebas de transferencia de datos verifican:

- la operación correcta de la transferencia de datos utilizando los valores negociados;
- la operación correcta del intercambio de testigos;
- la confirmación correcta de servicios confirmados;
- la reacción correcta a elementos inválidos (por ejemplo, no negociados).

d) *Recuperación*

Se realizan pruebas para verificar que una RSP puede realizar la recuperación correcta después de:

- aborto iniciado por el usuario;
- aborto iniciado por el proveedor;
- informes de excepción;
- puntos de verificación no reconocidos.

9 Estructura de las series de pruebas

Las series de pruebas SMIP (P2) y STRM (P1) tienen una estructura común, diferente de las series de pruebas STF.

9.1 *Estructura de las series de pruebas SMIP (P2) y STRM (P1)*

Las series de pruebas SMIP (P2) Y STRM (P1) están formadas por cinco grupos de casos de prueba:

a) *Pruebas iniciales*

Las pruebas iniciales verifican las características obligatorias en un pequeño número de casos de prueba. Han sido definidas para verificar que la realización admite correctamente las principales características obligatorias y que es capaz de continuar con todas las pruebas de conformidad.

b) *Pruebas X.409*

Las pruebas X.409 verifican la codificación y decodificación de los elementos de protocolo realizada por la RSP. Las pruebas de decodificación se realizan transmitiendo UDP de prueba a la RSP. Las pruebas de codificación se realizan verificando las UDP recibidas de la RSP.

c) *Pruebas del elemento de protocolo*

Las pruebas del elemento de protocolo identifican las finalidades de prueba para cada elemento de protocolo en los protocolos SMIP (P2)/STRM (P1). Esto es importante para garantizar una cobertura de pruebas completa para los protocolos SMIP (P2)/STRM (P1). Muchas de estas pruebas son realizadas necesariamente como parte de las pruebas del elemento de servicio.

d) *Pruebas del elemento de servicio*

Las pruebas del elemento de servicio verifican la capacidad de la RSP de admitir los elementos de servicio de la Recomendación X.400. Algunas de estas pruebas son realizadas durante las pruebas iniciales y las pruebas de la Recomendación X.409. Las pruebas del elemento de servicio incluyen pruebas para elementos de servicio específicos y pruebas para combinaciones de elementos de servicio interdependientes.

e) *Prueba adicional*

El grupo de prueba adicional verifica las características no incluidas en los otros grupos de pruebas.

Como se indica en los anteriores apartados a) a e), el número de casos de prueba ha sido reducido al mínimo aprovechando el hecho de que el funcionamiento de un caso de prueba dado puede abarcar más de un objetivo de prueba. La figura 6/X.403 muestra cómo algunos de los objetivos de prueba identificados en un grupo de prueba específico pueden lograrse por medio de casos de prueba de otro grupo.

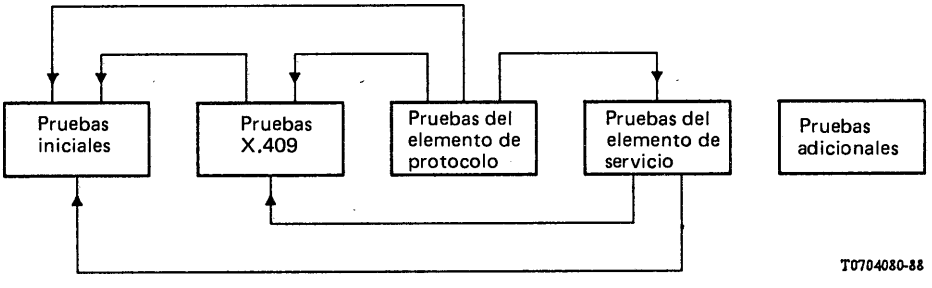


FIGURA 6/X.403

Estructura de las series de pruebas SMIP(P2) y STRM(P1)

9.2 *Estructura de la serie de pruebas STF*

La serie de pruebas STF está formada de cinco grupos de casos de prueba:

- pruebas del establecimiento de asociación;
- pruebas de liberación de asociación;
- pruebas de transferencia de datos;
- pruebas de recuperación de asociación;
- pruebas X.409.

Las pruebas del establecimiento de asociación verifican la negociación de los elementos de conexión.

Las pruebas de liberación de asociación verifican la liberación ordenada de las asociaciones.

Las pruebas de transferencia de datos verifican que los datos sean transferidos correctamente y de acuerdo con los valores de los elementos de conexión negociados durante el establecimiento de la asociación.

Las pruebas de recuperación de asociación verifican que la RSP pueda recuperarse de las interrupciones de conexión, en actividades internas y externas.

Las pruebas de la Recomendación X.409 verifican la codificación y decodificación por la RSP de los datos de usuario de servicio de sesión.

10 Información que deben suministrar los realizadores

10.1 *Enunciado de conformidad de realización de protocolo (ECRP)*

El enunciado de conformidad de realización de protocolo (ECRP), es una información suministrada por un realizador, que especifica las características de protocolo establecidas en un sistema de tratamiento de mensajes.

Esta información se utiliza durante las pruebas de conformidad:

- para verificar que las características de protocolo que han sido establecidas sean congruentes con los requisitos de conformidad, en términos de las características obligatorias y facultativas de las Recomendaciones de la serie X.400;
- para seleccionar las pruebas de originador que se realizarán. Las pruebas de destinatario y de relevo se realizarán para verificar el comportamiento del sistema, incluso cuando se le pide que maneje características que no realiza.

En los anexos B, C y D se muestran las proformas de ECRP para SMIP (P2), STRM (P1) y STF. Estas proformas especifican la información que debe suministrar un realizador respecto a:

- los servicios aceptados para las funciones de origen, recepción y relevo;
- las características de protocolo que han sido establecidas para admitir dichos servicios.

El ECRP de SMIP (P2) incluye explícitamente elementos de servicio STRM (P1) puestos a disposición por el SMIP (P2). Para evitar duplicación con la serie de pruebas (STRM (P1), las pruebas de los elementos de servicios STRM (P1) no están incluidas en la serie de pruebas SMIP (P2). Cuando la prueba de STRM (P1) se realiza sin utilizar un AU, puede ser necesario repetir las pruebas de STRM (P1) utilizando un AU para poder asegurar la conformidad con el SMIP (P2).

10.2 *Información suplementaria de realización de protocolo para pruebas (ISRP)*

La información suplementaria de realización de protocolo para pruebas (ISRP) es suministrada por un realizador, especificando la información que necesita el probador para realizar una serie de pruebas.

Las series de pruebas de SMIP (P2), STRM (P1) y STF definen el comportamiento de la realización en términos de primitivas de servicio abstracto. Para poder invocar y observar este comportamiento durante la ejecución de las pruebas, el operador de las pruebas debe conocer cómo estas primitivas de servicio abstracto (si las hay) pueden invocarse u observarse en el interfaz de usuario accesible real.

Las proformas ECRP de SMIP (P2), STRM (P1) y STF enumeran todas las primitivas de servicio abstracto de capa superior de la RSP utilizadas en las definiciones de pruebas y requerirán que el realizador especifique cómo se pueden invocar u observar estas primitivas (si las hay).

11 Notación de pruebas

11.1 *Definiciones*

La notación utilizada para expresar las especificaciones de prueba STM utiliza las siguientes definiciones:

a) **serie de pruebas**

Conjunto de casos de prueba, posiblemente combinados dentro de grupos de prueba jerarquizados, necesarios para realizar las pruebas de conformidad de una realización.

Las series de pruebas no implican una orden de ejecución.

b) **grupo de pruebas**

Conjunto de casos de prueba relacionados. Los grupos de pruebas pueden estar jerarquizados para proporcionar una estructura lógica de los casos de prueba.

c) **caso de pruebas**

Especifica la secuencia de los eventos de prueba necesarios para lograr el propósito de la prueba y asignar un veredicto de «favorable», «desfavorable» o «dudoso».

d) **evento de prueba**

Unidad indivisible de especificación de prueba a nivel de abstracción de la especificación (por ejemplo, envío o recepción de una sola UDP).

e) **usuario**

Proceso de interfaz de usuario o aplicación de computador que utiliza un STM.

11.2 *Notación*

Las series de pruebas de conformidad para los sistemas de tratamiento de mensajes utilizan la notación combinada tabular y de árbol descrita en el anexo A de la presente Recomendación.

Cada especificación de serie de prueba está formada de seis secciones:

1) *Introducción*

Contiene una descripción general del objeto de las pruebas y de la estructura de la serie de pruebas.

2) *Resumen de casos de pruebas*

Es una lista de todas las pruebas, indicando el identificador de prueba, la referencia de la prueba y un título breve para cada uno de los casos de prueba de la serie de pruebas.

3) *Parte declaraciones*

Declara los nombres y tipos de todos los elementos que serán utilizados en la definición de los casos de pruebas.

4) *Parte dinámica*

Este es el cuerpo principal de la serie de pruebas y define los casos de prueba en términos de árboles de comportamiento.

5) *Parte limitaciones*

Especifica los valores de las PSA y UDP utilizadas en la parte dinámica.

6) *Referencias recíprocas*

Proporciona un índice de todos los valores utilizados en el cuerpo principal de la serie de pruebas.

12 Procedimientos de evaluación de la conformidad (véase la figura 7/X.403)

Esta Recomendación trata únicamente de las especificaciones de pruebas abstractas para los sistemas de tratamiento de mensajes. No trata de la realización de estas especificaciones de prueba ni de su ejecución. Este apartado de las Recomendaciones tiene únicamente propósitos informativos, para describir, en términos generales, cómo pueden realizarse las pruebas reales.

12.1 *Visión de conjunto del procedimiento*

Los procedimientos necesarios para evaluar la conformidad de una realización comprenden:

- la cumplimentación de proformas ISRP y ECRP por el proveedor de la realización;
- la evaluación de estos documentos;
- la selección y ejecución de casos de prueba;
- el análisis de los resultados y la producción de informes de prueba.

12.2 *Análisis del ECRP*

La primera fase en la evaluación de la conformidad es garantizar que las características anunciadas como aceptadas por una RSP, satisfagan los requisitos de conformidad correspondientes. Los requisitos de conformidad para las realizaciones SMIP (P2), STRM (P1) y STF están definidos en el § 7 de esta Recomendación. Esta verificación se realiza analizando la información contenida en los documentos del ECRP.

12.3 *Selección de caso de prueba*

Las pruebas que deben realizarse se seleccionan principalmente sobre la base de la información contenida en los ECRP. Para cada característica aceptada, en los ECRP, se seleccionan los casos de prueba correspondientes entre las series de prueba y se ejecutan para verificar la correcta realización de estas características en una extensa gama de condiciones válidas e inválidas.

Para características no aceptadas, se ejecutarán algunos casos de prueba de destinatario para explorar las respuestas de la RSP. Puesto que en general las Recomendaciones de la serie X.400 (1984) no definen la conducta que se espera en estas situaciones, estas pruebas se pueden superar con casi cualquier comportamiento, excepto fallo catastrófico de la RSP.

La información contenida en el ISRP también puede indicar ciertas limitaciones sobre los casos de prueba que se pueden ejecutar.

12.4 *Ejecución de las pruebas*

Se recomienda que las pruebas de los sistemas de tratamiento de mensajes se lleven a cabo en el siguiente orden: primero STF, después STRM (P1), y finalmente SMIP (P2).

Sin embargo, el orden de los casos de prueba dentro de las series de prueba no implica un orden de ejecución. Con independencia de la Recomendación general de que se ejecute primero el grupo de pruebas inicial de SMIP (P2)/STRM (P1), el orden de ejecución de las pruebas puede ser determinado por los operadores de prueba, teniendo en cuenta el entorno de la prueba y los instrumentos de prueba.

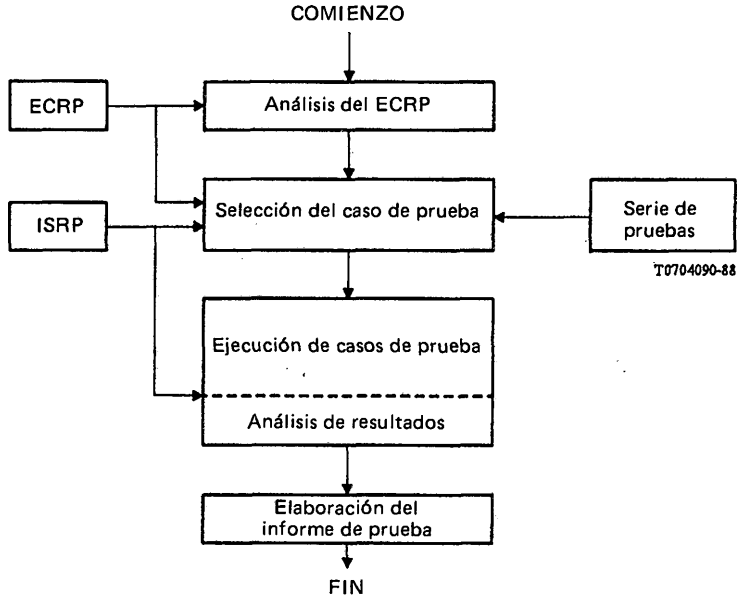


FIGURA 7/X.403

Procedimiento de evaluación de la conformidad

ANEXO A

(a la Recomendación X.403)

Notación de pruebas

A.1 *Introducción*

Este anexo forma parte integrante de la Recomendación y describe la notación utilizada en los manuales y series de prueba.

La notación de prueba que se describe se basa en la notación de prueba denominada notación combinada tabular y de árbol (NCTA) que ha sido desarrollada conjuntamente por la ISO y el CCITT.

La notación descrita en esta Recomendación se deriva de una forma inicial de NCTA y ha sido desarrollada específicamente para las especificaciones de pruebas de conformidad de los STM.

Cada una de las series de pruebas STM se especifica en cinco partes:

- parte declaración;
- parte dinámica;
- parte limitaciones;
- identificación de caso de prueba;
- referencias recíprocas.

A.2 *Parte declaración*

La parte declaración declara el entorno y los objetos utilizados en las series de prueba y está compuesta de siete secciones:

- configuraciones de prueba;
- parámetros de la serie de pruebas (PSP);
- puntos de acceso al servicio (PAS);
- primitivas de servicio abstracto (PSA);
- unidades de datos de protocolo (UDP);
- temporizadores;
- abreviaturas.

A.2.1 *Configuraciones de prueba*

En esta sección se enuncian los puntos de control y observación.

A.2.2 *Parámetros de la serie de pruebas*

Cada serie de pruebas STM tiene un conjunto de parámetros cuyos valores se fijan antes de hacer la prueba y se utilizan para definir un entorno de prueba específico.

Los PSP se presentan en forma tabular tal como se muestra en la figura A-1/X403.

PARÁMETROS DE LA SERIE DE PRUEBAS		
NOMBRE	TIPO y LIMITACIONES	COMENTARIOS

FIGURA A-1/X.403

Parámetros de la serie de pruebas

Por convenio, el nombre de cada parámetro de la serie de pruebas de la serie de prueba STM tiene la forma:

PSP_ <nombre>

A.2.3 *Puntos de acceso al servicio (PAS)*

Los puntos de acceso al servicio se utilizan como puntos de control y observación en las series de prueba STM y se presentan en forma tabular como se indica en la figura A-2/X.403.

PAS	
NOMBRE	PAPEL

FIGURA A-2/X.403

Puntos de acceso al servicio

Por convenio, el nombre de un PAS en la serie de prueba STM es generalmente una letra mayúscula, como T, U, V (para PAS del probador) o I, J, K (para PAS de la RSP).

A.2.4 *Primitivas de servicio abstracto*

Cada tipo de PSA y sus parámetros asociados utilizados en la serie de pruebas se presentan en forma tabular como se indica en la figura A-3/X.403.

PSA:	PAS:	COMENTARIO:	
NOMBRE	GAMA DE VALORES O TIPO	COMENTARIOS	C/O

FIGURE A-3/X.403

Primitivas de servicio abstracto

El nombre de la PAS se anota en el campo «PAS» y se deriva del nombre correspondiente en las Recomendaciones de la serie X.400. El PAS en la que se presenta la PSA se anota en la columna «NOMBRE», junto con la información en las «Condiciones/Obligatorio» (C/O).

Puesto que las Recomendaciones no definen PSA de SMIP (P2), para describir las pruebas de conformidad ha sido necesario establecer PSA ficticias en el límite superior de la capa de agente de usuario. Sin embargo, esto no implica que los fabricantes deban establecer estos PSA en sus sistemas. Únicamente sirven para formalizar los requisitos de observación e invocación de los elementos del servicio de SMIP utilizando estas nuevas PSA. La relación entre los elementos de servicio SMIP y la conducta real de la RCP debe especificarse en el ECRP, de acuerdo con la realización.

A.2.5 *Unidades de datos de protocolo*

Los tipos de UDP utilizadas en la serie de pruebas se presentan en forma tabular, como se muestra en la figura A-4/X.403. Estas UDP no están definidas explícitamente en las series de pruebas, sino que se presentan como una referencia exacta a la definición completa en las Recomendaciones de la serie X.400, dentro de la sección de tipo del cuadro.

DECLARACIÓN DE TIPO DE DATOS
COMENTARIOS:
NOMBRE DE TIPO:

FIGURA A-4/X.403

Unidades de datos del protocolo

A.2.6 *Temporizadores*

Esta sección indica los temporizadores que deben utilizarse. Los valores de temporizador son expresiones en términos de parámetros de series de prueba, y son fijos para la totalidad de las series de prueba. Los valores del temporizador se enuncian en forma tabular, como se indica en la figura A-5/X.403.

DECLARACIÓN DE TEMPORIZADOR		
NOMBRE DEL TEMPORIZADOR	VALOR	COMENTARIO

FIGURA A-5/X.403

Temporizadores

A.2.7 *Abreviaturas*

Las abreviaturas utilizadas en la serie de prueba se definen en forma tabular como se indica en la figura A-6/X.403.

ABREVIATURAS		
ABREVIATURA	NOMBRE COMPLETO	COMENTARIO

FIGURA A-6/X.403

Abreviaturas

A.3 *Parte dinámica*

La parte dinámica define los casos de prueba de una serie de pruebas en forma de árboles de comportamiento.

Los § A.3.1 y A.3.2 describen, en términos generales, cómo se definen los árboles de comportamiento.

El § A.3.3 describe el contenido y uso de la biblioteca por defecto.

El § A.3.4 describe el contenido y uso de la biblioteca de paso de prueba.

El § A.3.5 describe cómo se especifica cada caso de prueba en el cuerpo principal de una serie de pruebas.

A.3.1 *Cuadro proforma de comportamientos de prueba* (véase la figura A-7/X.403)

<título> COMPORTAMIENTO				
IDENTIFICADOR: <usado únicamente para bibliotecas>				
COMENTARIOS: <usado únicamente para bibliotecas>				
POR DEFECTO:				
DESCRIPCIÓN DE COMPORTAMIENTO	ETIQUETA	REFERENCIA DE LIMITACIONES	COMENTARIOS	RESULTADOS
Comentarios ampliados: <facultativo>				

FIGURA A-7/X.403

Descripción de comportamiento

<título> COMPORTAMIENTO:

Título del comportamiento: POR DEFECTO para la biblioteca por defecto; DINÁMICO para la biblioteca de paso de prueba y casos de prueba.

IDENTIFICADOR:

Proporciona un identificador único para la descripción de comportamiento.

POR DEFECTO:

Enumera los identificadores de las descripciones de comportamiento por defecto que deben utilizarse junto con el comportamiento dinámico que aparece en la parte «DESCRIPCIÓN DE COMPORTAMIENTO».

DESCRIPCIÓN DE COMPORTAMIENTO:

Se define el comportamiento de la prueba utilizando una notación de árbol tal como se describe en el § A.3.2.

ETIQUETA:

La columna ETIQUETA puede utilizarse para identificar sucesos. Las ramas entre los sucesos (es decir, «GO TO») se especifican por «Etiqueta → » en el árbol de comportamiento.

REFERENCIA DE LIMITACIONES:

Para cada comportamiento de la PSA de la línea del árbol de comportamiento, esta columna proporciona la referencia del valor específico PSA definido en la parte de limitaciones.

COMENTARIOS:

Esta columna permite los comentarios que facilitan la comprensión de los eventos. Los comentarios adicionales pueden proporcionarse en la zona de «comentarios ampliados». Esta columna también puede utilizarse para identificar UDP de prueba asociadas con los eventos de prueba.

RESULTADO:

Esta columna indica qué eventos de prueba generan veredictos de prueba. Los valores de los veredictos de prueba son:

- Favorable: No se detectó ningún error de comportamiento en la RSP.
- Desfavorable: Se detectó un comportamiento falso en la RSP.
- Dudoso: El comportamiento observado no permite la asignación de un veredicto de aprobado o fallado.

A.3.2 *Notación de árbol para comportamiento de prueba*

Los árboles de comportamiento se definen en términos de eventos que, generalmente, tienen la forma:

<PAS>!<evento>

o la forma:

<PAS>?<evento>

El <PAS> es el punto de control y observación en el cual ocurre el <evento>. Los PAS utilizados son los mencionados en la parte declaración.

El símbolo «!» indica que el evento fue enviado desde el PAS y «?» indica que el evento es recibido en el PAS.

El <evento> puede ser:

- un evento PSA;
- un evento temporizador;
- un seudoevento OTHERWISE (DEOTRAFORMA).

A.3.2.1 *Eventos PSA únicos*

Si el <evento> es un evento PSA, los nombres de las PSA están especificados en la parte de declaración (el valor se especifica como una referencia en la columna REFERENCIA DE LIMITACIONES).

Renglón de ejemplo para un evento PSA:

I?DELind

Esto significa que se recibió una indicación de entrega en el PAS de la RSP I.

A.3.2.2 *Eventos de temporizador únicos*

Si el <evento> es un evento temporizador, estará en la forma de:

<operación> <parámetro>

La operación de «arranque» puede tomar una de dos formas:

Arranque <tipo de temporizador>

Arranque (<tipo de temporizador>, <identificación del temporizador>)

donde <tipo de temporizador> se define en la parte de declaración y tiene un valor fijo asociado, definido en términos de PSP. La <identificación del temporizador> permite unir un nombre a un caso de tipo de temporizador.

Las otras operaciones son:

- Cancelar: cancela un temporizador en marcha o suspendido;
- Suspender: suspende un temporizador en marcha;
- Reiniciar: reinicia un temporizador suspendido;
- Temporización: expiración de un temporizador en marcha.

Estas operaciones pueden tomar una de dos formas:

<operación> <tipo de temporizador>

<operación> <identificador de temporizador>

donde <operación> designa la operación. Cuando un temporizador fue arrancado utilizando la forma «arranque <tipo de temporizador>», se debe utilizar la forma «<operación> <tipo de temporizador>»; cuando se arrancó el temporizador utilizando la forma «arranque <identificador del temporizador>», debe utilizarse la forma «<operación> <identificador del temporizador>».

Ejemplo:

I!Arranque T/I-temporizador_1

significa que en el PAS de la RSP I se arrancó el T/I-temporizador_1 (por ejemplo para el tiempo de transmisión necesario para transferir un UDPAU desde el probador hasta el usuario de la RSP).

I?Temporización T/I-temporizador_1

significa que se recibió en el PAS de la RSP la temporización del temporizador mencionado.

A.3.2.3 *Eventos OTHERWISE únicos*

Si el <evento> es un seudoevento OTHERWISE, esto indica un evento no especificado.

Ejemplo:

T?OTHERWISE

significa que en el PAS T del probador se recibió un evento no especificado.

A.3.2.4 *Árboles de comportamiento*

Los árboles de comportamiento combinan eventos en dos formas:

- como secuencias de eventos;
- como sucesos alternativos.

Los dos tipos de combinaciones se diferencian por su respectiva alineación vertical y de sangrado.

Ejemplo de una secuencia de eventos:

I!SUBreq
 I?SUBcon
  T?TRNind

Esto significa que el PAS I envía primero una petición de depósito, después el mismo PAS recibe una confirmación de depósito, tras de lo cual el PAS T del probador recibe una indicación de transferencia.

Ejemplo de eventos alternativos:

T?DELind
T?Temporización I/T-temporizador

Esto significa que el PAS T recibió una indicación de entrega, o bien recibió la temporización.

Para constituir un árbol de comportamiento complejo, se pueden mezclar los dos tipos de combinaciones.

Ejemplo:

I!SUBreq
 I?SUBcon } eventos alternativos
  T?TRNind }
T?DISind

Esto significa que después de enviar I una petición de depósito se recibió en I una confirmación de depósito, seguida por la recepción en T de una indicación de transferencia, o se recibió en T una indicación de desconexión.

A.3.3 *Biblioteca por defecto*

Los comportamientos por defecto generales que se utilizan en varios casos de prueba se definen en la biblioteca por defecto utilizando el formato que se muestra en la figura A-8/X.403. El nombre del defecto tiene la siguiente forma:

BIB_ <nombre>

o

BIB_ <nombre> [X]

donde X reserva un lugar que es reemplazado por un PAS real cuando el elemento por defecto se aplica a un caso de prueba individual.

Nota – Cuando el comportamiento por defecto individual se aplica a un solo caso de prueba, la tabla de comportamiento está asociada con dicho caso de prueba y el identificador no lleva el prefijo «BIB_».

COMPORTAMIENTO POR DEFECTO				
IDENTIFICADOR POR DEFECTO: BIB_				
COMENTARIOS:				
POR DEFECTO:				
DESCRIPCIÓN DE COMPORTAMIENTO	ETIQUETA	REFERENCIA DE LIMITACIONES	COMENTARIOS	RESULTADOS
Comentarios ampliados: <facultativo>				

FIGURA A-8/X.403

Comportamiento por defecto

A.3.4 *Biblioteca de paso de prueba* (véase la figura A-9/X.403)

Cuando se utiliza una secuencia de pasos de prueba en varios casos de prueba, pueden incluirse en la biblioteca de pasos de prueba y reciben un nombre en la forma siguiente:

BIB_ <nombre>

Nota – Cuando un paso de prueba se aplica a un solo caso de prueba la tabla de comportamiento está asociada a dicho caso de prueba y el identificador no lleva el prefijo «BIB»_.

A.3.5 *Caso de prueba* (véase la figura A-10/X.403)

Cada caso de prueba del cuerpo principal de la serie de prueba se describe en términos de tres encabezamientos [a) a c)], y un árbol de comportamiento [d)].

a) *Referencia de prueba e identificador de prueba*

Estos elementos dan una referencia e identificador únicos para cada caso de prueba y se describen en su totalidad en el § A.5.

b) *Resumen*

Proporciona una breve descripción general de la finalidad de la prueba.

c) *Descripción de la prueba (facultativa)*

Proporciona una descripción oficiosa de las acciones y eventos que deben realizarse durante la prueba, así como los criterios oficiosos para el veredicto.

d) *Árbol de comportamiento*

El comportamiento dinámico se describe utilizando la notación de árbol definida en el § A.3.2.

COMPORTAMIENTO DINÁMICO				
IDENTIFICADOR PASO DE PRUEBA: BIB_				
COMENTARIOS:				
POR DEFECTO:				
DESCRIPCIÓN DE COMPORTAMIENTO	ETIQUETA	REFERENCIA DE LIMITACIONES	COMENTARIOS	RESULTADOS
Comentarios ampliados: <facultativo>				

FIGURA A-9/X.403

Comportamiento de paso de prueba

COMPORTAMIENTO DINÁMICO				
POR DEFECTO: (Véase la nota 1)				
DESCRIPCIÓN DE COMPORTAMIENTO	ETIQUETA	REFERENCIA DE LIMITACIONES	COMENTARIOS	RESULTADOS
(Véase la nota 2)				(Véanse las notas 3 y 4)
Comentarios ampliados: <facultativo>				

Nota 1 – En este campo se insertan todos los identificadores de biblioteca por defecto utilizados. Cuando sea necesario, también se identificará el PAS al cual se aplicaron. Si, por ejemplo, el campo contiene la inscripción:

BIB_inesperado [T]

ello significa que el subárbol asociado con este comportamiento por defecto se considera asociado al PAS T.

Nota 2 – El comportamiento de la biblioteca de paso de prueba se incluye en el árbol de comportamiento utilizando la siguiente notación:

+ <Identificador de biblioteca de paso de prueba>.

Nota 3 – El árbol de comportamiento de cada paso de prueba proporciona los veredictos de favorable, desfavorable y, si procede, dudoso.

Nota 4 – Cuando se utilizan los elementos de la biblioteca por defecto, es posible que algunas de las alternativas de veredicto queden «ocultas» en el elemento de la biblioteca por defecto.

FIGURA A-10/X.403

Comportamiento de caso de prueba

A.4 *Parte de limitaciones* (véase la figura A-11/X.403)

La parte de limitaciones de una serie de pruebas especifica los valores y codificación para todos los casos de PSA, UDP de prueba, UDP de base y componentes de la biblioteca. La parte de limitaciones está dividida en las siguientes secciones:

- introducción a la parte de limitaciones;
- limitaciones PSA;
- limitaciones UDP de prueba;
- limitaciones UDP de base;
- biblioteca de componentes.

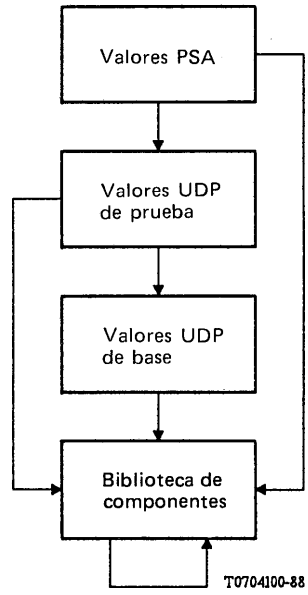


FIGURA A-11/X.403

Estructura de la parte de limitaciones

A.4.1 *Limitaciones PSA*

Los valores de las PSA se definen como casos específicos de un PSA genérico.

A.4.1.1 *Especificación de una PSA «genérica»*

Una PSA genérica se define utilizando el formato que aparece en la figura A-12/X.403.

La columna «CAMPOS» se utiliza para enumerar todos los parámetros de la PSA.

La columna «VALOR o REFERENCIA» se utiliza para especificar un valor para cada parámetro, lo cual puede hacerse de cuatro formas:

a) como referencia que puede ser un nombre PSP o un nombre de componente de biblioteca;

b) como un valor explícito;

c) como «–» para indicar que este parámetro puede omitirse en casos específicos de esta PSA.

d) como «?» para indicar que, si hay interés en este componente, y para las PSA «petición», este parámetro debe tener un valor definido en un caso particular.

<nombre PSA>	<nombre abreviado>	GENÉRICO
CAMPOS	VALOR o REFERENCIA	COMENTARIO
<campo_1>	<instante PSP>	O
<campo_2>	<componente BIB>	O
<campo_3>	?	C
<campo_4>	–	no aplicable
<campo_5>	–	C

FIGURA A-12/X.403

Especificación de una PSA genérica

A.4.1.2 *Especificaciones de casos de PSA*

Los valores específicos de las PSA se definen utilizando el formato tabular que aparece en la figura A-13/X.403.

<nombre PSA>	<nombre genérico abreviado>	CASOS
NOMBRE DEL CASO	PARÁMETRO MODIFICADO	VALOR o REFERENCIA
<caso_1>	<campo_3>	<prueba_udp_1>
<caso_2>	<campo_3> <campo_6>	<prueba_udp_2> <componente BIB>
<caso_3>	<campo_3> <campo_7> <campo_8>	<prueba_udp_3> <instante PSP> <valor dado>

FIGURA A-13/X.403

Valor de PSA específica

La columna «NOMBRE DEL CASO» se utiliza para identificar casos específicos de la PSA utilizada en la serie de pruebas.

La columna «PARÁMETRO MODIFICADO» identifica, para las PSA «petición», aquellos parámetros cuyos valores deberán modificarse a partir de la especificación PSA genérica, y para las PSA «notificación» aquellos parámetros cuyos valores deben verificarse.

La columna «VALOR o REFERENCIA» puede contener valores específicos o referencias a los componentes de biblioteca de la PSA o UDP de prueba.

A.4.2 *Especificación de valores UDP*

La serie de prueba STM contiene un gran número de valores UDP de prueba. Cada UDP está definido en términos de modificaciones a uno de los pocos UDP de «base».

Por comodidad, los componentes UDP que se utilizan comúnmente están definidos en una biblioteca y son utilizados por las UDP de prueba y UDP de base como referencia.

A.4.3 *UDP de base*

A.4.3.1 *Especificación de UDP de base*

Las UDP de base en sí mismas, no se utilizan como UD de prueba, pero sirven de base para derivar las UDP de prueba. Normalmente, sólo hay que especificar unas pocas UDP de base.

El nomre de una UDP de base tiene la siguiente forma:

BASE_ <UDPtipodenombre> _ <número>

Ejemplo de una UDP de base:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
BASE_IM-UAPDU_1		
SEQUENCE {		
Heading	[BASE_IM-UAPDU_1_Heading]	
Body	[BASE_IM-UAPDU_1_Body]	
}		
BASE_IM-UAPDU_1_Heading		
SET {		
IPMessageID	[L_IPMessageID_20]	
}		
BASE_IM-UAPDU_1_Body		
SEQUENCE OF {		
BodyPart	[L_BodyPart_20]	
}		

El valor o la referencia de valor de cada elemento de la estructura se especifica dentro de corchetes («[» y «]») bajo el encabezamiento de VALOR o REFERENCIA.

Cuando se especifica, para pruebas de codificación/decodificación, la codificación de una UDP, se utilizan dos columnas adicionales para especificar el código de identificación [ID] y el indicador de longitud [LI] de cada elemento de la UDP. El formato para esto se muestra en el siguiente ejemplo:

DESCRIPCIÓN	ID	LI	VALOR o REF	COMENTARIO
L_Phantasy_2				
SEQUENCE {	['AO'H]	[LI]		IA5Text
SET {	['31'H]	[LI]		
repertoire INTEGER	['80'H]	[LI]	[5]	ia5
}				
IA5String	['36'H]	['8106'H]		constructor
	['04'H]	['01'H]	[«1»]	
	['04'H]	['02'H]	[«23»]	
}				

Los valores de ID y LI pueden especificarse en forma explícita para permitir la definición de códigos inválidos y varias formas de códigos válidos. Se utiliza la abreviatura nemotécnica «LI» para indicar que se permite cualquier codificación válida de longitud.

A.4.3.2 *Identificación de los componentes que deben modificarse*

Un componente que vaya a ser reemplazado en una UDP se identifica por un trayecto a través de la declaración de la UDP. El trayecto se representa como una lista de elementos, cada uno separado del siguiente por medio de «.». Los elementos de la lista pueden ser etiquetas que aparecen en un UDP DE BASE, componentes que aparecen en el lado izquierdo de una declaración etiquetada, o componentes que aparecen en el lado izquierdo de la expansión de una referencia de biblioteca, en el lado derecho de una declaración.

Por ejemplo, considérense las siguientes definiciones:

```
Instance_
   SET{
      a                 [value]
      b                 [L_Component_1]
   }

L_Component_1
   SET{
      c                 [value]
      d                 [L_Component_2]
   }

L_Component_2
   SEQUENCE
      e                 [value]
   }
```

Nota – [L_Component_1] está en la biblioteca de componente.

Para hacer referencia a «a», el trayecto debe ser instance_1.a

Para hacer referencia a «e», el trayecto debe ser instance_1.b.d.e.

A.4.4 *UDP de prueba*

Las UDP de prueba se definen en términos de operaciones sobre las UDP de base. Estas operaciones se refieren a los componentes de biblioteca, PSP o valores específicos.

Hay dos tipos de UDP de prueba:

– *UDP enviadas por el probador* (RSP como destinatario)

  Por convenio, los nombres de estas UDP se presentan en la forma

  <UDP nombre>_x_<número>

  donde *x* es el número de UDP de base de la cual se derivan las UDP de prueba.

– *UDP recibidas por el probador* (RSP como originador)

  Por convenio, los nombres de estas UDP presentan la forma

  <UDP nombre>_0_<número>

  donde «0» indica que estas UDP de prueba no se derivan de una UDP de base.

A.4.4.1 *UDP de prueba enviadas por el probador*

Una UDP de prueba enviada por el probador a la RSP, normalmente se forma a partir de una UDP de base por medio de la operación REPLACE (REEMPLAZAR).

La especificación tiene la siguiente forma:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
<test PDU to be specified>		
<base PDU to be used> REPLACE <base PDU part> BY <partial ASN.1 tree>	[<value>]	

Para los convenios de asignación de valores, véase el § A.4.6.

Ejemplo:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
IM-UAPDU-1-18		

BASE_IM-UAPDU_1
REPLACE
  BASE_IM-UAPDU. Heading
BY
  SET {
  IPMessageID
  originator ORDescriptor
}
	
	[L_IPMessageID_7]
	[L_ORDescriptor_11]
		
		Library Components

Para construir en las UDP de prueba componentes inválidos que hayan de ser enviados por el probador, algunas veces se utiliza la operación abstracta REDEFINE (REDEFINIR). Se utiliza conjuntamente con la operación REPLACE en la siguiente forma:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
<test PDU to be specified>		
REDEFINE <Type to be redefined> <base PDU to be used> REPLACE <base PDU part> BY <partial ASN.1 tree>	 :: = <new definition> [<value>]	

El alcance del nuevo tipo definido está limitado a la definición UDP que contiene la operación REDEFINE.

Adviértase que si el <valor> es una referencia a un elemento definido en otra parte (por ejemplo, un PSP o un componente de biblioteca), la definición del nuevo tipo no afecta al propio elemento referenciado, sino únicamente a su utilización en la UDP real.

Ejemplo:

```
IM_UAPDU_1_3

REDEFINE
ORName :: = [APPLICATION 1] IMPLICIT SEQUENCE {
                                P1.StandardAttributeList
                                P2.DomainDefinedAttributeList      OPTIONAL
BASE_IM_UAPDU_1
REPLACE
   BASE_IM_UAPDU_1_Heading
BY
   SET {
        IPMessageID                                    [L_IPMessageID_1]
        originator ORDescriptor                        [L_ORDescriptor_1]
}
```

El error que se debe construir aquí es la etiqueta errónea del tipo ORName (la etiqueta correcta sería [APLICATIÓN 0]). El alcance de la definición de tipo erróneo creada por «REDEFINE» está limitado a todas las veces que se presente ORName en la definición de IM_UDPAU_1_3. Esto significa que se utiliza L_ORDescripor_1 con el tipo ORName modificado, mientras que la utilización de este componente de biblioteca en otras UDP o componentes permanece inalterada.

A.4.4.2 *UDP de prueba recibidas por el probador*

Para las UDP recibidas, normalmente sólo una parte de la UDP se relaciona con la finalidad de la prueba.

Un componente que reviste interés es identificado y se le asigna su valor utilizando las técnicas descritas en el § A.4.3.

El esquema de especificación tiene la siguiente forma:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
<test PDU to be specified>		
Partial definition – Components of interest		
<Test PDU part>	[<value>]	

Ejemplo:

DESCRIPCIÓN		VALOR o REFERENCIA	COMENTARIO
SR-UAPDU-0-95			
Partial definition – Components of interest			
SR-UAPDU.CHOICE.nonReceipt			
reason	INTEGER	[1]	autoforward
comments	PrintableString	["on holiday]	
returned	IM-UAPDU	[L_IMUAPDU_2]	
SR-UAPDU.report			
IPMessageID		[L_IPMessageID_15]	

A.4.5 *Biblioteca de componentes*

Los componentes de las UDP están definidos en la biblioteca y se mencionan en las especificaciones de UDP de base, en las especificaciones de UDP de prueba y en otros componentes de la biblioteca.

El nombre de un componente de biblioteca tiene la forma:

L_ <NSA.1 nombre de tipo> _ <número>

y se especifica utilizando las técnicas descritas en el § A.4.3.

Ejemplo:

DESCRIPCIÓN	VALOR o REFERENCIA	COMENTARIO
L_Phantasy_1		
SEQUENCE {		
SET {		
SET {		
ContentType	[2]	p2
originator		
PI.ORName	[TSP_ORName_1]	Test Suite Parameter
original		
SET {BIT STRING}	[{'20H'}]	IA5 Text
DeliveryFlags	['40H']	Conversion Prohibited
thisRecipient		
PI.ORName	[TPS_ORName_1]	
submission TIME	[TPS_UTCTime_1]	
}		
}		
IM-UAPDU	[L_IM-UAPDU_1]	Library Cpt
}		

A.4.6 *Convenios de valor*

Cuando se definen valores o referencias de valor para los componentes UDP, se aplican los siguientes convenios:

Las referencias de valor identifican componentes definidos dentro de la biblioteca de componentes o dentro de la sección de parámetros de la serie de prueba. Los valores CharacterString pueden especificarse dentro de dobles comillas (por ejemplo, «abc»); los valores BitString se especifican dentro de apóstrofos (por ejemplo 'OA' H ó '0001'B; notación hexadecimal o notación binaria); los valores enteros se especifican como caracteres numéricos (por ejemplo, 2); los conjuntos y secuencias de valores se especifican dentro de llaves, separados por una coma (por ejemplo {«abc», 'OA'H}).

Para las UDP enviadas por el probador:

[?] indica que el valor no influye sobre la prueba y que puede ser cualquier valor legal acorde con la norma de protocolo o con el servicio correspondiente.

[–] Indica que el parámetro está ausente.

[*] Indica que el valor será insertado por el probador antes de la ejecución de la prueba.

Para las UDP recibidas por el probador:

[?] indica que el probador no necesita verificar el valor del parámetro.

[–] indica que el probador verificará la ausencia del parámetro.

Obsérvese que los símbolos «?» y «–» en las asignaciones de valores de los componentes UDP tienen otro significado que «?» y «–» en los esquemas de PSA genéricas.

A.5 *Identificación del caso de prueba*

Los casos de prueba se identifican totalmente utilizando cuatro componentes:

- un identificador de grupo de prueba;
- un identificador de subgrupo;
- un identificador de validez;
- un número de prueba;

Estos cuatro componentes se especifican en dos formas equivalentes:

- como referencia de prueba, en la que los cuatro componentes son textuales y descriptivos.

  Ejemplo: OriginalEncodedInfoTypeIndication/Recipient/Valid/2

- como un identificador de prueba, donde los cuatro componentes son numéricos y conocidos.

  Ejemplo: 307.2.1.2.

A.5.1 *Identificación de SMIP (P2) y STRM (P1)*

A.5.1.1 *Grupos de prueba*

Para los grupos de prueba se han asignado intervalos de números como se indica a continuación:

Pruebas iniciales	001 - 099
Pruebas X.409	100 - 199
Pruebas de los elementos de protocolo (para los elementos que se presentan con frecuencia)	200 - 299
Pruebas de los elementos de servicio X.400	300 - 399
Pruebas adicionales	400 - 499

A.5.1.2 *Subgrupos*

Se han asignado identificadores numéricos a los subgrupos de pruebas como se indica a continuación:

Originador	1
Destinatario	2
Codificador	1
Decodificador	2
Relevador	3
Relevador-destinatario	4
Relevador-originador	5

A.5.1.3 *Identificadores de validez*

Los casos de prueba que ejercen un comportamiento válido se diferencian de los que ejercen la reacción de la RSP ante un comportamiento no válido utilizando los identificadores numéricos que se indican seguidamente:

Válido	1
No válido	2

A.5.1.4 *Números de caso de prueba*

Los casos de prueba para un grupo/subgrupo/validez especial están numerados en forma secuencial.

A.5.2 *Identificación STF*

A.5.2.1 *Grupos de prueba*

Se han asignado intervalos de números para los grupos de prueba, como se muestra a continuación:

Establecimiento de la asociación	1
Liberación de la asociación	2
Transferencia de datos	3
Recuperación de asociación	4
Pruebas X.409	5

A.5.2.2 *Subgrupos*

Se han asignado identificadores numéricos a los subgrupos STF, como se muestra seguidamente:

Iniciador	1
Respondedor	2
Emisor	1
Destinatario	2

A.5.2.3 *Identificadores de validez*

Los casos de prueba que ejercen un comportamiento válido se diferencian de los que ejercen la reacción de RSP ante un comportamiento inválido e inoportuno utilizando identificadores numéricos, como se muestra seguidamente:

Válido	1
No válido	2
Inoportuno	3

A.6 *Referenciación recíproca*

A.6.1 *Numeración de referencias recíprocas*

Las series de pruebas STRM (P1) y SMIP (P2) contienen un sistema de referencias recíprocas para las PSA, UDP de prueba y componentes de biblioteca. Las referencias recíprocas aparecen en los márgenes derecho e izquierdo de la serie de pruebas como se muestra en la figura A-14/X.403.

Los números en el margen izquierdo de la serie de pruebas están en orden secuencial y son «identificadores de lugar». Se presentan siempre que una PSA, UDP de prueba o componente de biblioteca se encuentra dentro de la serie de pruebas.

Cada vez que se presenta una PSA, UDP de prueba o componente de biblioteca, también se ponen números en el margen derecho. Estos números son referencias hacia adelante o hacia atrás respecto a los identificadores de lugar de las otras apariciones de las PSA, UDP de prueba o componente de biblioteca.

Cuando no puede encontrarse una referencia hacia atrás o hacia adelante, se imprime un punto («.») en el margen derecho. Este no debe aparecer en las series de pruebas totalmente definidas.

Cuando un renglón en la serie de pruebas contiene más de una PSA, UDP de prueba o componente de biblioteca, las referencias recíprocas para cada elemento del renglón se separan por medio de barras verticales («|») en el margen derecho, tal como se muestra en la figura A-15/X.403.

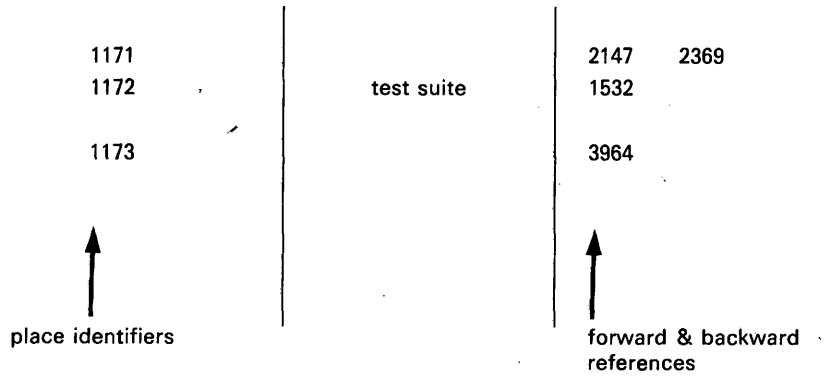


FIGURA A-14/X.403

Referenciación recíproca

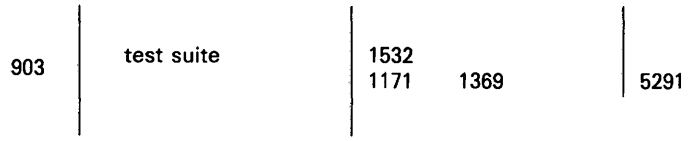


FIGURA A-15/X.403

Referencias recíprocas múltiples

A.6.2 *Listado de las referencias recíprocas*

Al final de la serie de pruebas STRM (P1) y SMIP (P2) hay un listado de las referencias recíprocas de todas las PSA, UDP de prueba y componentes de biblioteca junto con los identificadores de lugar de todas las veces que aparecen dentro de la serie de pruebas.

Ejemplo:

```
:
:
:
IM_UAPDU_1_14          586 1467
IM_UAPDU_1_15          587 1470
:
:
:
```

Los números de la derecha indican los lugares en los que ese elemento aparece dentro de la serie de pruebas.

ANEXO B

(a la Recomendación X.403)

Proformas ECRP de SMIP(P2)

B.1 *Generalidades*

Como prerrequisito para las pruebas de conformidad, el proveedor de un sistema SMIP(P2) debe proporcionar un enunciado de conformidad de realización de protocolo (ECRP).

La proforma ECRP SMIP(P2) contenida en este anexo especifica la información que debe suministrarse.

Esta información es necesaria para la selección del caso de prueba. Los proveedores deben tener en cuenta que se realizarán pruebas para verificar que los servicios anunciados como no admitidos de hecho no están presentes, en vez de estar realizados incorrectamente.

La ECRP SMIP(P2) se divide en dos partes:

- una parte que solicita información relativa a la aceptación de los elementos de servicio;
- una parte que solicita información relativa a la aceptación de los elementos del protocolo.

La información sobre la aceptación del elemento de servicio se solicita en forma de cuadro en el que, para cada elemento de servicio:

- se indica, en las columnas «STD», la condición del elemento de servicio como obligatorio (O), facultativo (F) o no aplicable (–);
- el proveedor indica, en las columnas «IMP» la aceptación real del elemento de servicio por parte de la realización en el origen y el destino.

La información sobre la aceptación del elemento del protocolo se solicita en forma de cuadro, donde para cada elemento de protocolo:

- se indica la condición del elemento del protocolo al origen y en el destino como obligatorio (O), o facultativo (F) en las columnas denominadas («STD»);
- se indica cualquier limitación a la realización en la columna denominada «CONST STD», en donde las limitaciones se interpretan como un mínimo para recepción y un máximo para origen;
- el proveedor indica, en la columna «STATUS IMP» la aceptación real del elemento de servicio por parte de la realización en el origen o en el destino;
- el proveedor indica en las columnas «CONST IMP» las limitaciones reales de la realización en el origen y en el destino.

  Las limitaciones pueden expresarse como una longitud o tamaño (octetos, bits, ...), un valor (32k – 1) o el número de veces que ocurre el suceso (4), según el elemento que se limita.

B.2 *Proforma de los elementos de servicio ECRP SMIP(P2)*

Los requisitos de las Recomendaciones X.400 se muestran en las columnas STD de la proforma utilizando las siguientes claves:

O Elemento obligatorio (Recomendación X.401, básico o esencial facultativo)

F Elemento facultativo (Recomendación X.401, adicional facultativo)

– Elemento de servicio no aplicable.

Los proveedores de una realización deben utilizar las columnas IMP de la proforma para especificar la información relativa a la aceptación de los elementos de servicio. Se sugiere, por conveniencia, que los proveedores indiquen únicamente con una «X» los elementos de servicio que no se admiten.

B.3 *Proformas de los elementos de protocolo SMIP(P2) ECRP*

En las columnas STATUS STD de las proformas, en los cuadros B-2/X.403 a B-4/X.403 se muestran los requisitos de las Recomendaciones X.400 utilizando las siguientes claves:

O Elemento obligatorio (Recomendación X.401, básico o esencial facultativo)

F Elemento facultativo (Recomendación X.401, adicional facultativo).

CUADRO B-1/X.403

Proforma de los elementos de servicio SMIP (P2)

ELEMENTO DE SERVICIO	ORIGEN		RECEPCIÓN	
	STD	IMP	STD	IMP
Identificación de mensaje IP	O		O	
Cuerpo tipificado	O		O	
Indicación de destinatario en copia ciega	F		O	
Notificación de no recepción	F		F	
Notificación de recepción	F		F	
Indicación de autoreenviado	F		O	
Indicación del originador	O		O	
Indicación de usuarios autorizantes	F		O	
Indicación de destinatarios de copia primaria	O		O	
Indicación de fecha de expiración	F		O	
Indicación de referencia recíproca	F		O	
Indicación de importancia	F		O	
Indicación de obsolescencia	F		O	
Indicación de sensibilidad	F		O	
Indicación de tema	O		O	
Indicación de respuesta a mensaje IP	O		O	
Indicación de petición de respuesta	F		O	
Indicación de mensaje IP reenviado	F		O	
Indicación de encripción de parte del cuerpo	F		O	
Cuerpo con múltiples partes	F		O	
Receptor alternativo admitido	F		F	
Prohibición de conversión	O		O	
Entrega diferida	O		–	
Cancelación de entrega diferida	F		–	
Notificación de entrega	O		–	
Publicación de otros destinatarios	F		O	
Conversión explícita	F		–	
Grado de selección de entrega	O		O	
Entrega a múltiples destinos	O		–	
Prevención de la notificación de no entrega	F		–	
Sonda	F		–	
Devolución del contenido	F		–	
Asignación de destinatario alternativo	–		F	
Retener para entrega	–		F	
Conversión implícita	F		F	

Los elementos de protocolo que corresponden directamente a los elementos de servicio se indican como obligatorios si sus elementos de servicio correspondientes aparecen en la Recomendación X.401 (1984) como básico o esencial facultativo, y como facultativos si los elementos de servicio correspondientes aparecen en la Recomendación X.401 (1984) como adicionales facultativos. Otros elementos de protocolo se indican como obligatorios o facultativos de acuerdo a su asignación en las definiciones UDPA4 en la Recomendación X.420 (1984).

Las limitaciones pragmáticas de la guía del realizador X.400 aparecen en las columnas CONST STD de las proformas, en los cuadros B-2/X.403 a B-4/X.403.

Los proveedores de una realización deben utilizar:

- las columnas STATUS IMP de cada proforma para especificar la información relativa a la aceptación de los elementos de protocolo. Por conveniencia, se sugiere que los proveedores indiquen con una «X» únicamente los elementos de protocolo que no sean aceptados;
- las columnas CONST IMP de cada proforma para especificar las limitaciones reales de la realización.

CUADRO B-2/X.403

Proforma ORDescriptor

ORDescriptor	ORIGINADOR			RECEPCIÓN			CONST STD octetos
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	STD	
ORName and/or FreeFormName	O			O			
ORName	F			F			
StandardAttributeList	O			O			
CountryName	F			F			
PrintableString	O			O			2
NumericString	O			O			3
ADMDName	F			F			
PrintableString	O			O			16
NumericString	O			O			16
X121Address	F			F			15
TerminalID	F			F			24
PrivateDomainName	F			F			
PrintableString	O			O			16
NumericString	O			O			16
OrganizationName	F			F			64
UniqueUAIdentifier	F			F			32
PersonalName	F			F			64
surname	O			O			40
givenName	F			F			16
Initials	F			F			5
generationQualifier	F			F			3
OrganizationUnit	F			F			32
DomainDefinedAttrList	F			F			4
type	O			O			8
value	O			O			128
FreeFormName	F			F			128
TelephoneNumber	F			F			32

CUADRO B-3/X.403

Proforma IM-UDPAU

NOMBRE UDPAU: IM-UDPAU	ORIGINADOR			RECEPCIÓN			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
ENCABEZAMIENTO	O			O			
IPMessageID ORName PrintableString	O F O			O F O			 64
Originator (ORDescr.)	O			O			
AuthorizingUser (ORDescr.)	F			O			
PrimaryRecipient (ORDescr) ReportRequest ReplyRequest	O F F			O F F			
CopyRecipient (ORDescr.) ReportRequest ReplyRequest	O F F			O F F			
BlindCopyRecipient (ORDes) ReportRequest ReplyRequest	F F F			O F F			
InReplyTo (IPMessageID) ORName PrintableString	O F O			O F O			 64
Obsoletes (IPMessageId) ORName PrintableString	F F O			O F O			 64
CrossReference (IPM-Id) ORName PrintableString	F F O			O F O			 64
Subject	O			O			256
ExpiryDate	F			O			
ReplyBy	F			O			
ReplyToUser (ORDescr.)	F			O			
Importance	F			O			
Sensitivity	F			O			
Autoforwarded	F			O			
Cuerpo	O			O			
IA5Text repertoire IA5String	F F O			F F O			

CUADRO B-3/X.403 *(cont.)*

NOMBRE UDPAU: IM-UDPAU	ORIGINADOR			RECEPCIÓN			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
G3Fax	F			F			
NumberOfPages	F			F			
G3NonBasicParams	F			F			
BitString	O			O			
TTX	F			F			
NumberOfPages	F			F			
TelexCompatible	F			F			
TeletexNonBasicParams	F			F			
GraficCharacterSet	F			F			
PageFormats	F			F			
MiscTerminalCapability	F			F			
PrivateUse	F			F			
T61String	O			O			
TIF.O	F			F			
T73Document	O			O			
TIF.1	F			F			
T73Document	O			O			
Videotex	F			F			
Videotexstring	O			O			
SFD	F			F			
SFD.Document	O			O			
TLX	F			F			
Voice	F			F			
Bit string	O			O			
Encrypted	F			F			
Bit string	O			O			
NationallyDefined	F			F			
ForwardedIPMessage	F			F			
Delivery	F			F			
DeliverEnvelope	F			F			
ContentType	O			O			
Originator	O			O			
Original	O			O			
Priority	F			F			
DeliveryFlags	O			O			
OtherRecipients	F			F			
ThisRecipient	O			O			
IntendedRecipient	F			F			
Concreted	F			F			
Submission	O			O			
IM-UAPDU	O			O			

CUADRO B-4/X.403

Proforma SR-UDPAU

NOMBRE UDPAU: SR-UDPAU	ORIGINADOR			RECEPCIÓN			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
NonReceiptInformation	O			O			
Reason	O			O			
NonReceiptQualifier	F			F			
Comments	F			F			256
Returned	F			F			
ReceiptInformation	O			O			
ReceptionTime	O			O			
TypeOfReceipt	F			F			
SupplementaryInformation	F			F			64
Reported (IPMessageId)	O			O			
ORName	F			F			
PrintableString	O			O			64
ActualRecipient (ORDescr.)	F			F			
IntendedRecipient (ORDescr)	F			F			
Converted	F			F			

ANEXO C

(a la Recomendación X.403)

Proformas ECRP de STRM(P1)

C.1 *Generalidades*

Como prerrequisito a las pruebas de conformidad, el proveedor de una realización STRM(P1) debe proporcionar un enunciado de conformidad de realización del protocolo (ECRP).

La proforma ECRP STRM(P1) contenida en este anexo especifica la información que debe suministrarse.

Esta información es necesaria para la selección del caso de prueba. Los proveedores deben tener en cuenta que se realizarán pruebas para verificar que los servicios que aparecen como no aceptados, de hecho no estén presentes en vez de estar realizados incorrectamente.

El ECRP STRM(P1) se divide en dos partes:

- una parte que solicita información relativa a la aceptación de los elementos de servicio;
- una parte que solicita información relativa a la aceptación de los elementos de protocolo.

La información sobre la aceptación de los elementos de servicio se solicita en forma de cuadro en el que, para cada elemento de servicio:

- se indica, en las columnas «STD» la condición del elemento de servicio como obligatorio (O), facultativo (F) o no aplicable (–);
- el proveedor indica, en las columnas «IMP» la aceptación real del elemento de servicio por parte de la realización en el origen y el destino.

La información sobre la aceptación de los elementos de protocolo se solicita en forma de cuadro en el que, para cada elemento de protocolo:

- se indica, en las columnas «STD», la condición del elemento de protocolo en el origen y el destino como: obligatorio (O) o facultativo (F);
- se indica cualquier limitación a la realización en la columna «CONST STD», interpretándose las limitaciones como un mínimo para la recepción y un máximo para el origen;
- el proveedor indica, en la columna «STATUS IMP» la aceptación real del elemento de servicio por parte de la realización en el origen y en la recepción;
- el proveedor indica en las columnas «CONST IMP» las limitaciones reales de la realización en el origen y en el destino.

  Las limitaciones pueden expresarse como una longitud o tamaño (octetos, bits, ...), un valor (32k – 1) o el número de veces que ocurre el suceso (4), según el elemento que se limita.

C.2 *Capacidad del originador/destinatario/relevo*

Los proveedores de una implementación deben especificar las capacidades de originador/destinatario/relevo bajo la columna REALIZADO del cuadro C-1/X.403.

CUADRO C-1/X.403

CAPACIDAD	REALIZADO
Originador	
Destinatario	
Relevo	

C.3 *Proforma de elementos de servicio ECRP STRM(P1)*

Los requisitos de la Recomendación X.400 se indican en las columnas STD de la proforma, utilizando las siguientes claves:

O Elemento obligatorio (Recomendación X.401, básico o esencial facultativo)

F Elemento facultativo (Recomendación X.401, adicional facultativo)

– Elemento de servicio no aplicable

Los proveedores de la realización deberán utilizar las columnas IMP de la proforma para especificar la información sobre la aceptación de los elementos de servicio. Se sugiere, para mayor conveniencia, que los proveedores indiquen por medio de una «X» únicamente aquellos elementos de servicio que no sean aceptados.

CUADRO C-2/X.403

Proforma de elementos de servicio STRM (P1)

ELEMENTO DE SERVICIO	ORIGINADOR		RECEPCIÓN		RELEVO	
	STD	IMP	STD	IMP	STD	IMP
Indicación de tipo de contenido	O		O		–	
Indicación de conversión	O		O		O	
Indicación de hora de entrega	O		O		–	
Identificación de mensaje	O		O		–	
Notificación de no entrega	O		O		O	
Indicación de tipos de información codificada original	O		O		–	
Tipos de información codificada certificada	O		O		–	
Indicación de hora de depósito	O		O		–	
Destinatario alternativo permitido	O		F		–	
Entrega diferida	O		–		–	
Cancelación de entrega diferida	O		–		–	
Notificación de entrega	O		O		–	
Publicación de otros destinatarios	O		O		O	
Grado de selección de entrega	O		O		–	
Entrega a múltiples destinos	O		O		O	
Prevención de notificación de no entrega	F		F		F	
Devolución de contenidos	F		F		F	
Prohibición de conversión	O		O		–	
Conversión explícita	F		F		F	
Conversión implícita	F		F		F	
Sonda	O		O		O	
Retener para entrega	–		F		–	
Asignación de destinatario alternativo	–		F		–	

C.4 *Proformas de los elementos de protocolo STRM(P1)*

Los requisitos de la Recomendación X.400 aparecen bajo la columna STATUS STD de las proformas en los cuadros C-3/X.403 a C-6/X.403 utilizando las siguientes claves:

O Elemento obligatorio (Recomendación X.401, básico o esencial facultativo)

F Elemento facultativo (Recomendación X.401, adicional facultativo)

En los cuadros que siguen, los elementos de protocolo que corresponden directamente a los elementos de servicio se indican como obligatorios si sus elementos de servicio aparecen en la Recomendación X.401 (1984) como básico o esencial facultativo, y como facultativos si los elementos de servicio correspondientes aparecen en la Recomendación X.401 (1984) como adicional facultativo. Otros elementos del protocolo se indican como obligatorios o facultativos dependiendo de la asignación que se haya dado en las definiciones UDPM de la Recomendación X.411 (1984).

Para las funciones de relevo, los elementos de protocolo se indican como obligatorios o facultativos basándose únicamente en su condición dentro de la especificación del protocolo P1.

Las restricciones pragmáticas de la guía del realizador X.400 se indican en las columnas CONS STD de las proformas en los cuadros C-3/X.403 a C-6/X.403.

Los proveedores de la realización deberán utilizar:

- la columna STATUS IMP de cada proforma para especificar la información relativa a la aceptación de los elementos de protocolo. Se sugiere, por comodidad que los proveedores indiquen por medio de una «X» únicamente aquellos elementos de protocolo que no sean aceptados;
- las columnas CONS IMP de cada proforma para especificar las limitaciones reales de la realización.

CUADRO C-3/X.403

Proforma ORName y EncodedInformationType

	ORIGINADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
ORName	O			O			O			
StandardAttributeList	O			O			O			
CountryName	F			F			F			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
X121Address	F			F			F			15 Ch
TerminalID	F			F			F			24 Ch
PrivateDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
OrganizationName	F			F			F			64 Ch
UniqueUAIdentifier	F			F			F			32 Ch
PersonalName	F			F			F			64 Ch
surname	O			O			O			40 Ch
givenName	F			F			F			16 Ch
initials	F			F			F			5 Ch
generationQualifier	F			F			F			3 Ch
OrganizationUnit	F			F			F			32 Ch
DomainDefinedAttributeList	F			F			F			8 Ch
type	O			O			O			
value	O			O			O			128 Ch
EncodedInformationType										
BITSTRING	O			O			O			32 bits
G3NonBasisParams	F			F			F			
TeletexNonBasisParams	F			F			F			
PresentationCapabilities	F			F			F			

CUADRO C-4/X.403

Proforma UserUDPM

NOMBRE UDPM: Usuario UDPM	ORIGINADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
UMPDU ENVELOPE	O			O			O			
MPDUIdentifier	O			O			O			
GlobalDomainIdentifier	O			O			O			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
PrivateDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
IA5String	O			O			O			32 Ch
Originator	O			O			O			
OriginalEncodedInformationType	O			O			O			
ContentType	O			O			O			16 Ch
UaContentID	F			F			F			
Priority	O			O			O			
PerMessageFlag	O			O			O			16 b
DisclosureRecipients	O			O			O			
ConversionProhibited	O			O			O			
AlternateRecipientAllowed	O			F			F			
ContentReturnRequest	F			F			F			
DeferredDelivery	O			F			F			
PerDomainBilateralInfo	F			F			F			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
BilateralInfo	O			O			O			a)

CUADRO C-4/X.403 *(cont.)*

NOMBRE UDPM: Usuario UDPM	ORIGINADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
RecipientInfo	O			O			O			
Recipient	O			O			O			
ExtensionIdentifier	O			O			O			b)
PerRecipientFlag	O			O			O			
ResponsabilityFlag	O			O			O			
ReportRequest	O			O			O			
UserReportRequest	O			O			O			
ExplicitConversion	F			F			F			
TraceInformation	O			O			O			
GlobalDomainIdentifier	O			O			O			
DomainSuppliedInfo	O			O			O			
Arrival	O			O			O			
Deferred	O			O			O			
Action relayed or rerouted	O			F			F			
Converted	F			F			F			
Previous	F			F			F			
UMPDU-CONTENT	O			O			O			

a) 1024 octetos.

b) Valor máximo 32k – 1.

CUADRO C-5/X.403

Proforma DeliveryReportUDPM

NOMBRE UDPM: DeliveryReportMPDU	ORIGINADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
DELIVERYREPORTENVELOPE	O			O			O			
Report	O			O			O			
GlobalDomainIdentifier	O			O			O			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
PrivateDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
IA5String	O			O			O			32 Ch
Originator	O			O			O			
TraceInformation	O			O			O			
GlobalDomainIdentifier	O			O			O			
DomainSuppliedInfo	O			O			O			
Arrival	O			O			O			
Deferred	O			O			O			
Action relayed or rerouted	O			F			F			
Converted	F			F			F			
Previous	F			F			F			
DELIVERYREPORTCONTENT	O			O			O			
Original MPDU-Identifier	O			O			O			
GlobalDomainIdentifier	O			O			O			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
PrivateDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
IA5String	O			O			O			32 Ch
Intermediate	F			F			F			
TraceInformation	O			O			O			
GlobalDomainIdentifier	O			O			O			
DomainSuppliedInfo	O			O			O			
Arrival	O			O			O			
Deferred	O			O			O			
Action relayed or rerouted	O			F			F			
Converted	F			F			F			
Previous	F			F			F			

CUADRO C-5/X.403 *(cont.)*

NOMBRE UDMP: DeliveryReportMPDU	ORIGNADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
UAContentId	F			F			F			
ReportRecipientInfo	O			O			O			
Recipient	O			O			O			
ExtensionIdentifier	O			O			O			32k – 1
PerRecipientFlag	O			O			O			
ResponsabilityFlag	O			O			O			
ReportRequest	O			O			O			
UserReportRequest	O			O			O			
LastTraceInformation	O			O			O			
arrival	O			O			O			
converted	F			F			F			
Report	O			O			O			
DeliveredInfo	O			O			O			
Delivery	O			O			O			
TypeOfUA	F			F			F			
NonDeliveredInfo	O			O			O			
ReasonCode	O			O			O			
DiagnosticCode	F			F			F			
IntendedRecipient	F			F			F			
SupplementaryInform.	F			F			F			64 Ch
Returned	F			F			F			
BillingInformation	F			F			F			a)

a) 1024 octetos.

CUADRO C-6/X.403

Proforma ProbeUDPM

NOMBRE UDPM: ProbeMPDU	ORIGINADOR			RECEPCIÓN			RELEVO			CONST
	STATUS		CONST	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD	IMP	IMP	STD
PROBE ENVELOPE	O			O			O			
Probe	O			O			O			
GlobalDomainIdentifier	O			O			O			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
PrivateDomainName	F			F			F			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
IA5String	O			O			O			32 Ch
Originator	O			O			O			
ContentType	O			O			O			
UAContentId	F			F			F			
OriginalEncodedInformationType	O			O			O			
TraceInformation	O			O			O			
GlobalDomainIdentifier	O			O			O			
DomainSuppliedInfo	O			O			O			
Arrival	O			O			O			
Deferred	O			O			O			
Action relayed or rerouted	O			F			F			
Converted	F			F			F			
Previous	F			F			F			
PerMessageFlag	O			O			O			
DisclosureRecipients	O			O			O			
ConversionProhibited	O			O			O			
AlternateRecipientAllowed	O			F			F			
ContentReturnRequest	F			F			F			
ContentLength	F			F			F			
PerDomainBilateralInfo	F			F			F			
CountryName	O			O			O			
NumericString	O			O			O			3 Ch
PrintableString	O			O			O			3 Ch
AdministrationDomainName	O			O			O			
NumericString	O			O			O			16 Ch
PrintableString	O			O			O			16 Ch
BilateralInfo	O			O			O			a)
RecipientInfo	O			O			O			
Recipient	O			O			O			
ExtensionIdentifier	O			O			O			b)
PerRecipientFlag	O			O			O			
ResponsibilityFlag	O			O			O			
ReportRequest	O			O			O			
UserReportRequest	O			O			O			
Explicitconversion	F			F			F			

a) 1024 octetos.

b) Valor máximo 32k – 1.

ANEXO D

(a la Recomendación X.403)

Proformas ECRP de STF

D.1 *Generalidades*

Como prerrequisito a las pruebas de conformidad de una realización STF, el proveedor debe proporcionar un enunciado de conformidad de realización de protocolo (ECRP).

La proforma ECRP STF en este anexo especifica la información que debe suministrarse.

Esta información es necesaria para la selección del caso de prueba. Los proveedores deberán tener en cuenta que las pruebas se realizan únicamente para verificar que los servicios que aparecen como no aceptados, de hecho no están presentes y no que están realizados de forma incorrecta.

El ECRP STF se presenta en tres partes:

- Dos partes que recaban información relativa a la aceptación de las primitivas de servicio STF.

  Si las primitivas tienen únicamente parámetros obligatorios deben señalarse como «no aceptadas» si cualquiera de sus parámetros no es aceptado.
- Una parte que solicita información relativa a la aceptación de elementos de protocolo.

La información sobre la aceptación de elementos de servicio se solicita en forma tabular en donde, para cada elemento:

- se indica en las columnas «STD» la condición del elemento de servicio como obligatoria (O, facultativa (F), condicional (C) o no aplicable (–);
- el proveedor indica, en las columnas «IMP», la aceptación real del elemento de servicio por parte de la realización como iniciador o receptor.

La información sobre la aceptación del elemento de protocolo se solicita en forma tabular en la que para cada elemento de protocolo:

- se indica en las columnas «STD» la condición del elemento de protocolo en el que la RSP es iniciador o receptor como obligatorio (O) o facultativo (F);
- se indica en las columnas «CONS STD» cualquier limitación de la realización, las limitaciones se interpretan como un mínimo para la recepción y un máximo para el origen;
- el proveedor indica, en la columna STATUS IMP», la aceptación real del elemento de protocolo por parte de la realización como iniciador o receptor;
- el proveedor indica, en las columnas «CONST IMP», las limitaciones reales de la realización como iniciador o receptor.

  Las limitaciones pueden expresarse como una longitud o tamaño (octetos, bit, ...) o un valor (32) dependiendo del elemento que se está limitando.

D.2 *Proforma de las primitivas de servicio ECRP STF*

Los requisitos de las Recomendaciones X.400 se indican en las columnas STD de la proforma utilizando las siguientes claves:

O Elemento obligatorio

F Elemento facultativo

Los proveedores de la comodidad deberán utilizar las columnas IMP de la proforma para especificar la información relativa a la aceptación de los elementos de servicio. Se sugiere, por comodidad, que los proveedores indiquen con una «X» únicamente las primitivas de servicio que no sean aceptadas.

D.3 *Proforma de parámetros de servicio ECRP STF*

Los parámetros de servicio STF se ponen en correspondencia con sesión y presentación como sigue:

- Los parámetros de Petición ABIERTO e Indicación ABIERTO se ponen en correspondencia con Petición S-CONEXIÓN e Indicación S-CONEXIÓN y con la P-Conexión correspondiente.
- Se hace corresponder Respondedor/Iniciador-dirección y turno inicial con S-CONEXIÓN.

- El modo de diálogo, protocolo de aplicación y datos de usuario se hacen corresponder con P-Conexión.
- Los parámetros de Respuesta ABIERTO y Confirmación ABIERTO se hacen corresponder con P-Aceptación y R-Rechazo.

CUADRO D-1/X.403

Servicio STF	INICIADOR		RESPONDEDOR	
	STATUS		STATUS	
	STD	IMP	STD	IMP
ABIERTO	O		O	
CERRADO	O		O	
CESIÓN TURNO	F		F	
SOLICITUD TURNO	F		F	
TRANSFERENCIA	O		O	
EXCEPCIÓN	O		O	

Puesto que todos los parámetros de servicio ABIERTO se hacen corresponder con el elemento de protocolo P-Conexión (aparte de la dirección de respuesta y turno inicial que son obligatorios), en los cuadros D-2/X.403 a D-5/X.403 se solicita aparentemente información duplicada respecto a la solicitada en el cuadro D-6/X.403.

Sin embargo, los cuadros D-2/X.403 a D-5/X.403 son útiles ya que aseguran que todos los parámetros obligatorios son realmente aceptados y porque facilitan la revisión de la conformidad estática.

Los requisitos de las Recomendaciones X.400 se muestran en las columnas STD de la proforma utilizando las siguientes claves:

O Parámetros obligatorios

F Parámetros facultativos

C Parámetros condicionales

– Parámetros de servicio no aplicables.

Los proveedores de la realización deberán utilizar las columnas IMP de la proforma para especificar la información relativa a la aceptación de elementos de servicio. Se sugiere por comodidad, que los proveedores indiquen con una «X» únicamente los elementos de servicio que no estén aceptados.

D.4 *Elementos de protocolo STF*

Los requisitos de las Recomendaciones X.400 se indican en la columna STATUS STD de la proforma de los cuadros D-6/X.403 a D-9/X.403 utilizando las siguientes claves:

O Elemento obligatorio

F Elemento facultativo

Las restricciones pragmáticas de guía del realizador X.400 aparecen en las columnas CONST STD de la proforma en los cuadros D-6/X.403 a D-9/X.403.

Los proveedores de una realización deberán utilizar:

- la columna STATUS IMP de la proforma para especificar información relativa a la aceptación de elementos de protocolo. Se sugiere que por comodidad los proveedores indiquen con una «X» únicamente los elementos de protocolo que no estén aceptados;
- las columnas CONST IMP de la proforma para especificar las limitaciones reales de la realización.

CUADRO D-2/X.403

Petición ABIERTO	INICIADOR	
	STATUS	
	STD	IMP
Petición ABIERTO		
Dirección-respondedor	O	
Modo-diálogo	O	
monólogo	O	
twa	F	
Turno inicial	O	
iniciador	O	
respondedor	–	
Protocolo aplicación	O	
P1	O	
Datos de usuario	C	

CUADRO D-3/X.403

Indicación ABIERTO	RESPONDEDOR	
	STATUS	
	STD	IMP
Indicación ABIERTO	O	
Dirección iniciador	O	
Modo-diálogo	O	
monólogo	O	
twa	O	
Turno inicial	O	
iniciador	O	
respondedor	–	
Protocolo aplicación	O	
P1	O	
Datos de usuario	C	

CUADRO D-4/X.403

Respuesta ABIERTO	INICIADOR	
	STATUS	
	STD	IMP
Respuesta ABIERTO		
Disposición	O	
aceptado	C	
rechazado	C	
Datos de usuario	C	
Motivo del rechazo	C	
modo de diálogo inaceptable	C	
fallo de autenticación	C	
ocupado	C	

CUADRO D-5/X.403

Confirmación ABIERTO	RESPONDEDOR	
	STATUS	
	STD	IMP
Confirmación ABIERTO		
Disposición	O	
aceptado	C	
rechazado	C	
Datos de usuario	C	
Motivo del rechazo	C	
modo de diálogo inaceptable	C	
fallo de autenticación	C	
ocupado	C	

Para algunos parámetros resulta aplicable un solo valor (por ejemplo DataTransferSyntax: O). Existen otros parámetros (por ejemplo checkpointSize, RefuseReason) que pueden variar bajo diversas circunstancias y condiciones de tiempo de operación. Dicha información se encuentra en un ISRP y si el parámetro no ha sido fijado, se puede hacer referencia a dicho ISRP dentro del campo de limitaciones.

En una recuperación, se utiliza SessionConnectionId en P-Conexión y P-Aceptación. Este SessionConnectionId puede o no estar codificado de acuerdo con las especificaciones de la Recomendación X.409. Esta información no es importante para los ECRP puesto que no es un criterio para la revisión de conformidad estática o para la selección de caso de prueba y normalmente debe ser proporcionado en un ISRP.

CUADRO D-6/X.403

P-Conexión	INICIADOR			RESPONDEDOR			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
PConnect	O			O			
DataTransferSyntax	O			O			
PUserData	O			O			
checkpointSize	F			O			
windowSize	F			O			
dialogueMode	F			O			
monologue	O			O			
twa	F			O			
ConnectionData	O			O			512
open	O			O			
null	O			O			
MTAName	O			O			32 oct
Password	O			O			64 oct
recover	F			O			
SessionConnectionIden.	O			O			
CallingSSUserReferen.	O			O			64 oct
CommonReference	O			O			
AdditionalRef.Info	F			F			4 oct
applicationProtocol	F			O			

CUADRO D-7/X.403

P-Aceptación	INICIADOR			RESPONDEDOR			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
PAccept	O			O			
DataTransferSyntax	O			O			
PuserData	O			O			
checkpointSize	F			F			
windowSize	F			F			
ConnectionData	O			O			512
open	O			O			
null	O			O			
MTAName	O			O			32 oct
Password	O			O			64 oct
recover	F			F			
SessionConnectionIden.	O			O			
CallingSSUserReferen.	O			O			64 oct
CommonReference	O			O			
AdditionalRef.Info.	F			F			4 oct

CUADRO D-8/X.403

P-Rechazo	INICIADOR			RESPONDEDOR			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
PRefuse	O			O			
RefuseReason	O			O			
rtsBusy	C			O			
cannotRecover	C			O			
validationFailure	C			O			
unacceptableDialogueMode	C			O			

CUADRO D-9/X.403

AbortInformation	INICIADOR			RESPONDEDOR			CONST
	STATUS		CONST	STATUS		CONST	
	STD	IMP	IMP	STD	IMP	IMP	STD
AbortInformation	O			O			
AbortReason	F			F			
localSystemProblem	C			O			
invalidParameter	C			O			
unrecognizedActivity	C			O			
temporaryProblem	C			O			
protocolError	C			O			
transferCompleted	C			O			
reflectedParameter	F			F			

SISTEMAS DE TRATAMIENTO DE MENSAJES: CONVENIOS PARA LA DEFINICIÓN DEL SERVICIO ABSTRACTO [1]

(Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión, controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) que el tratamiento de mensajes es una compleja tarea de procesamiento de información distribuido;

(c) que se necesita un medio para la definición abstracta de dichas tareas;

(d) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(e) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT,

recomienda por unanimidad

(1) que los convenios para la definición de servicios abstractos sean los establecidos en la sección 2;

(2) que las técnicas para la realización de los servicios abstractos así definidos sean las estipuladas en la sección 3.

ÍNDICE

SECCIÓN 1 – *Introducción*

0 Introducción

1 Objeto

2 Referencias

3 Definiciones

4 Abreviaturas

5 Convenios
- 5.1 NSA.1
- 5.2 Términos

SECCIÓN 2 – *Convenios para la definición del servicio abstracto*

6 Visión de conjunto

7 Modelos abstractos
- 7.1 Objetos abstractos
- 7.2 Puertos abstractos
- 7.3 Servicios abstractos
- 7.4 Perfeccionamientos abstractos

[1] La Recomendación X.407 y la norma ISO 10021-3 [Information Processing Systems – Text Communication – MOTIS – Abstract Service Definition Conventions] se elaboraron en estrecha colaboración y están técnicamente armonizadas.

8 Servicios abstractos

8.1 Procedimientos abstractos
8.2 Operaciones abstractas de vinculación
8.3 Operaciones abstractas de desvinculación
8.4 Operaciones abstractas
8.5 Errores abstractos

SECCIÓN 3 – *Realizaciones del servicio abstracto*

9 Visión de conjunto

10 Realizaciones ISA

10.1 Realizaciones SOD
10.2 Realizaciones no SOD

11 Realizaciones de propiedad

11.1 Realizaciones distribuidas
11.2 Realizaciones no distribuidas

Anexo A – Ejemplo del uso de la notación de servicio abstracto

Anexo B – Definición de las referencias de identificadores de objeto

Anexo C – Definición de referencia de la notación

Anexo D – Diferencias entre la Recomendación CCITT y la norma de la ISO

Anexo E – Índice.

SECCIÓN 1 – INTRODUCCIÓN

0 Introducción

Esta Recomendación forma parte de un conjunto de Recomendaciones sobre el tratamiento de mensajes. Este conjunto constituye un esquema completo del sistema de tratamiento de mensajes (STM) realizado por cualquier número de sistemas abiertos cooperantes.

El sistema de tratamiento de mensajes que ofrecen estas Recomendaciones es un sistema complejo de procesamiento de información distribuido, muchos de cuyos componentes tienen estas mismas características.

Esta Recomendación especifica los convenios para definir las tareas de procesamiento de información distribuido del tratamiento de mensajes y también puede ser útil para otras aplicaciones.

El texto de esta Recomendación es objeto de un acuerdo entre el CCITT y la ISO. La especificación ISO correspondiente es ISO 10021-3.

1 Objeto

Esta Recomendación establece los convenios utilizados para especificar las tareas de procesamiento de información distribuido necesarias para el tratamiento de mensajes.

Esta Recomendación está estructurada de la siguiente manera. La presente sección 1 es la introducción. La sección 2 especifica los convenios para la definición abstracta de una tarea de procesamiento de información distribuido. La sección 3 establece los principios para realizar en forma concreta los aspectos de comunicación de dichas tareas, por ejemplo, los protocolos de interconexión de sistemas abiertos (ISA). Los anexos ofrecen información complementaria importante.

No hay requisitos en cuanto a la conformidad con esta Recomendación.

ARCHIVES U.I.T. GENÈVE

2 Referencias

Esta Recomendación menciona los siguientes documentos:

Recomendación X.200 Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 7498).

Recomendación X.208 Especificación de la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8824).

Recomendación X.209 Especificación de las reglas básicas de codificación para la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8825).

Recomendación X.217 Definición de servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 8649).

Recomendación X.219 Operaciones a distancia: modelo, notación y definición del servicio (véase también la Norma ISO 9072-1).

3 Definiciones

Para los fines de esta Recomendación, se aplicarán las definiciones del anexo E y las mencionadas a continuación.

Esta Recomendación se basa en los conceptos expuestos en la Recomendación X.200 y utiliza los siguientes términos definidos en la misma:

a) sintaxis abstracta;
b) capa de aplicación;
c) unidad de datos de protocolo de aplicación (UDPA);
d) protocolo de aplicación;
e) elemento de servicio de aplicación (ESA);
f) sintaxis de transferencia concreta;
g) tarea de procesamiento de información distribuido;
h) servicio de capa;
i) capa;
j) sistema abierto;
k) interconexión de sistemas abiertos (ISA);
l) sistema abierto real.

Esta Recomendación utiliza los siguientes términos, definidos en la Recomendación X.208.

a) notación de sintaxis abstracta uno (NSA.1);
b) tipo (de datos);
c) valor (de datos);
d) importación;
e) entero;
f) macro;
g) módulo;
h) identificador de objeto;
i) rótulo.

Esta Recomendación utiliza los siguientes términos definidos en la Recomendación X.209:

a) reglas básicas de codificación.

Esta Recomendación utiliza los siguientes términos definidos en la Recomendación X.217:

a) contexto de aplicación (CA).

Esta Recomendación utiliza los siguientes términos definidos en la Recomendación X.219:

a) operación de vinculación;
b) error;
c) enlazado;
d) operación;
e) servicio de operación a distancia (SOD);
f) operaciones a distancia;
g) operación de desvinculación.

4 Abreviaturas

Para los fines de esta Recomendación, se aplican las abreviaturas del anexo E.

5 Convenios

Esta Recomendación utiliza los siguientes convenios descriptivos:

5.1 *NSA.1*

Esta Recomendación utiliza las convenciones descriptivas basadas en la NSA.1 para los fines indicados:

a) Para definir las macros OBJECT, PORT y REFINE, la notación macro NSA.1 de la Recomendación X.208.

b) Para definir las macros ABSTRACT-BIND, -UNBIND, -OPERATION y -ERROR, las macros BIND, UNBIND, OPERATION y ERROR de la Recomendación X.219.

c) Para especificar la sintaxis abstracta de los objetos de información en el ejemplo del anexo A, la propia NSA.1.

d) Para especificar diversos *modelos abstractos* del ejemplo del anexo A, los macros OBJECT, PORT y REFINE del § 7.

e) Para especificar diversos *servicos abstractos* del ejemplo del anexo A, los macros ABSTRACT-BIND, -OPERATION y -ERROR del § 8.

La NSA.1 aparece tanto en el cuerpo de esta Recomendación, para facilitar la exposición, como en los anexos como referencia, en una forma bastante redundante. Si se encuentran diferencias entre los dos, se indica un error de especificación.

Obsérvese que los rótulos NSA.1 son implícitos en todos los módulos NSA.1 de los anexos; los módulos son definitivos a este respecto.

5.2 *Términos*

En esta Recomendación, los términos definidos aparecen en **negrita**; en *bastardilla* cuando aparecen antes de su definición, y de la manera normal en todos los demás casos.

Los nombres propios se escriben con mayúscula y los términos genéricos no.

SECCIÓN 2 – CONVENIOS PARA LA DEFINICIÓN DEL SERVICIO ABSTRACTO

6 Visión de conjunto

Cuando se debe describir y especificar una tarea compleja de procesamiento de información distribuido es conveniente comenzar especificando la tarea en términos abstractos, y no en términos concretos. Esto garantiza que los requisitos funcionales de la tarea se establezcan en forma independiente de su realización concreta. Dicha separación es importante, entre otras cosas, porque cada aspecto de la tarea puede prestarse para *varias* realizaciones concretas. En un sistema de transferencia de mensajes que comprende, por ejemplo, tres agentes de transferencia de mensajes, el primero y el segundo pueden interactuar utilizando la comunicación ISA, y el segundo y el tercero por medios patentados.

Esta sección especifica los convenios para la descripción abstracta de una tarea de procesamiento de información distribuido, tanto macroscópica como microscópicamente. La primera descripción se llama *modelo abstracto* y la segunda *servicio abstracto.*

En esta sección se definen instrumentos formales para especificar *servicios* y *modelos abstractos.* En el anexo A se ofrece un ejemplo completo de su utilización. Puede ser conveniente que el lector consulte dicho anexo, por ejemplo, por sus ilustraciones al leer la presente sección.

Esta sección comprende los siguientes temas:

a) *Modelos abstractos*

b) *Servicios abstractos*

Nota – Los instrumentos formales mencionados más arriba no son ni un lenguaje de descripción formal ni un sustituto del mismo. Simplemente, son la notación NSA.1 que sirve de base a los convenios descriptivos informales definidos en esta sección.

7 Modelos abstractos

La descripción macroscópica de una tarea de procesamiento de información distribuido se llama **modelo abstracto (modelo)** de dicha tarea y del entorno en el que se realiza. Se basa en los conceptos de *objetos, puertos, servicio* y *perfeccionamientos abstractos.* (El concepto de servicio abstracto se elabora con más detalle en el § 8.)

7.1 *Objetos abstractos*

Un **objeto abstracto (objeto)** es una entidad funcional tal vez una de varias que interactúan entre sí. Los objetos son de diferentes tipos, que determinan su función y comportamiento. Por ejemplo, un objeto de un tipo puede representar un sistema, y múltiples objetos de otro tipo sus usuarios. Los objetos interactúan por medio de *puertos abstractos.*

Un tipo de objeto se especifica por medio de la macro OBJECT. Dicha especificación enumera los tipos de *puertos abstractos* que dan accesso a dicho objeto. Por cada tipo de puerto *asimétrico,* la especificación indica si los puertos son puertos *consumidores* o *suministradores.*

```
OBJECT MACRO ::=
BEGIN

TYPE NOTATION   ::= "PORTS" "{" PortList "}" | empty
VALUE NOTATION  ::= value (VALUE OBJECT IDENTIFIER)

PortList        ::= Port "," PortList | Port
Port            ::= value (PORT) PortType

PortType        ::= Symmetric | Asymmetric

Symmetric       ::= empty
Asymmetric      ::= Consumer | Supplier

Consumer        ::= "[C]"

Supplier        ::= "[S]"

END
```

Un valor de dato del tipo OBJECT es un identificador de objeto que identifica de forma única e inequívoca el tipo de objeto especificado.

Nota – El uso de la palabra clave "OBJECT" se limita a la NSA.1. Su sustitución por un vocablo adecuado en el presente contexto requiere ulterior estudio.

7.2 *Puertos abstractos*

Un **puerto abstracto (puerto)** es un punto en el que un objeto abstracto interactúa con otro objeto abstracto. Los puertos son de diferentes tipos, lo que determina los tipos de interacciones que permiten. Por ejemplo, los puertos de un tipo pueden representar los medios por los cuales se accede a un sistema de guía, y los puertos de otro tipo, los medios por los que el mismo se administra.

Los tipos de puertos son a su vez de las dos especies siguientes:

a) **simétrico**: todos los casos de un tipo de puerto simétrico son idénticos;

b) **asimétrico**: cada caso de un tipo de puerto asimétrico es de una de dos clases; **suministrador** o **consumidor**.

Nota – Con frecuencia, la asignación de los términos «suministrador» y «consumidor» es intuitiva. Por ejemplo, se puede considerar naturalmente que un sistema de archivo, presenta puertos suministrados a sus usuarios y administradores. Sin embargo, en rigor, la asignación de los dos términos es arbitraria.

Dos objetos pueden interactuar entre sí por medio de un puerto en cada uno de ellos, únicamente mientras dichos puertos estén en contacto o **unidos**. Las acciones por medio de las que se inicia y termina este estado para uno o más pares de puertos, se llaman **vinculación** y **desvinculación**, respectivamente.

Dos puertos pueden estar unidos únicamente si **concuerdan**. Dos puertos cualesquiera de un mismo tipo simétrico, concuerdan. Dos puertos de un mismo tipo asimétrico concuerdan si, y únicamente si, uno es suministrador y el otro consumidor.

Un tipo de puerto se especifica por medio del macro PORT. Tal especificación identifica las *operaciones abstractas* que representan las interacciones posibles mientras dos de dichos puertos están unidos. Si no se indica ninguna, las *operaciones abstractas* se consideran no especificadas.

```
PORT MACRO ::=
BEGIN

TYPE NOTATION    ::= Operations | empty
VALUE NOTATION   ::= value (VALUE OBJECT IDENTIFIER)

Operations       ::= Symmetrical | Asymmetrical

Symmetrical      ::= "ABSTRACT" "OPERATIONS" "{" OperationList "}"
Asymmetrical     ::= OneSided | TwoSided

OneSided         ::= Consumer | Supplier
TwoSided         ::= Consumer Supplier | Supplier Consumer

Consumer         ::= "CONSUMER" "INVOKES" "{" OperationList "}"
Supplier         ::= "SUPPLIER" "INVOKES" "{"OperationList"}"

OperationList    ::= Operation "," OperationList | Operation
Operation        ::= value (ABSTRACT-OPERATION) | --identifica la operación abstracta
                                                  por valor de datos
                     type --identifica la operación abstracta por tipo de datos

END
```

Si el tipo de puerto es simétrico, ambos objetos ofrecen todas las *operaciones abstractas* enumeradas. Si el tipo de puerto es asimétrico, la macro diferencia entre las *operaciones abstractas* que ofrecen un objeto con puerto consumidor y aquellas que ofrecen un objeto con el puerto proveedor.

Un valor de datos del tipo PORT es un identificador de objeto que en forma única e inequívoca identifica el tipo de puerto especificado.

7.3 *Servicios abstractos*

Un **servicio abstracto** es un conjunto de capacidades que un objeto ofrece a otro por medio de uno o más de sus puertos. Al primer objeto se le denomina **proveedor de servicio abstracto (proveedor)** y al segundo, **usuario de servicio abstracto (usuario)**. Cada puerto en cuestión puede ser simétrico o asimétrico y si es lo segundo puede ser consumidor o suministrador.

Un servicio abstracto puede tener cualquier número de usuarios y proveedores.

Cuando los puertos de servicio abstracto de un proveedor estén unidos a los puertos concordantes de un usuario, se dice que entre los dos objetos existe una **asociación abstracta (o asociación)**.

Un servicio abstracto se especifica como se indica en el § 8.

Nota – Un servicio abstracto dentro de la capa de aplicación tiene una finalidad muy similar a los servicios de capa de las capas ISA inferiores.

7.4 *Perfeccionamientos abstractos*

Un objeto puede verse de diferentes maneras en diferentes momentos. Algunas veces es conveniente considerar un objeto como atómico. Esto ocurre, por ejemplo, cuando se describe la forma en que un objeto interactúa con otros objetos externos a él mismo, es decir, cuando se especifica su servicio abstracto. Otras veces es más adecuado considerar un objeto como compuesto, es decir constituido de otros objetos. Este podría ser el caso, por ejemplo, cuando se describe la forma en que se realiza un objeto.

Como cualquier objeto, los objetos componentes tienen puertos. Algunos de estos son visibles en la «superficie» del objeto construido. Otros permiten la interacción de los objetos componentes, admitiendo así la disposición y uso de servicios menos abstractos entre los objetos componentes, que cooperan para proporcionar el servicio abstracto general del objeto construido.

La descomposición funcional de un objeto en varios objetos menores se conoce como **perfeccionamiento abstracto (perfeccionamiento)** de dicho objeto.

La técnica de perfeccionamiento puede aplicarse en forma recurrente. Un objeto componente puede perfeccionarse para revelar *su* estructura interna. Esto puede continuar hasta que se llega a los objetos componentes, considerados como atómicos.

Un perfeccionamiento se especifica con la macro REFINE. Identifica el objeto cuya estructura interna se está revelando y los objetos componentes utilizados en su construcción. Cada objeto componente puede considerarse como único o como recurrente. La macro también indica cuáles puertos de los objetos componentes están unidos a puertos de otros objetos componentes y cuáles son visibles en la superficie del objeto compuesto.

```
REFINE MACRO ::=
BEGIN

TYPE NOTATION    ::= Object "AS" ComponentList
VALUE NOTATION   ::= value (VALUE OBJECT IDENTIFIER)

ComponentList    ::= Component ComponentList | Component
Component        ::= ObjectSpec Ports

ObjectSpec       ::= Object | Object "RECURRING"

Ports            ::= PortSpecList | empty
PortSpecList     ::= PortSpec PortSpecList | PortSpec
PortSpec         ::= value (PORT) PortSide PortStatus

PortSide         ::= Consumer | Supplier | empty
Consumer         ::= "[C]"
Supplier         ::= "[S]"

PortStatus       ::= "VISIBLE" | "PAIRED" "WITH" ObjectList

ObjectList       ::= Object "," ObjectList | Object
Object           ::= value (OBJECT)

END
```

Un valor de datos del tipo REFINEMENT es un identificador de objeto.

Nota – Al igual que con los objetos, en principio los puertos, pueden considerarse de diferentes maneras en diferentes momentos. En algunos casos es conveniente considerar un (par) puerto como atómico. Sin embargo, se puede imaginar el perfeccionamiento de un puerto para examinar cómo puede proporcionar comunicación de este tipo. En este contexto, un puerto par, se considera como aceptado por una colección de objetos. Esto mejoraría la especificación de las capacidades de comunicación. Este concepto de «perfeccionamiento de puerto» no se estudia más a fondo en esta versión de la presente Recomendación.

8 Servicios abstractos

Una descripción microscópica de una tarea de procesamiento de información distribuido es una especificación del servicio abstracto que define la forma en que se inicia, controla y termina una tarea. Se basa en los conceptos de *operaciones abstractas vinculadas, operaciones desvinculadas, operaciones y errores,* así como en el concepto promotor de *procedimientos abstractos.*

Nota – Las macros definidas más abajo implican el uso de NSA.1 para especificar argumentos, resultados y parámetros. Por ejemplo, cualquier rótulo específico del contexto, asignado en el curso de las especificaciones, si bien no tiene sentido en dicho contexto, desempeña un papel importante en una realización SOD del servicio abstracto.

8.1 *Procedimientos abstractos*

Un **procedimiento abstracto (procedimiento)** es una tarea que realiza un objeto a solicitud de otro. El hacer la solicitud y llevar a cabo la tarea se conoce como **invocación y ejecución** del procedimiento. Los objetos que producen y actúan por dicha solicitud se conocen respectivamente como **invocador y ejecutor**.

Un procedimiento puede (pero no necesariamente) requerir que un invocador, al hacer la invocación, suministre al ejecutor un objeto único de información de un tipo específico, que se conoce como **argumento** del procedimiento.

Cada ejecución del procedimiento tiene un resultado, éxito o fracaso. Se considera que un procedimiento tiene éxito si se ejecuta en su totalidad y que es un fracaso si se termina prematuramente.

Un procedimiento puede requerir (pero no necesariamente) que el ejecutor informe del éxito al invocador. Puede pedir (pero no necesariamente) además que suministre, cuando informa del éxito, un objeto único de información de un tipo prescrito, que se conoce como el resultado del procedimiento.

Un procedimiento puede (pero no necesariamente) requerir que el ejecutor informe al invocador del fracaso. Puede (pero no necesariamente) requerir además que le suministre cierta información cuando notifica el fracaso.

Nota – En los puntos subsiguientes se utiliza la NSA.1 para especificar la sintaxis abstracta de los argumentos y resultados de los procedimientos (así como de los parámetros de *errores abstractos*). Estos usos de NSA.1 no implican que estos objetos de información sean transportados *necesariamente* entre sistemas abiertos. En especial, el que los objetos de información, por su descripción en NSA.1 y sus reglas de codificación básica, tengan sintaxis de transferencia concretas, no tiene importancia en el presente contexto. NSA.1 es simplemente un instrumento cómodo para la descripción formal de la sintaxis abstracta de los objetos de información.

8.2 *Operaciones abstractas de vinculación*

Una **operación abstracta de vinculación** es un procedimiento cuya realización satisfactoria une a uno o más pares de puertos abstractos. El objeto que invoca una operación abstracta de vinculación se conoce como **iniciador** y el que la realiza es el **respondedor**.

Una operación abstracta de vinculación sirve para vincular un grupo especial de puertos del iniciador a un grupo concordante del respondedor. Cuando uno o más de los puertos son asimétricos, la operación abstracta de vinculación puede servir para unir únicamente el lado consumidor, el lado suministrador o cualquiera de ellos.

Una operación abstracta de vinculación es un procedimiento general completo, salvo cuando la información se transmite al invocador luego de un fracaso, se verá limitada a un solo objeto de información denominado **información de error**.

Una operación abstracta de vinculación se especifica por la macro ABSTRACT-BIND cuya definición es la siguiente:

```
ABSTRACT-BIND MACRO ::=
BEGIN

TYPE NOTATION   ::= Ports Bind
VALUE NOTATION  ::= value (VALUE BindType)

Ports           ::= "TO" "{" PortList "}" | empty
PortList        ::= Port "," PortList | Port
Port            ::= value (PORT) PortSide
PortSide        ::= Consumer | Supplier | empty
Consumer        ::= "[C]"
Supplier        ::= "[S]"

Bind            ::= type (BindType) -- ha de ser un tipo BIND
                    | empty <BindType ::= BIND>

END
```

La cláusula «Puertos» introducida por la palabra clave «TO», enumera los puertos de un respondedor que se vincularán en esta operación abstracta de vinculación. Si se lista un puerto asimétrico, sin haber sido calificado por «[S]» o «[C]», eso significa que la operación abstracta de vinculación puede utilizarse en la unión de dicho puerto en cualquier dirección.

Obsérvese que la especificación del argunemto, resultado y/o información de error se logra por medio de la macro BIND de operaciones a distancia (incrustada), definida en la Recomendación X.219 y la macro devolverá un valor de ese tipo. Si no hay se devolverá el «BIND» normal.

Nota – La relación ABSTRACT-BIND y -BIND puede hacer trivial la realización del SOD en un servicio abstracto; véase el § 10.1.

Un servicio abstracto por lo común comprende una operación abstracta de vinculación para cada tipo de puerto involucrado en su provisión. Cuando hay varios tipos de puertos involucrados, sus operaciones abstractas de vinculación pueden, pero no necesariamente, ser diferentes.

8.3 *Operaciones abstractas de desvinculación*

Una **operación abstracta de desvinculación** es un procedimiento cuya realización, satisfactoria o no, desvincula dos puertos. Es invocada por el objeto que invocó la vinculación abstracta correspondiente (es decir el inciador) y ejecutada por el respondedor.

Una operación abstracta de desvinculación sirve para desvincular un grupo especial de puertos del iniciador de un grupo concordante del respondedor. Cuando uno o más de los puertos del grupo son asimétricos, la operación abstracta de desvinculación puede servir para desvincular únicamente del lado consumidor, del lado suministrador o de cualquiera de ellos.

Una operación abstracta de desvinculación es un procedimiento general completo, excepto, si la información se transmite al invocador en caso de fracaso, estará limitada a un solo objeto de información denominado **información de error**.

Una operación abstracta de desvinculación se especifica por medio de la macro ABSTRACT-UNBIND, cuya definición es la siguiente:

```
ABSTRACT-UNBIND MACRO ::=
BEGIN

TYPE NOTATION   ::= Ports Unbind
VALUE NOTATION  ::= value (Value UnbindType)

Ports           ::= "FROM" "{" PortList "}"
PortList        ::= Port "," PortList | Port
Port            ::= value (PORT) PortSide
PortSide        ::= Consumer | Supplier | empty
Consumer        ::= "[C]"
Supplier        ::= "[S]"

Unbind          ::= type (UnbindType) |
                    -- must be an UNBIND type
                    | empty <UnbindType ::= UNBIND>

END
```

La cláusula «puertos» introducida por la palabre clave «FROM», enumera los puertos de un respondedor del que se desvinculará esta operación abstracta de desvinculación. Si se enumera un puerto asimétrico, sin haber especificado «[S]» o «[C]», la operación abstracta de desvinculación separará dicho puerto en cualquier dirección (si bien la dirección real está determinada por la dirección en que se realizó la vinculación.

Obsérvese que la especificación del argumento, resultado y/o información de error va acompañada de una macro UNBIND de operaciones a distancia (incrustada), definida en la Recomendación X.219; la macro devolverá un valor de ese mismo tipo. Si no se proporciona, se devolverá el «UNBIND» por defecto.

Nota – La relación ABSTRACT-UNBIND y UNBIND hace trivial la realización del SOD en un servicio abstracto; véase el § 10.1.

Un servicio abstracto por lo general, incluye una operación abstracta de desvinculación por cada tipo de puerto involucrado en esta disposición. Cuando hay participación de varios puertos, sus operaciones abstractas de desvinculación pueden, pero no obligatoriamente, ser diferentes.

8.4 *Operaciones abstractas*

Una **operación abstracta** es un procedimiento que puede invocarse en el contexto de dos puertos vinculados. Su fracaso no afecta la vinculación. Si los puertos son asimétricos, el puerto prescribirá si el invocador es el objeto que cuenta con el puerto consumidor, el objeto con el puerto suministrador o cualquiera de éstos. Si los puertos son simétricos o asimétricos, el objeto restante es el realizador.

Una operación abstracta es un procedimiento general completo, excepto para la información transmitida al invocador en cado de fracaso. Una operación abstracta falla cuando encuentra un *error abstracto*, entonces la información que transmite se limita a informar sobre dicho error abstracto. Para cada operación abstracta se prescribe si se notifica el fallo y de ser así, que errores abstractos pueden presentarse.

Una operación abstracta se especifica con la macro ABSTRACT-OPERATION. Su definición es idéntica a la de la macro OPERATION de operaciones a distancia, especificada en la Recomendación X.219.

```
MACRO ABSTRACT-OPERATION ::= OPERATION
```

Un servicio abstracto comprende cero o más operaciones abstractas para cada tipo de puerto involucrado en esta disposición. Cuando participan varios tipos de puertos, pueden, pero no necesariamente, tener operaciones abstractas en común.

Nota – La equivalente de ABSTRACT-OPERATION y OPERATION ayuda a hacer trivial la realización SOD de un servicio abstracto; véase el § 10.1.

8.5 *Errores abstractos*

Un **error abstracto** es una condición excepcional que puede surgir durante la ejecución de una operación abstracta, provocando su fracaso.

Cuando se infoma de un error abstracto, el ejecutor transmite al invocador la identidad del error abstracto y posiblemente un objeto de información único denominado su **parámetro**. Para cada error abstracto se prescribe si se devuelve un parámetro y de ser así, su tipo.

Un error abstracto se especifica con la macro ABSTRACT-ERROR. Su definición es idéntica a la de la macro ERROR de operaciones a distancia, especificada en la Recomendación X.219.

MACRO ABSTRACT-ERROR ::= ERROR

Un servicio abstracto comprende cero o más errores abstractos notificados por sus operaciones abstractas.

Nota – La equivalencia de ABSTRACT-ERROR y ERROR ayudan a hacer trivial la realización SOD de un servicio abstracto; véase el § 10.1.

SECCIÓN 3 – REALIZACIONES DEL SERVICIO ABSTRACTO

9 Visión de conjunto

Una vez que la tarea de procesamiento de información distribuido se ha descrito y especificado en términos abstractos, es necesario establecer la forma en que cada aspecto debe realizarse. Como se sugirió anteriormente, cada aspecto puede admitir varias realizaciones concretas.

Esta sección establece principios para la realización concreta de servicios y modelos abstractos. Una *x* **real** es el sistema o proceso de computador, o el sistema abierto real que realiza concretamente, un objeto abstracto de tipo *x*.

Esta sección cubre los siguientes asuntos:

a) Realizaciones ISA

b) Realizaciones de concesión.

Nota – Los aspectos de un modelo asbtracto que se subrayan aquí, son puertos abstractos y sus vinculaciones. Esto se debe a que los puertos abstractos marcan el límite, no sólo entre objetos abstractos, sino también entre sistemas físicos que realizan concretamente dichos objetos abstractos. Así, los puertos abstractos y las vinculaciones son las partes del modelo abstracto que, si se desea que exista interfuncionamiento de los sistemas abiertos, deben construirse o ser construibles con los instrumentos ISA.

10 Realizaciones ISA

Un objetivo primordial de las Recomendaciones del CCITT y de las Normas de la ISO es especificar cómo se realizan las tareas de procesamiento de información distribuida cuando se llevan a cabo por varios sistemas abiertos reales cooperantes.

En el entorno ISA, los objetos se realizan por medio de procesos de aplicación, en general con unas relaciones de correspondencia de muchos objetos a muchos procesos de aplicación. La comunicación entre objetos, realizada por procesos de aplicación en diferentes sistemas abiertos, se logra por medio de los protocolos de aplicación ISA (consistentes en contextos de aplicación). Un contexto de aplicación realiza así la vinculación, uso y desvinculación de varios pares de puertos.

La especificación de un contexto de aplicación se hace en términos de la operación coordinada de varios elementos de servicio-aplicación. La realización resulta especialmente idónea para especificar si un elemento de servicio-aplicación está definido para corresponder a cada puerto cuya comunicación debe aceptarse.

A continuación se examina la realización de vinculaciones y puertos abstractos por medio de ESA y CA. Se tienen en cuenta tanto las realizaciones SOD como las que no son SOD.

10.1 *Realizaciones SOD*

La realización concreta de puertos y vinculaciones con frecuencia es trivial cuando se logra por medio de operaciones a distancia.

Esto es porque resulta inmediato definir un servicio abstracto en el que existe un protocolo de aplicación basado en SOD, que sea funcionalmente idéntico a él. Esto a su vez es cierto, porque el marco de especificación de servicios abstractos es isomorfo con la especificación de protocolos de aplicación basados en el SOD. En el cuadro 1/X.407 se enumeran las correspondencias inherentes al isomorfismo.

CUADRO 1/X.407

Correspondencias entre servicios abstractos y protocolos basados en SOD

Aspecto del servicio abstracto	Aspecto del protocolo basado en SOD
Operación abstracta de vinculación	Operación de vinculación
Operación abstracta de desvinculación	Operación de desvinculación
Operación abstracta	Operación
Error abstracto	Error

Las correspondencias del cuadro se deben a que los aspectos correspondientes se especifican formalmente utilizando macros estrechamente relacionadas o equivalentes, como se resume en el cuadro 2/X.407:

CUADRO 2/X.407

Macros SOD y servicio abstracto equivalente

Macro servicio abstracto	Macro SOD
ABSTRACT-BIND	BIND
ABSTRACT-UNBIND	UNBIND
ABSTRACT-OPERATION	OPERATION
ABSTRACT-ERROR	ERROR

En el anexo A se analizan por medio de un ejemplo las definiciones de CA y ESA basadas en SOD que realizan concretamente puertos abstractos.

Para que la realización sea trivial, es necesario que exista una operación abstracta de vinculación que una todos los puertos que deben acoplarse por pares.

Nota – Cuando en un servicio abstracto involucrado hay más de un puerto (par) es necesario diseñar la operación abstracta de vinculación para los puertos específicamente involucrados. (Actualmente) no existe ninguna disposición para la síntesis automática de una vinculación abstracta adecuada, basada por ejemplo, en las definiciones de operaciones abstractas de vinculación definidas para los puertos individuales.

10.2 *Realizaciones no SOD*

La realización concreta de vinculaciones y puertos es una tarea más sustancial cuando se intenta por otros medios que no son operaciones a distancia y se puede decir muy poco sobre la propuesta general.

A pesar de lo anterior, son importantes las dos observaciones siguientes:

a) La realización concreta de un servicio abstracto es un protocolo de aplicación que se simplifica mucho al utilizar NSA.1 para definir sus UDPA. Esto se debe a que la especificación del protocolo puede importar simplemente los tipos y valores pertinentes de la especificación del servicio abstracto.

b) La realización concreta de un servicio abstracto cuyas operaciones abstractas no informan de sus resultados es conceptualmente sencilla. Esto se debe a que cada una de dichas operaciones abstractas representa una interacción que comprende una sola UDPA. A partir de estas interacciones, las más simples posibles, se puede en forma arbitraria, construir otras complejas.

11 Realizaciones de propiedad

Un objetivo secundario de las Recomendaciones del CCITT y de las Normas de la ISO es garantizar que las partes de una tarea de procesamiento de información distribuido que son realizadas por medios propios, mantengan la funcionalidad general deseada del sistema.

A continuación se examina brevemente la realización de unión y puertos abstractos por medios propios. Se consideran tanto las realizaciones distribuidas, como las no distribuidas.

11.1 *Realizaciones distribuidas*

La realización concreta de puertos y vinculaciones por medio de concesiones de protocolos de comunicación computarizados es un asunto local. La especificación de la funcionalidad visible, incluida en el servicio abstracto proporciona una guía a los ejecutores de las realizaciones de propiedad para que cuando dichas realizaciones sean correcctas, pueden jugar el papel adecuado en la tarea general.

11.2 *Realizaciones no distribuidas*

La realización concreta de puertos y vinculaciones por medio de mecanismos dentro de un solo computador es un asunto local. Al igual que en el caso considerado en el § 11.1, la especificación de servicio abstracto sirve como guía al ejecutor para garantizar que la realización en propiedad pueda, de todas formas, desempeñar el papel adecuado en la tarea general.

ANEXO A

(a la Recomendación X.407)

Ejemplo del uso de la notación de servicio abstracto

Este anexo no forma parte de esta Recomendación.

Este anexo ilustra el uso de la notación de servicio y modelo abstracto por medio de un ejemplo. El ejemplo implica dos sistemas, los *sistemas verde* y *amarillo* y sus entornos, los **entornos verde** y **amarillo**.

El ejemplo utiliza las notaciones de modelo abstracto para describir por separado los entornos (§ A.2 y A.4) y para mostrar cómo se relacionan sus sistemas: uno está construido a partir del otro (§ A.6). Para describir las capacidades de cada sistema (§ A.3 y A.5) se utiliza la notación de servicio abstracto. El ejemplo concluye realizando los puertos de los sistemas como CA y ESA utilizando la notación SOD de la Recomendación X.219 según sea adecuado para la comunicación ISA (§ A.7 y A.8).

A.1 *Asignación de identificadores de objeto*

Los módulos NSA.1 definidos en este anexo requieren la asignación de varios identificadores de objeto. Todos se definen a continuación utilizando NSA.1. Las asignaciones son definitivas, excepto las de los módulos NSA.1 y las referentes a los convenios de definición del servicio de aplicación. Las asignaciones definitivas de los primeros se presentan en los módulos mismos; otras referencias a ellas aparecen en las cláusulas IMPORT. La última es fija.

```
ExampleObjectIdentifiers {joint-iso-ccitt
        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo
-- Exporta todo.

IMPORTS -- nada --;

ID ::= OBJECT IDENTIFIER

-- Ejemplo (no definitivo) de los convenios de definición del servicio abstracto

id-asdc-ex ID ::= {joint-iso-ccitt mhs-motis(6) asdc(2) example(1)}
        -- no definitivo

-- Categorías

id-mod  ID ::= {id-asdc-ex 0} -- módulos; no definitivo
id-ot   ID ::= {id-asdc-ex 1} -- tipos objeto
id-pt   ID ::= {id-asdc-ex 2} -- tipos puerto
id-ref  ID ::= {id-asdc-ex 3} -- perfeccionamientos
id-ac   ID ::= {id-asdc-ex 4} -- contextos de aplicación
id-ase  ID ::= {id-asdc-ex 5} -- elementos del servicio de aplicación
id-as   ID ::= {id-asdc-ex 6} -- sintaxis abstractas

-- Módulos

id-mod-object-identifiers ID ::= {id-mod 0} -- no definitivo
id-mod-ye-refinement      ID ::= {id-mod 1} -- no definitivo
id-mod-y-abstract-service ID ::= {id-mod 2} -- no definitivo
id-mod-ge-refinement      ID ::= {id-mod 3} -- no definitivo
id-mod-g-abstract-service ID ::= {id-mod 4} -- no definitivo
id-mod-ys-refinement      ID ::= {id-mod 5} -- no definitivo
id-mod-ys-realization     ID ::= {id-mod 6} -- no definitivo
id-mod-gs-realization     ID ::= {id-mod 7} -- no definitivo

-- Tipos objeto

id-ot-y-environment     ID ::= {id-ot 0}
id-ot-y-user            ID ::= {id-ot 1}
id-ot-y-system          ID ::= {id-ot 2}
id-ot-g-environment     ID ::= {id-ot 3}
id-ot-g-user            ID ::= {id-ot 4}
id-ot-g-manager         ID ::= {id-ot 5}
id-ot-g-system          ID ::= {id-ot 6}
id-ot-agent             ID ::= {id-ot 7}

-- Tipos puerto

id-pt-y-use             ID ::= {id-pt 0}
id-pt-g-use             ID ::= {id-pt 1}
id-pt-g-management      ID ::= {id-pt 2}

-- Perfeccionamientos

id-ref-y-environment    ID ::= {id-ref 0}
id-ref-g-environment    ID ::= {id-ref 1}
id-ref-y-system         ID ::= {id-ref 2}

-- Contextos de aplicación

id-ac-y-use             ID ::= {id-ac 0}
id-ac-g-use             ID ::= {id-ac 1}
id-ac-g-management      ID ::= {id-ac 2}
```

-- *Elementos del servicio de aplicación*

```
id-ase-y-use            ID ::= { id-ase 0 }
id-ase-g-use            ID ::= { id-ase 1 }
id-ase-g-management     ID ::= { id-ase 2 }
```

-- *Sintaxis abstractas*

```
id-as-y-use             ID ::= { id-as 0 }
id-as-g-use             ID ::= { id-as 1 }
id-as-g-management      ID ::= { id-as 2 }
```

END -- *de IdentificadoresObjetoEjemplo*

A.2 *Perfeccionamiento del entorno amarillo*

El entorno amarillo, descrito en la figura A-1/X.407, se perfecciona formalmente más adelante, utilizando las macros OBJECT y REFINE.

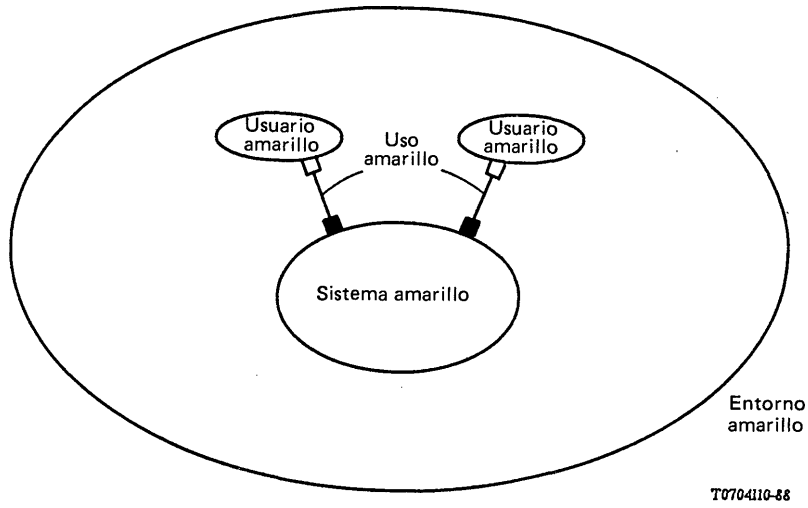


FIGURA A-1/X.407

Entorno amarillo

Como lo indica la figura A-1/X.407 y lo confirma más adelante la especificación NSA.1, el entorno amarillo puede modelarse como un objeto que puede descomponerse en un objeto central, el **sistema amarillo**, y un número cualquiera de otros objetos periféricos, **usuarios amarillos**. El sistema amarillo interactúa con los usuarios amarillos por medio de sus puertos de **utilización amarillos**.

```
YellowEnvironmentRefinement { joint-iso-ccitt
      mhs-motis(6) asdc(2) example(1) modules(0) ye-refinement(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo

EXPORTS
      yellow-environment, yellow-environment-refinement,
      yellow-system, yellow-user;
```

```
IMPORTS
        -- Servicio abstracto amarillo
                yellow-use
                ....
                FROM YellowAbstractService { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) y-abstract-service(2) }

        -- Identificadores de objeto – ejemplo
                id-ot-y-environment, id-ot-y-system, id-ot-y-user,
                id-ref-y-environment
                ....
                FROM ExampleObjectIdentifiers { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0) }

        -- Notación de servicio abstracto
                OBJECT, REFINE
                ....
                FROM AbstractServiceNotation { joint-iso-ccitt
                        mhs-motis(6) asdc(2) modules(0) notation(1) };


-- Entorno amarillo

yellow-environment OBJECT
        ::= id-ot-y-environment


-- Perfeccionamiento del entorno amarillo

yellow-environment-refinement REFINE yellow-environment AS
        yellow-user RECURRING
        yellow-system
                yellow-user [S] PAIRED WITH yellow-user
        ::= id-ref-y-environment


-- Tipos de objeto componente

yellow-user OBJECT
        PORTS {
                yellow-user [C] }
        ::= id-ot-y-user

yellow-system OBJECT
        PORTS {
                yellow-user [S] }
        ::= id-ot-y-system

END -- del perfeccionamiento del entorno amarillo
```

A.3 *Definición del servicio abstracto amarillo*

El servicio abstracto que proporciona el sistema amarillo a sus usuarios se define formalmente más adelante, utilizando las macros PORT y ABSTRACT-BIND, -OPERATION y -ERROR.

Como se indica en la especificación NSA.1, el servicio abstracto que proporciona el sistema amarillo comprende puertos de un solo tipo: de usuario amarillo. Cada puerto comprende un número de operaciones abstractas que informan colectivamente sobre un número de errores abstractos. El sistema amarillo protege sus puertos por medio de una operación abstracta de vinculación, **vinculación amarilla**, que requiere que los usuarios se identifiquen en forma convincente antes de que pueda haber una interacción ulterior. Una operación abstracta de **desvinculación amarilla**, constituye el paso final necesario para concluir una interacción.

```
YellowAbstractService { joint-iso-ccitt
        mhs-motis(6) asdc(2) example(1) modules(0) y-abstract-service(2) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo
```

```
EXPORTS
        AuthenticateUser, Yellow-operation-1, ... yellow-use;


IMPORTS
        -- Ejemplo de identificadores de objeto
                id-pt-y-use
                ....
                FROM ExampleObjectIdentifiers { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0) }

        -- Notación de servicio abstracto
                ABSTRACT-BIND, ABSTRACT-ERROR, ABSTRACT-OPERATION, PORT
                ....
                FROM AbstractServiceNotation { joint-iso-ccitt
                        mhs-motis(6) asdc(2) modules(0) notation(1) };


-- Tipo de puerto

yellow-use PORT
        CONSUMER INVOKES {
                Yellow-operation-1, ... }
        ::= id-pt-y-use


-- Operación abstracta de vinculación

Credentials ::= SET {
                name      [0] IA5String,
                password  [1] IA5String }

YellowBind ::= ABSTRACT-BIND
                TO { yellow-use[S] }
        BIND
                ARGUMENT credentials Credentials
                        BIND-ERROR ENUMERATED {
                                name-or-password-invalid(0) }


-- Operación abstracta de desvinculación

YellowUnbind ::= ABSTRACT-UNBIND
        FROM { yellow-use[S] }


-- Operaciones abstractas

Yellow-operation-1 ::= ABSTRACT-OPERATION
                ARGUMENT ...
                RESULT ...
                ERRORS {
                        yellow-error-1, ... }
...


-- Errores abstractos

yellow-error-1 ABSTRACT-ERROR
                PARAMETER ...
                ::= 1
...

END -- del servicio abstracto amarillo
```

A.4 *Perfeccionamiento del entorno verde*

El entorno verde, descrito en la figura A-2/X.407, se perfecciona formalmente más adelante, utilizando las macros OBJECT y REFINE.

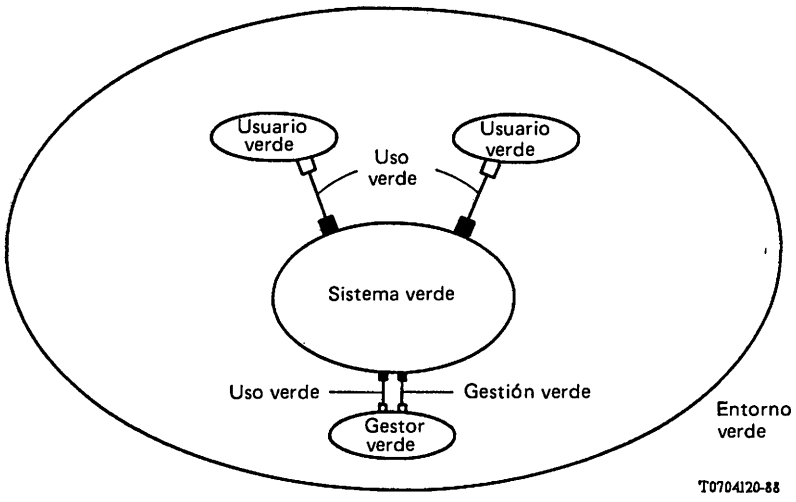


FIGURA A-2/X.407

Entorno verde

Como indica la figura A-2/X.407 y lo confirma la especificación NSA.1 que sigue, el entorno verde puede modelarse como un objeto que puede descomponerse en un objeto central, el **sistema verde**; un número cualquiera de otros objetos periféricos, **usuarios verdes**; y cualquier número de otros objetos adicionales, **gestores verdes**. El sistema verde interactúa con los gestores y usuarios verdes por medio de sus puertos de **usuarios verdes** y con los gestores verdes (aislados) por medio de sus puertos de **gestión verdes**.

```
GreenEnvironmentRefinement {joint-iso-ccitt
        mhs-motis(6) asdc(2) example(1) modules(0) ge-refinement(3)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo


EXPORTS
        green-environment, green-environment-refinement,
        green-manager, green-system, green-user;


IMPORTS
        -- Servicio abstracto verde
                green-use, green-management
                ....
                FROM GreenAbstractService {joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) g-abstract-service(4)}

        --Ejemplo de identificadores de objeto
                id-ot-g-environment, id-ot-g-manager, id-ref-g-environment
                id-ot-g-user, id-ot-g-sytem,
                ....
                FROM ExampleObjectIdentifiers {joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0)}

        -- Notación de servicio abstracto
                OBJECT, REFINE
                ....
                FROM AbstractServiceNotation {joint-iso-ccitt
                        mhs-motis(6) asdc(2) modules(0) notation(1)};
```

```
-- Entorno verde

green-environment OBJECT
        ::= id-ot-g-environment


-- Perfeccionamiento del entorno verde

green-environment-refinement REFINE green-environment AS
        green-user      RECURRING
        green-manager RECURRING
        green-system
                green-use           [S] PAIRED WITH { green-user, green-manager }
                green-management [S] PAIRED WITH { green-manager }
        ::= id-ref-g-environment


-- Tipos de objeto componente

green-user OBJECT
        PORTS {
                green-use           [C] }
        ::= id-ot-g-user

green-manager OBJECT
        PORTS {
                green-use           [C],
                green-management [C] }
        ::= id-ot-g-manager

green-system OBJECT
        PORTS {
                green-use           [S],
                green-management [S] }
        ::= id-ot-g-system

END -- del perfeccionamiento del entorno verde
```

A.5 *Definición del servicio abstracto verde*

El servicio abstracto que proporciona el sistema verde a sus usuarios y gestores se define formalmente más adelante utilizando las macros PORT y ABSTRACT-BIND, -OPERATION y -ERROR.

Como se indica en la especificación NSA.1, el servicio abstracto que proporciona el sistema verde comprende puertos de dos tipos, verde de usuario y verde de gestión. Un puerto de cualquiera de los dos tipos comprende un número de operaciones abstractas que notifican de forma colectiva un cierto número de errores abstractos. El sistema verde protege sus puertos por medio de operaciones abstractas de vinculación, **autenticación de usuario** y **autenticación de gestor**, que requieren que los usuarios y gestores se identifiquen en forma convincente antes de poder continuar la interacción. No se especifica ninguna operación abstracta de desvinculación, lo que indica que no se requiere un paso de finalización para concluir una interacción.

```
GreenAbstractService { joint-iso-ccitt
        mhs-motis(6) asdc(2) example(1) modules(0) g-abstract-service(4) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo


EXPORTS
        AuthenticateManager, AuthenticateUser, green-management,
        Green-management-operation-1, ... green-use,
        Green-use-operation-1, ...;
```

```
IMPORTS
        -- Ejemplo de identificadores de objeto
                id-pt-g-use, id-pt-g-management
                ....
                FROM ExampleObjectIdentifiers {joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0)}

        -- Notación de servicio abstracto
                PORT, ABSTRACT-BIND, ABSTRACT-OPERATION, ABSTRACT-ERROR
                ....
                FROM AbstractServiceNotation {joint-iso-ccitt
                        mhs-motis(6) asdc(2) modules(0) notation(1)};


-- Tipos de puerto

green-use PORT
        CONSUMEER INVOKES{
                Green-use-operation-1, ...}
        ::= id-pt-g-use

green-management PORT
        CONSUMER INVOKES{
                Green-management-operation-1, ...}
        ::= id-pt-g-management


-- Operaciones abstractas – vinculación

Credentials ::= SET{
        name     [0] IA5String,
        password [1] IA5String}

AuthenticateUser ::= ABSTRACT-BIND
        ARGUMENT credentials Credentials
        BIND-ERROR ENUMERATED{
                name-or-password-invalid(0)}

AuthenticateManager ::= ABSTRACT-BIND
        ARGUMENT credentials Credentials
        BIND-ERROR ENUMERATED{
                name-or-password-invalid(0),
                not-a-manager        (1)}


-- Operaciones abstractas

Green-use-operation-1 ::= ABSTRACT-OPERATION
        ARGUMENT ...
        RESULT ...
        ERRORS{
                green-error-1, ...}
...

Green-management-operation-1 ::= ABSTRACT-OPERATION
        ARGUMENT ...
        RESULT ...
        ERRORS{
                green-error-1, ...}
...


-- Errores abstractos

green-error-1 ABSTRACT-ERROR
        PARAMETER ...
        ::= 1
...

END -- del servicio abstracto verde
```

A.6 *Perfeccionamiento del sistema amarillo*

El sistema amarillo, descrito en la figura A-3/X.407, se perfecciona formalmente más adelante utilizando las macros OBJECT y REFINE.

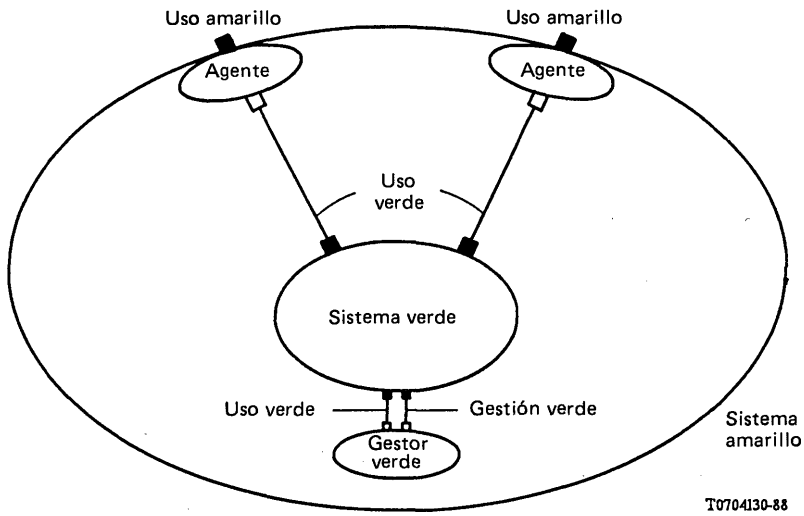


FIGURA A-3/X.407

Sistema amarillo

Como indica la figura A-3/X.407 y lo confirma la especificación NSA.1 el sistema amarillo, cuando se examina de cerca, tiene componentes. En especial, el sistema amarillo comprende el sistema verde y los gestores verdes, aumentado por objetos de una variedad hasta ahora no vista, el *agente*. Un **agente** actúa como intermediario entre el sistema verde y el usuario amarillo. Se podría decir que es un valor añadido al sistema verde. En cualquier caso, es el proveedor de un puerto de uso amarillo y el consumidor de un puerto de uso verde.

```
YellowSystemRefinement {joint-iso-ccitt
    mhs-motis(6) asdc(2) example(1) modules(0) ys-refinement(5)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo

EXPORTS
    agent, yellow-system-refinement;
```

```
IMPORTS
        -- Perfeccionamiento del entorno amarillo
                yellow-system, yellow-use
                ....
                FROM YellowEnvironmentRefinement { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) ye-refinement(1) }

        -- Perfeccionamiento del entorno verde
                green-management, green-manager, green-system,
                green-use
                ....
                FROM GreenEnvironmentRefinement { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) ge-refinement(3) }

        -- Ejemplo de identificadores de objeto
                id-ot-agent, id-ref-y-system
                ....
                FROM ExampleObjectIdentifiers { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0) }

        -- Notación de servicio abstracto
        OBJECT REFINE
                FROM AbstractServiceNotation { joint-iso-ccitt
                        mhs-motis(6) asdc(2) modules(0) notation(1) };


-- Perfeccionamiento del entorno amarillo

yellow-system-refinement REFINE yellow-system AS
        agent RECURRING
                yellow-use          [S] VISIBLE
        green-manager RECURRING
        green-system
                green-use           [S] PAIRED WITH agent, green-manager
                green-management    [S] PAIRED WITH green-manager
        ::= id-ref-y-system


-- Tipo de objeto componente

agent OBJECT
        PORTS {
                yellow-use          [S],
                green-use           [C] }
        ::= id-ot-agent

END -- del perfeccionamiento del sistema amarillo
```

A.7 *Realización del sistema amarillo*

El servicio abstracto del sistema amarillo se realiza formalmente a continuación, por medio del SOD, utilizando las macros APPLICATION-CONTEXT y APPLICATION-SERVICE-ELEMENT de la Recomendación X.219.

Como se indica en la especificación NSA.1, el servicio abstracto que proporciona el sistema amarillo se realiza como una sola ESA, la **ESA-uso-amarillo**, y un solo CA con el correspondiente **CA-uso-amarillo**. Cada operación abstracta de vinculación, operación abstracta o error abstracto en el servicio abstracto tiene una operación correspondiente de unión, operación o error equivalente y en la realización basada en el SOD respectivamente.

Obsérvese que las operaciones reciben asignación de valores enteros; las operaciones abstractas correspondientes ni requieren, ni reciben dichos valores.

```
YellowSystemRealization { joint-iso-ccitt
        mhs-motis(6) asdc(2) example(1) modules(0) ys-realization(6) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo
```

```
EXPORTS
        yellow-use-AC, yellow-use-ASE;


IMPORTS
        -- Servicio abstracto amarillo
                Yellow-operation-1, ... yellow-use, YellowBind,
                YellowUnbind
                ....
                FROM YellowAbstractService { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) y-abstract-service(2) } ,

        -- Ejemplo identificadores de objeto
                id-ac-y-use, id-as-y-use, id-ase-y-use
                ....
                FROM ExampleObjectectIdentifiers { joint-iso-ccitt
                        mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0) }

        UDPA operaciones a distancia
                rOSE
                ....
                FROM Remote-Operations-APDUs { joint-iso-ccitt
                        remote-operations(4) apdus(1) }

        -- Control de asociación
                aCSE
                ....
                FROM Remote-Operations-Notation-extension
                        { joint-iso-ccitt remote-operations(4)
                        notation-extension(2) }

        -- Ampliación de notación de operaciones a distancia
                APPLICATION-CONTEXT, APPLICATION-SERVICE-ELEMENT
                ....
                FROM Remote-Operations-Notation-extension { joint-iso-ccitt
                        remote-operations(4) notation-extension(2) };


aCSE-AS OBJECT INDENTIFIER ::=
                { joint-iso-ccitt association-control(2)
                abstractSyntax(1) apdus(0) version1(1) }


-- Contexto de aplicaciones

yellow-use-AC APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND YellowBind
        UNBIND YellowUnbind
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { yellow-use-ASE }
        ABSTRACT SYNTAXES { yellow-use-AS, aCSE-AS }
        ::= id-ac-y-use


-- Elemento de servicio de aplicación

yellow-use-ASE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                yellow-operation-1, ... }
        ::= id-ase-y-use

yellow-operation-1 Yellow-operation ::= 1
...


-- Sintaxis abstracta

yellow-use-AS OBJECT IDENTIFIER ::= id-as-y-use

END -- de realización del sistema amarillo
```

A.8 *Realización del sistema verde*

El servicio abstracto del sistema verde se realiza formalmente más adelante, por medio del SOD, utilizando las macros APPLICATION-CONTEXT y APPLICATION-SERVICE-ELEMENT de la Recomendación X.219.

Como se indica en la especificación NSA.1, el servicio abstracto que proporciona el sistema verde se realiza como dos ESA, la **ESA-uso-verde** y la **ESA-gestión-verde** y los dos CA correspondientes, **CA-uso-verde** y **CA-gestión-verde**. Cada operación abstracta de unión, operación abstracta o error abstracto en el servicio abstracto tienen una operación correspondiente y equivalente de vinculación, operación o error, respectivamente en su realización basada en el SOD.

Obsérvese que estas operaciones reciben valores enteros, las operaciones abstractas correspondientes ni requieren, ni reciben dichos valores.

```
GreènSystemRealization { joint-iso-ccitt
    mhs-motis(6) asdc(2) example(1) modules(0) gs-realization(7) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo


EXPORTS
    green-management-AC, green-management-ASE, green-use-AC,
    green-use-ASE;


IMPORTS
    -- Servicio abstracto verde
        AuthenticateManager, AuthenticateUser,
        green-management, Green-management-operation-1, ...
        green-use, Green-use-operation-1, ...
        ....
        FROM GreenAbstractService { joint-iso-ccitt
            mhs-motis(6) asdc(2) example(1) modules(0) g-abstract-service(4) }

    -- Ejemplo de identificadores de objeto
        id-ac-g-use,          id-ase-g-use,          id-as-g-use,
        id-ac-g-management,   id-ase-g-management,   id-as-g-management
        ....
        FROM ExampleObjectIdentifiers { joint-iso-ccitt
            mhs-motis(6) asdc(2) example(1) modules(0) object-identifiers(0) }

    -- UDPA de operaciones a distancia
        rOSE
        ....
        FROM Remote-Operations-APDUs { joint-iso-ccitt
            remote-operations(4) apdus(1) }

    -- Control de asociación
        aCSE
        ....
        FROM Remote-Operations-Notation-extension { joint-iso-ccitt
            remote-operations(4) notation-extension(2) }

    -- Ampliación de notación de operaciones a distancia
        APPLICATION-CONTEXT, APPLICATION-SERVICE-ELEMENT
        ....
        FROM Remote-Operations-Notation-extension { joint-iso-ccitt
            remote-operations(4) notation-extension(2) };


aCSE-AS OBJECT IDENTIFIER ::=
        { joint-iso-ccitt association-control(2)
        abstractSyntax(1) apdus(0) version(1) }
```

```
-- Contexto de aplicación

green-use-AC APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND AuthenticateUser
        UNBIND NoOperation
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { green-use-ASE }
        ABSTRACT SYNTAXES { green-use-AS, aCSE-AS }
        ::= id-ac-g-use

green-management-AC APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND AuthenticateManager
        UNBIND NoOperation
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { green-management-ASE }
        ABSTRACT SYNTAXES { green-management-AS, aCSE-AS }
        ::= id-ac-g-management

NoOperation ::= UNBIND


-- Elementos de servicio de aplicación

green-use-ASE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                green-use-operation-1, ... }
        ::= id-ase-g-use

green-management-ASE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                green-management-operation-1, ... }
        ::= id-ase-g-management

green-use-operation-1 Green-use-operation-1 ::= 1
...

green-management-operation-1 Green-management-operation-1 ::= 50
...


-- Sintaxis abstractas

green-use-AS OBJECT IDENTIFIER ::= id-as-g-use

green-management-AS OBJECT IDENTIFIER ::= id-as-g-management

END -- de realización del sistema verde
```

ANEXO B

(a la Recomendación X.407)

Definición de las referencias de identificadores de objeto

Este anexo forma parte integrante de esta Recomendación.

Este anexo define, con fines de referencia, varios de los identificadores de objeto citados en los módulos NSA.1 del anexo C. Utiliza la NSA.1.

Con excepción de los asignados en el anexo A, todos los identificadores de objeto que asigna esta Recomendación están considerados en este anexo. El anexo es definitivo, excepto para los propios módulos NSA.1 y el objeto de los convenios de definición de servicio de aplicación. Las asignaciones definitivas para los módulos se presentan en los módulos mismos; en la sección IMPORT aparecen otras referencias. La última es fija.

```
ASDCObjectIdentifiers { joint-iso-ccitt
      mhs-motis(6) asdc(2) modules(0) object-identifiers(0) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo

-- Exporta todo.

IMPORTS -- nada --;

ID ::= OBJECT IDENTIFIER

-- Convenios (no definitivos) de definición del servicio abstracto

id-asdc ID ::= { joint-iso-ccitt mhs-motis(6) asdc(2) } -- no definitivo

-- Categorías

id-mod ID ::= { id-asdc 0 } -- módulos; no definitivo
id-ex  ID ::= { id-asdc 1 } -- ejemplo; no definitivo

-- Módulos

id-mod-object-identifiers ID ::= { id-mod 0 } -- no definitivo
id-mod-notation           ID ::= { id-mod 1 } -- no definitivo

END -- de identificadores de objeto ASDC
```

ANEXO C

(a la Recomendación X.407)

Definición de la referencia de notación

Este anexo forma parte integrante de esta Recomendación.

Este anexo, complemento de la sección 2, define, con fines de referencia, la notación para especificar modelos y servicios abstractos. Utilizar la NSA.1.

```
AbstractServiceNotation { joint-iso-ccitt
      mhs-motis(6) asdc(2) modules(0) notation(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
-- Prólogo

EXPORTS
      ABSTRACT-BIND, ABSTRACT-ERROR, ABSTRACT-OPERATION,
      ABSTRACT-UNBIND, OBJECT, PORT, REFINE;

IMPORTS
      -- Notación de operaciones a distancia
            BIND, ERROR, OPERATION, UNBIND
            ----
            FROM Remote-Operations-Notation { joint-iso-ccitt
                  remote-operations(4) notation(0) };
```

-- *Macro objeto*

```
OBJECT MACRO ::=
BEGIN

TYPE NOTATION       ::= "PORTS" "{" PortList "}" | empty
VALUE NOTATION      ::= value (VALUE OBJECT IDENTIFIER)

PortList            ::= Port " , " PortList | Port
Port                ::= value (PORT) PortType

PortType            ::= Symmetric | Asymmetric

Symmetric           ::= empty
Asymmetric          ::= Consumer | Supplier

Consumer            ::= "[C]"
Supplier            ::= "[S]"

END
```

-- *Macro puerto*

```
PORT MACRO ::=
BEGIN

TYPE NOTATION       ::= Operations | empty
VALUE NOTATION      ::= value (VALUE OBJECT IDENTIFIER)

Operations          ::= Symmetrical | Asymmetrical

Symmetrical         ::= "ABSTRACT" "OPERATIONS" "{" OperationList "}"
Asymmetrical        ::= OneSided | TwoSided

OneSided            ::= Consumer | Supplier
TwoSided            ::= Consumer Supplier | Supplier Consumer

Consumer            ::= "CONSUMER" "INVOKES" "{" OperationList "}"
Supplier            ::= "SUPPLIER" "INVOKES" "{" OperationList "}"

OperationList       ::= Operation "," OperationList | Operation
Operation           ::= value (ABSTRACT-OPERATION)

END
```

-- *Macro perfeccionamiento*

```
REFINE MACRO ::=
BEGIN

TYPE NOTATION       ::= Object "AS" ComponentList
VALUE NOTATION      ::= value (VALUE OBJECT IDENTIFIER)

ComponentList       ::= Component ComponentList | Component
Component           ::= ObjectSpec PortSpecList

ObjectSpec          ::= Object | Object "RECURRING"

PortSpecList        ::= PortSpec PortSpecList | PortSpec
PortSpec            ::= value (PORT) PortType PortStatus

PortType            ::= Consumer | Supplier | empty
Consumer            ::= "[C]"
Supplier            ::= "[S]"

PortStatus          ::= "VISIBLE" | "PAIRED" "WITH" ObjectList

ObjectList          ::= Object " , " ObjectList | Object
Object              ::= value (OBJECT)

END
```

-- Macros vinculación abstracta, desvinculación, operación y error

```
ABSTRACT-BIND MACRO ::=
BEGIN

TYPE NOTATION       ::= Ports Bind
VALUE NOTATION      ::= value (VALUE BindType)

Ports               ::= "TO" "{" PortList "}" | empty
PortList            ::= Port " , " PortList | Port
Port                ::= value (PORT) PortSide
PortSide            ::= Consumer | Supplier | empty
Consumer            ::= "[C]"
Supplier            ::= "[S]"

Bind                ::= type (BindType) -- ha de ser un tipo BIND
                        | empty <BindType ::= BIND>

END
```

```
ABSTRACT-UNBIND MACRO ::=
BEGIN

TYPE NOTATION       ::= Ports Unbind
VALUE NOTATION      ::= value (VALUE UnbindType)

Ports               ::= "FROM" "{" PortList "}" | empty
PortList            ::= Port " , " PortList | Port
Port                ::= value (PORT) PortSide
PortSide            ::= Consumer | Supplier | empty
Consumer            ::= "[C]"
Supplier            ::= "[S]"

Unbind              ::= type (UnbindType) -- ha de ser un tipo UNBIND
                        | empty <UnbindType ::= UNBIND>

END
```

```
ABSTRACT-OPERATION MACRO ::= OPERATION

ABSTRACT-ERROR MACRO ::= ERROR

END -- de notación de servicio abstracto
```

ANEXO D

(a la Recomendación X.407)

Diferencias entre la Recomendación del CCITT y la Norma de la ISO

Este anexo no forma parte de esta Recomendación.

Este anexo enumera todas las diferencias, salvo las puramente estilísticas, entre esta Recomendación y la Norma internacional ISO correspondiente.

No existen diferencias entre las dos especificaciones.

ANEXO E

(a la Recomendación X.407)

Índice

Este anexo constituye el índice de esta Recomendación. Proporciona el número o números de apartado(s) en que se define cada elemento de las diferentes categorías. La cobertura de cada categoría es exhaustiva.

Este anexo presenta un índice de los elementos (si los hay) en las siguientes categorías:

a) abreviaturas;
b) términos;
c) elementos de información;
d) módulos NSA.1;
e) macros NSA.1;
f) tipos NSA.1;
g) valores NSA.1;
h) *acuerdos bilaterales*;
i) elementos que requieren ulterior estudio;
j) elementos por preparar.

E.1 *Abreviaturas*

NSA.1 3
CA 3
ESA 3
ISA 3
SOD 3
UDPA 3

E.2 *Términos*

argumento 8.1
asociación 7.3
asociación abstracta 7.3
asimétrico 7.2
concordancia 7.2
consumidor 7.2
desvinculación 7.2
ejecución 8.1
ejecutador 8.1
error abstracto 8.5
información de error 8.3
iniciador 8.2
invocación 8.1
invocador 8.1
modelo 7
modelo abstracto 7
objeto 7.1
objeto abstracto 7.1
operación abstracta 8.4
operación abstracta de desvinculación 8.3
operación abstracta de vinculación 8.2
parámetro 8.5
perfeccionamiento 7.4
perfeccionamiento abstracto 7.4
procedimiento 8.1
procedimiento abstracto 8.1
proveedor 7.3
proveedor del servicio abstracto 7.3
puerto 7.2
puerto abstracto 7.2
real 9
realizador
respondedor 8.2
resultado 8.1
servicio abstracto 7.3
simétrico 7.2
suministrador 7.2
usuario 7.3
usuario de servicio abstracto 7.3
vinculación 7.2
vinculado 7.2

SISTEMAS DE TRATAMIENTO DE MENSAJES: REGLAS DE CONVERSIÓN DE TIPOS DE INFORMACIÓN CODIFICADA

(Málaga-Torremolinos, 1984; modificada en Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión, controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de servicios de mensajería interpersonal y de transferencia de mensajes;

(b) la necesidad de transferir mensajes de diferentes tipos que se presentan en una gran variedad de formatos;

(c) que las Recomendaciones de la serie F definen los servicios de telemática;

(d) que las Recomendaciones de la serie T definen los equipos terminales y procedimientos de control que han de utilizarse en los servicios telemáticos;

(e) que las Recomendaciones de la serie V especifican los medios para la comunicación de datos por la red telefónica;

(f) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(g) que un conjunto de Recomendaciones describe diversos aspectos del tratamiento de mensajes: X.400, X.402, X.403, X.407, X.408, X.411, X.413, X.419 y X.420;

(h) que el CCITT y la ISO han elaborado un conjunto adecuado de reglas de conversión;

(i) que, para aplicaciones de usuario específicas, pueden desarrollarse algunas variantes y aplicarse mediante acuerdo bilateral,

recomienda por unanimidad

(1) que la finalidad y campo de aplicación de esta Recomendación sean los expuestos en el § 1;

(2) que los aspectos generales de las reglas de conversión entre tipos de información codificada sean los que se describen en el § 2;

(3) que las reglas de conversión para tipos de información codificada particulares sean las que se definen en los puntos siguientes.

ÍNDICE

1 *Finalidad y objeto*

2 *Aspectos generales de la conversión*

2.1 Tipos de información codificada

2.2 Dos aspectos de la conversión

2.3 Pérdida de información

2.4 Propiedades de los tipos de información codificada

3 *Conversión desde TLX*

- 3.1 Conversión de TLX a texto AI5
- 3.2 Conversión de TLX a TTX
- 3.3 Conversión de TLX a FaxG3
- 3.4 Conversión de TLX a G4 Clase 1
- 3.5 Conversión de TLX a videotex
- 3.6 Conversión de TLX a voz
- 3.7 Conversión de TLX a modo mixto

4 *Conversión desde texto AI5*

- 4.1 Conversión de texto AI5 a TLX
- 4.2 Conversión de texto AI5 a TTX
- 4.3 Conversión de texto AI5 a FaxG3
- 4.4 Conversión de texto AI5 a G4 Clase 1
- 4.5 Conversión de texto AI5 a videotex
- 4.6 Conversión de texto AI5 a voz
- 4.7 Conversión de texto AI5 a modo mixto

5 *Conversión desde TTX*

- 5.1 Conversión de TTX a TLX
- 5.2 Conversión de TTX a texto AI5
- 5.3 Conversión de TTX a TTX
- 5.4 Conversión de TTX a FaxG3
- 5.5 Conversión de TTX a G4 Clase 1
- 5.6 Conversión de TTX a videotex
- 5.7 Conversión de TTX a voz
- 5.8 Conversión de TTX a modo mixto

6 *Conversión desde FaxG3*

- 6.1 Conversión de FaxG3 a FaxG3
- 6.2 Conversión de FaxG3 a G4 Clase 1
- 6.3 Conversión de FaxG3 a modo mixto

7 *Conversión desde G4 Clase 1*

- 7.1 Conversión de G4 Clase 1 a FaxG3
- 7.2 Conversión de G4 Clase 1 a G4 Clase 1
- 7.3 Conversión de G4 Clase 1 a modo mixto

8 *Conversión desde videotex*

- 8.1 Conversión de videotex a TLX
- 8.2 Conversión de videotex a texto AI5
- 8.3 Conversión de videotex a TTX
- 8.4 Conversión de videotex a FaxG3
- 8.5 Conversión de videotex a G4 Clase 1
- 8.6 Conversión de videotex a videotex
- 8.7 Conversión de videotex a voz
- 8.8 Conversión de videotex a modo mixto

9 *Conversión desde voz*

- 9.1 Conversión de voz a voz

10 *Conversión desde modo mixto*

10.1 Conversión de modo mixto a TLX
10.2 Conversión de modo mixto a texto AI5
10.3 Conversión de modo mixto a TTX
10.4 Conversión de modo mixto a FaxG3
10.5 Conversión de modo mixto a G4 Clase 1
10.6 Conversión de modo mixto a videotex
10.7 Conversión de modo mixto a voz
10.8 Conversión de modo mixto a modo mixto

Anexo A – Tablas de conversión de códigos

Anexo B – Abreviaturas

1 Finalidad y objeto

La presente Recomendación forma parte de un conjunto de Recomendaciones sobre tratamiento de mensajes. Este conjunto de Recomendaciones establece una especificación completa sobre el tratamiento de mensajes aplicable a un número cualquiera de sistemas abiertos cooperantes.

En esta Recomendación se especifican los algoritmos empleados por el STM al efectuar la conversión entre diferentes tipos de información codificada.

Hay otros aspectos del tratamiento de mensajes que están definidos en otras Recomendaciones. La totalidad del sistema y de los servicios de tratamiento de mensajes se especifican en la Recomendación X.400. La arquitectura global del STM está definida en la Recomendación X.402. En la Recomendación X.403 se describen las pruebas de conformidad para componentes STM. Los convenios aplicados para la definición de los servicios abstractos prestados por los componentes STM se definen en la Recomendación X.407. El servicio abstracto proporcionado por el STRM, y los procedimientos que rigen su funcionamiento distribuido, se definen en la Recomendación X.411. En la Recomendación X.413 se define el servicio abstracto proporcionado por la MM. En la Recomendación X.419 se especifican los protocolos de aplicación que rigen la interacción de los componentes STM. En la Recomendación X.420 se especifica el sistema de mensajería interpersonal, que es una aplicación del tratamiento de mensajes.

En el § 2 de esta Recomendación se describen los aspectos generales de la conversión en el STM. En los § 3 a 10 se definen reglas de conversión particulares. El anexo A contiene tablas de conversión de códigos y el anexo B las abreviaturas utilizadas.

2 Aspectos generales de la conversión

Entre los elementos de datos sujetos a conversión están el objeto y el cuerpo de un mensaje. La conversión tiene dos aspectos: formato y código. El aspecto de control se describe en otras Recomendaciones conexas.

2.1 *Tipos de información codificada*

Esta Recomendación define las reglas de conversión para los ocho tipos de información codificada utilizados en el STM. Para referirse a cada tipo, se utilizan los términos siguientes:

TLX	El código se define en la Recomendación F.1. El formato se define en la Recomendación S.5.
Texto AI5	El código se define en la Recomendación T.50.
TTX	El formato se define en las Recomendaciones F.200 y T.60, y el código se define en la Recomendación T.61.
FaxG3	El esquema de codificación se define en la Recomendación T.4, y la señalización del esquema de codificación se define en la Recomendación T.30.
G4 Clase 1	El formato y el esquema de codificación se definen en las Recomendaciones T.6, T.503 y T.563.
Videotex	El formato y el esquema de codificación se definen en las Recomendaciones T.101, T.504 y T.541.
Voz	El esquema de codificación será objeto de ulterior estudio.
Modo mixto	El formato y el esquema de codificación se definen en las Recomendaciones T.501 y T.561.

Nota – TLX: Télex, TTX: Teletex.

Los tipos TTX y FaxG3 tienen dos subtipos: básico y facultativo. El tipo G4 clase 1 y el modo mixto tienen dos subtipos: básico y no básico.

El cuadro 1/X.408 describe todas las conversiones imaginables entre los tipos y los subtipos mencionados anteriormente. Se caracteriza cada una de ellas como: (–) no conversión, a) posible sin pérdida de información, b) posible pero puede producirse pérdida de información, o c) no es práctica. Esta Recomendación define las reglas para la conversión de formato y código para conversiones de las categorías segunda y tercera.

CUADRO 1/X.408

Conversiones de tipos de información codificada

De \ A		TLX	Texto AI5	TTX		FAX G3		G4 Clase 1		Videotex	Voz	Modo mixto	
				básico	facultativo [1]	básico	facultativo [1]	básico	no básico [1]			básico	no básico [1]
TLX [4]		–	b [7]	a	a	a	a	a	a	b	UE	a	a
Texto IA5		b	–	b	b	b	b	b	b	b	UE	b	b
TTX	básico	b	b	–	a	a	a	a	a	a	UE	a	a
	facultativo [1]	b	b	b	b [2], [3]	b	b	b	b	a	UE	a	b [2], [3]
Fax G3	básico	c	c	c	c	–	a	a	a	c [5]	c	a	a
	facultativo [1]	c	c	c	c	b	b [2], [3]	b	b	c [5]	c	b	b
G4 Clase 1	básico	c	c	c	c	b	b	–	a	c [5]	c	a	a
	no básico [1]	c	c	c	c	b	b	b	b [2], [3]	c [5]	c	b	b [2], [3]
Videotex		b	b	b	b	b [6]	b [6]	b [6]	b [6]	b	UE	UE	UE
Voz		c	c	c	c	c	c	c	c	c	UE	c	c
Modo mixto	básico	b	b	b	b	b	b	a	a	b	UE	–	a
	no básico [1]	b	b	b	b [2], [3]	b	b	b	b [2], [3]	b	UE	b	b [2], [3]

– No conversión
a Posible sin pérdida de información
b Posible pero puede producirse pérdida de información
c No es práctica
UE Para ulterior estudio

[1] Especificado en las Recomendaciones pertinentes.

[2] No se pierde información si los terminales de origen y de destino tienen las mismas funciones facultativas.

[3] La información puede perderse si el terminal de origen utiliza funciones facultativas de las que carece el terminal de destino.

[4] Se supone que el carácter «¿Con quién comunico?» (WRU) es un elemento de protocolo utilizado para comunicar con el terminal teletex, y no forma parte del contenido del mensaje.

[5] Puede ser posible con pérdida de información, si el terminal de destino tiene la capacidad de tipo de información fotográfica.

[6] En la conversión de videotex, se puede perder información de color.

[7] Cuando el texto AI5 tiene menos de 69 caracteres por línea, puede perderse información de formato.

2.2 *Dos aspectos de la conversión*

Las reglas de conversión tienen dos aspectos:

1) el aspecto formato;
2) el aspecto código.

Las reglas de conversión para los tipos de información codificada que tienen estructuras lógicas serán objeto de ulterior estudio.

2.2.1 *Reglas fundamentales*

Si existe actualmente una norma sobre la conversión entre diferentes tipos de información, debe hacerse referencia a la misma sin ninguna modificación a menos que sea necesario. Si no existe se aplican las siguientes reglas fundamentales:

1) Si existen normas sobre el asunto y tipos de objeto, la regla de conversión debe definirse de manera que se mantenga la parte de intersección de las normas. La creación de nuevas reglas para partes sin intersección debe basarse en requisitos claros; de lo contrario no deben crearse.
2) Cuando no existen normas para el asunto ni para el tipo objeto, las reglas de conversión deberán definirse de manera que los tipos normalizados puedan adaptarse en la mayor medida posible para ambos sentidos de la conversión.
3) Cuando ninguno de los tipos tiene una norma, la definición de las reglas deberá ser objeto de ulterior estudio.

2.2.2 *Aspectos de formato*

El aspecto de formato representa los atributos dimensionales del espacio de presentación de los mensajes de usuario.

Debe especificarse el aspecto bidimensional (X e Y) de la conversión para un mensaje que se transfiere. Después deben definirse los parámetros para ese aspecto. Deberá ser objeto de ulterior estudio si la voz deberá considerarse o no en el mismo contexto.

a) El sentido X del espacio de presentación se define por uno de estos dos medios:
   1) El tamaño de un carácter y el número de caracteres que ha de presentarse.
   2) Longitud.

   Si el tipo de objeto tiene un tamaño menor en el sentido X que el tipo de asunto, deberá definirse un mecanismo de ajuste de la longitud de línea, tal como la inserción de un par CR-LF, como regla de conversión de formato.

b) El sentido Y del espacio de presentación se define por uno de estos dos medios:
   1) El número de líneas por espacio de presentación o por longitud unidad.
   2) Longitud.

   Si el tipo de objeto tiene un tamaño de página en el sentido Y menor que el del tipo de asunto, deberá definirse un mecanismo de cambio del formato de página, tal como la inserción de un par CR-FF, como regla de conversión de formato. Si el tipo de objeto no tiene limitación de longitud en el sentido Y y el tipo de asunto está paginado, deberá definirse alguna regla de conversión de formato, tal como la inserción de una o más líneas en blanco, para representar el límite de páginas.

   Al convertir caracteres a FaxG3 o G4 Clase 1, se aplicarán las reglas de formación de imágenes con arreglo a la Recomendación T.351.

2.2.3 *Aspecto de código*

En relación con el aspecto de código, el anexo A especifica la conversión entre diferentes tipos. Si hace falta, pueden encontrarse más informaciones en las distintas secciones.

2.3 *Pérdida de información*

2.3.1 *Hipótesis de partida en relación con la pérdida de información*

Cuando se consideró la conversión entre diferentes tipos de información codificada, se partió de ciertas hipótesis. Los cambios del tipo de carácter, del tamaño de los caracteres o del tipo de papel, etc., no se consideran una pérdida de información.

2.3.2 *Pérdida de información sobre el formato*

Las conversiones de formato adoptan dos formas diferentes: longitud de la línea y número de líneas. Son aplicables las siguientes definiciones:

1) *Longitud de la línea (número de caracteres)*
   a) longitud de la línea del originador menor o igual que la longitud de la línea del destinatario: no hay pérdida de información;
   b) longitud de la línea del originador mayor que la longitud de la línea del destinatario: pérdida de información.
2) *Longitud de la página (número de líneas)*
   a) longitud de la página del originador menor o igual que la longitud de la página del destinatario: no hay pérdida de información. No obstante, en las páginas del destinatario deberá insertarse un campo en blanco entre las páginas del originador;
   b) longitud de la página del originador mayor que la de la página del destinatario: no hay pérdida de información, siempre que la página del originador se haga corresponder con un número entero de páginas del destinatario.

Nota – También se puede perder información por las diferencias entre las zonas imprimible y reproducible en facsímil.

2.3.3 *Pérdida de información de código*

Si un carácter gráfico es reproducido de manera idéntica en ambos sistemas, no hay pérdida de información. Sin embargo, si se produce un cambio entre bastardilla, negrita, subrayado, normal o en color (como en el caso de videotex), esto podría considerarse una pérdida de información (por ejemplo, un tipo de reproducción podría significar un resultado financiero positivo, y el otro, un resultado negativo!). Esto requiere ulterior estudio.

Una conversión a un carácter similar, pero no idéntico, en el segundo sistema es pérdida de información. Una conversión de un carácter a muchos caracteres (por ejemplo, $ a dólar) es también pérdida de información.

2.4 *Propiedades de los tipos de información codificada*

A continuación se indican las propiedades de los tipos de información codificada contemplados en esta Recomendación.

2.4.1 *Tipo de información codificada TLX*

El tipo de información codificada TLX no es paginado. Una línea de texto TLX contiene como máximo 69 caracteres gráficos, según se define en la Recomendación S.5. El final de una línea se representa también por un par CR-LF del ATI2.

2.4.2 *Tipo de información codificada texto AI5*

El tipo de información codificada texto AI5 es paginado. Una línea de texto AI5 contiene un máximo de N_1 caracteres gráficos. El final de una línea se representa también por un par CR-LF del AI5. Una página de texto AI5 contiene un máximo de M_1 líneas. El final de una página se representa también por un par CR-FF del AI5.

Nota – En esta Recomendación no se suponen valores para N_1 o M_1 a menos que se indique de manera explícita en las secciones pertinentes. Un valor normal para N_1 es 80.

2.4.3 *Tipo de información codificada TTX*

El tipo de información codificada TTX es paginado. El formato de una página TTX se define por la «condición por defecto, del teletex básico» siguiente:

- tamaño del papel y orientación: formato de página básica con orientación vertical;
- espaciamiento de los caracteres: 2,54 mm;
- espaciamiento de las líneas: 4,23 mm;
- reproducción: reproducción por defecto.

Esto significa que el número máximo de caracteres por línea es 77 y el número máximo de líneas por página es 55. El final de una línea TTX se representa por un par CR-LF de TTX. El final de una página TTX se representa por un par CR-FF de TTX.

Nota – En la conversión desde teletex, cada línea teletex deberá ir precedida por 5 espacios reducidos por el número de retrocesos (BS) encontrados al comienzo de cada línea teletex (véase el § 7.6.9.1 de la Recomendación F.200).

2.4.4 *Tipo de información codificada FaxG3*

El tipo de información codificada FaxG3 es paginado. El formato de un FaxG3 es el descrito en la Recomendación T.4.

2.4.5 *Tipo de información codificada G4 Clase 1*

El tipo de información codificada G4 Clase 1 es paginado. El formato correspondiente a G4 Clase 1, se define en la Recomendación T.563.

2.4.6 *Tipo de información codificada videotex*

El tipo de información codificada videotex es paginado. Una línea videotex contiene un máximo N_2 caracteres gráficos. El final de una línea se representa por un par APD-APR de videotex. Una página videotex contiene un máximo de M_2 líneas en la zona de visualización definida. El final de una página se representa por un CS de videotex. La función de desplazamiento no se efectúa.

Entre los diversos elementos gráficos que puede tratar el videotex, las reglas siguientes se aplican solamente a los caracteres alfanuméricos en los elementos de datos de visualización. El empleo de la sintaxis de datos de interfuncionamiento (SDI) requiere ulterior estudio.

Nota – En esta Recomendación no se suponen valores de N_2 o M_2; estos valores pueden ser diferentes según la sintaxis utilizada.

2.4.7 *Tipo de información codificada voz*

Requiere ulterior estudio.

2.4.8 *Tipo de información codificada modo mixto*

El formato y esquema de codificación están definidos en las Recomendaciones T.501 y T.561.

3 Conversión desde TLX

3.1 *Conversión de TLX a texto AI5*

3.1.1 *Conversión de formato*

Una línea de TLX se convierte directamente en línea de texto AI5, si el número de caracteres gráficos de la línea de TLX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en la línea de texto AI5 (N_1) y si el número de líneas en un TLX no es mayor que el número de líneas disponibles en una página de texto AI5 (M_1).

Un par de CR-LF del ITA2 invoca una nueva línea de texto AI5. Si no hay un LF asociado con un CR, puede insertarse un LF después del CR.

Una línea de TLX deberá convertirse en el número adecuado de líneas de texto AI5 (con la posible inserción de un par CR-LF del AI5), si el número de caracteres gráficos de la línea TLX con conversión de código es mayor que N_1. Cada línea de texto AI5 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de texto AI5. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un texto TLX debería dividirse en el número adecuado de páginas de texto AI5 si el número de líneas TLX con conversión de código es mayor que M_1. Cada página de texto AI5 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página de texto AI5. El número de líneas en un TLX debería calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Nota – La inclusión del modo escape a datos en un TLX requiere ulterior estudio.

Otros aspectos distintos de los anteriores (por ejemplo, espaciamiento de los caracteres, espaciamiento de las líneas, etc.) están fuera del ámbito de esta regla de conversión.

3.1.2 *Conversión de código*

Esta regla de conversión de código se define en el anexo A.

3.2 *Conversión de TLX a TTX*

3.2.1 *Conversión de formato*

Un texto TLX se convierte directamente en un texto TTX si el número de caracteres gráficos de la línea TLX, con conversión de código, no es mayor que el número máximo de caracteres gráficos disponibles en una línea de texto TTX y si el número de líneas en un TLX no es mayor que el número de líneas disponibles en una página TTX.

Un par CR-LF del ATI2 invoca una nueva línea de texto TTX. Si no hay un LF asociado con un CR, puede insertarse un LF después del CR.

Una línea de texto TLX deberá convertirse en el número adecuado de líneas de texto TTX (con la posible inserción de un par CR-LF de TTX) si el número de caracteres gráficos de la línea TLX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de texto TTX. Cada línea de texto TTX dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de texto TTX. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un texto TLX deberá dividirse en el número adecuado de páginas TTX (con la posible inserción de un par CR-FF de TTX) si el número de líneas TLX con conversión de código es mayor que el número de líneas disponibles en una página TTX. Cada página TTX dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página TTX. El número de líneas en un TLX deberá calcularse tras la inserción de cuantos pares CR-LF de TTX sean necesarios.

3.2.2 *Conversión de código*

Esta regla de conversión se define en el anexo A.

3.3 *Conversión de TLX a FaxG3*

3.3.1 *Conversión de formato*

Un texto TLX se convierte directamente en un FaxG3 si el número de caracteres gráficos de la línea TLX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres FaxG3 y si el número de líneas en el TLX no es mayor que el número de líneas disponibles en una página FaxG3.

Un par CR-LF del ATI2 invoca una nueva línea de caracteres FaxG3. Si no hay un LF asociado con un CR, puede insertarse un LF después del CR.

Una línea de texto TLX deberá convertirse en el número adecuado de líneas de caracteres FaxG3 (con la posible inserción de un par CR-LF del ATI2) si el número de caracteres gráficos en una línea TLX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres FaxG3. Cada línea de caracteres FaxG3 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres FaxG3. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un texto TLX deberá dividirse en el número adecuado de páginas FaxG3 si el número de líneas TLX con conversión de código es mayor que el número disponible en una página FaxG3. Cada página FaxG3 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página FaxG3. El número de líneas en un TLX deberá calcularse tras la inserción de cuantos pares CR-LF del ATI2 sean necesarios.

La imaginización de caracteres en FaxG3 será conforme con la Recomendación T.351.

3.3.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

3.4 *Conversión de TLX a G4 Clase 1*

3.4.1 *Conversión de formato*

Un texto TLX se convierte directamente en un G4 Clase 1 si el número de caracteres gráficos de la línea TLX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1 y si el número de líneas del TLX no supera el número de líneas disponibles en una página G4 Clase 1.

Un par CR-LF del ATI2 invoca una nueva línea de caracteres G4 Clase 1. Si no hay un LF asociado con un CR, puede insertarse un LF después del CR.

Una línea de texto TLX deberá convertirse en el número adecuado de líneas de caracteres G4 Clase 1 (con la posible inserción de un par CR-LF del ATI2) si el número de caracteres gráficos en una línea TLX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1. Cada línea de caracteres G4 Clase 1 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres G4 Clase 1. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un texto TLX deberá dividirse en el número adecuado de páginas G4 Clase 1, si el número de líneas TLX con conversión de código, es mayor que el número disponible en una página G4 Clase 1. Cada página G4 Clase 1 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página G4 Clase 1. El número de líneas en un TLX deberá calcularse tras la inserción de cuantos pares CR-LF del ATI2 sean necesarios.

La imaginización de caracteres en G4 Clase 1 será conforme con la Recomendación T.351.

3.4.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

3.5 *Conversión de TLX a videotex*

3.5.1 *Conversión de formato*

Un texto TLX se convierte directamente en un videotex si el número de caracteres gráficos de la línea TLX con conversión de código no es mayor que el número de caracteres disponibles en la línea videotex, y si el número de líneas TLX no es mayor que el número de líneas disponibles en la página videotex.

Un par CR-LF del ATI2 invoca una nueva línea videotex. Si no hay un LF asociado con un CR, puede insertarse un LF después del CR.

Una línea de texto TLX deberá convertirse en el número adecuado de líneas videotex (con la posible inserción de un par APD-APR de la Recomendación T.101) si el numero de caracteres gráficos de una línea TLX con conversión de código supera el número de caracteres gráficos disponibles en una línea videotex (N_2). Cada línea videotex dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea videotex. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un texto TLX deberá dividirse en un número adecuado de páginas videotex si el número de líneas TLX con conversión de código es mayor que el número disponible en una página videotex (M_2). Cada página videotex dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página videotex. El número de líneas en un TLX deberá calcularse tras la inserción de cuantos pares APD-APR de la Recomendación T.101 sean necesarios.

Por definición, no se consideran pérdida de información la conversión de una línea TLX en una línea videotex ni la conversión de un texto TLX en una o varias páginas videotex.

3.5.2 *Conversión de código*

La conversión de código se especifica en el anexo A.

3.6 *Conversión de TLX a voz*

Requiere ulterior estudio.

3.7 *Conversión de TLX a modo mixto*

Requiere ulterior estudio.

4 Conversión desde texto AI5

4.1 *Conversión de texto AI5 a TLX*

4.1.1 *Conversión de formato*

Un texto AI5 se convierte directamente en un TLX si el número de caracteres gráficos de la línea de texto AI5 con conversión de código no es mayor que el número de caracteres disponibles en la línea TLX.

Un par CR-LF del AI5 invoca una nueva línea TLX. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea de texto AI5 deberá convertirse en el número adecuado de líneas TLX (con la posible inserción de un par CR-LF del AI5) si el número de caracteres gráficos de una línea TLX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea TLX. Cada línea TLX dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea TLX. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del AI5 se convierte en un par CR-LF del ATI2 más la adición facultativa de hasta 3 líneas en blanco.

4.1.2 *Conversión de código*

Esta regla de conversión se define en el anexo A.

Cuando el texto AI5 cambia de tipo la posición «letras» a la posición «cifras», se genera un cambio a cifras del ATI2. Cuando el texto AI5 cambia de la posición «cifras» a la posición «letras», se genera un cambio a letras del ATI2.

Al comienzo del mensaje, se generará un cambio a letras del ATI2 para garantizar que el TLX está en una posición conocida.

4.2 *Conversión de texto AI5 a TTX*

4.2.1 *Conversión de formato*

Un texto AI5 se convierte directamente en un TTX si el número de caracteres gráficos de la línea de texto AI5 con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea TTX y si el número de líneas del texto AI5 no es mayor que el número de líneas disponibles en una página TTX.

Un par CR-LF del AI5 invoca una nueva línea TTX. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea de texto AI5 deberá convertirse en el número adecuado de líneas TTX (con la posible inserción de un par CR-LF de TTX) si el número de caracteres gráficos de una línea de texto AI5 con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea TTX. Cada línea TTX dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles en una línea TTX. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del AI5 invoca una nueva página TTX.

Una página de texto AI5 deberá dividirse en el número adecuado de páginas TTX (con la posible inserción de un par CR-FF de TTX), si el número de líneas de texto AI5 con conversión de código es mayor que el número de líneas disponibles en una página TTX. Cada página TTX dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página TTX. El número de líneas en un texto AI5 deberá calcularse tras la inserción de cuantos pares CR-LF de TTX sean necesarios.

4.2.2 *Conversión de código*

Cada uno de los caracteres del AI5 se representa mediante siete bits (b_7-b_1). Los caracteres del AI5 se convierten en los correspondientes caracteres de la Recomendación T.61 añadiendo un octavo bit (b_8) de valor 0. La regla de conversión se especifica en el anexo A.

Nota – En el caso de «acento circunflejo», «acento grave» y «tilde», será objeto de estudio ulterior la posibilidad de elegir como códigos convertidos signos diacríticos de la Recomendación T.61.

4.3 *Conversión de texto AI5 a FaxG3*

4.3.1 *Conversión de formato*

Un texto AI5 se convierte directamente en un FaxG3 si el número de caracteres gráficos de la línea de texto AI5 con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres FaxG3 y si el número de líneas del texto AI5 no es mayor que el número de líneas disponibles en una página FaxG3.

Un par CR-LF del AI5 invoca una nueva línea de caracteres FaxG3. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea de texto AI5 deberá convertirse en el número adecuado de líneas de caracteres FaxG3 (con la posible inserción de un par CR-LF del AI5) si el número de caracteres gráficos de una línea de texto AI5 con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres FaxG3. Cada línea de caracteres FaxG3 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres FaxG3. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del AI5 invoca una nueva página FaxG3.

Una página de texto AI5 deberá dividirse en el número adecuado de páginas FaxG3 si el número de líneas de texto AI5 con conversión de código es mayor que el número disponible de líneas en una página FaxG3. Cada página FaxG3 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página FaxG3. El número de líneas de un texto AI5 se deberá calcular tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Al convertir de texto AI5 a FaxG3, el formato de imagen FaxG3 tendrá 80 caracteres por línea, con un margen izquierdo de 20 mm y 55 líneas por página.

La imaginización de caracteres en FaxG3 será conforme con la Recomendación T.351.

4.3.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

4.4 *Conversión de texto AI5 a G4 Clase 1*

4.4.1 *Conversión de formato*

Un texto AI5 se convierte directamente en G4 Clase 1 si el número de caracteres gráficos de la línea de texto AI5 con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1 y si el número de líneas de texto AI5 no es mayor que el número de líneas disponibles en una página G4 Clase 1.

Un par CR-LF del AI5 invoca una nueva línea de caracteres de G4 Clase 1. Si no hay un LF asociado a un CR, se puede insertar un LF después del CR.

Una línea de texto AI5 deberá convertirse en el número adecuado de líneas de caracteres G4 Clase 1 (con la posible inserción de un par CR-LF del AI5) si el número de caracteres gráficos en una línea de texto AI5 con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1. Cada línea de caracteres G4 Clase 1 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres G4 Clase 1. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del AI5 invoca una nueva página G4 Clase 1.

Una página de texto AI5 deberá dividirse en el número adecuado de páginas G4 Clase 1 si el número de líneas de texto AI5 con conversión de código es mayor que el número disponible en una página G4 Clase 1. Cada página G4 Clase 1 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página G4 Clase 1. El número de líneas en un texto AI5 deberá calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Al convertir de texto AI5 a G4 Clase 1, el formato de imagen G4 Clase 1 tendrá 80 caracteres por línea, con un margen izquierdo de 20 mm y 55 líneas por página.

La imaginización de caracteres en G4 Clase 1 será conforme con la Recomendación T.351.

4.4.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

4.5 *Conversión de texto AI5 a videotex*

4.5.1 *Conversión de formato*

Un texto AI5 se convierte directamente en un videotex si el número de caracteres gráficos de la línea de texto AI5 con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea videotex y si el número de líneas en el texto AI5 no es mayor que el número de líneas disponibles en la página videotex.

Un par CR-LF del AI5 invoca una nueva línea videotex. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea de texto AI5 deberá convertirse en el número adecuado de líneas videotex (con la posible inserción de un par APD-APR de la Recomendación T.101) si el número de caracteres gráficos en una línea de texto AI5 con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea videotex. Cada línea de caracteres videotex dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres videotex. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del AI5 invoca una nueva página videotex.

Una página de texto AI5 deberá dividirse en el número adecuado de páginas videotex (con la posible inserción de una CS de la Recomendación T.101) si el número de líneas de texto AI5 con conversión de código es mayor que el número de líneas disponibles en una página videotex. Cada página videotex dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página videotex. El número de líneas en un texto AI5 deberá calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Por definición, no se considera pérdida de información la conversión de una línea de texto AI5 en una línea videotex, ni la conversión de una página de texto AI5 en una o varias páginas videotex comenzando cada página de texto AI5 con una nueva página videotex.

4.5.2 *Conversión de código*

La regla de conversión se especifica en el anexo A.

4.6 *Conversión de texto AI5 a voz*

Requiere ulterior estudio.

4.7 *Conversión de texto AI5 a modo mixto*

Requiere ulterior estudio.

5 Conversión desde TTX

5.1 *Conversión de TTX a TLX*

5.1.1 *Conversión de formato*

Un TTX se convierte directamente en un TLX si el número de caracteres gráficos de la línea TTX con conversión de código no es mayor que el número de caracteres disponibles en la línea TLX.

Un par CR-LF de TTX invoca una línea TLX. Si no hay un LF asociado a un CR, se puede insertar un LF después del CR.

Una TTX deberá convertirse en el número adecuado de líneas TLX (con la posible inserción de un par CR-LF del ATI2) si el número de caracteres gráficos de una línea TLX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea TLX. Cada línea TLX dividida (excepto la última) puede contener el máximo número de caracteres gráficos disponibles para la línea TLX. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF de TTX se convierte en un par CR-LF del ATI2 más la adición facultativa de hasta 3 líneas en blanco.

5.1.2 *Conversión de código*

Esta regla de conversión se define en el anexo A.

Cuando el TTX cambia de la posición «letras» a la de «cifras», se generará un cambio a «cifras» del ATI2. Cuando el TTX cambia de la posición «cifras» a la de «letras» se generará un cambio a «letras» del ATI2.

Al comienzo del mensaje, se generará un cambio a «letras» del ATI2 para garantizar que el TLX está en una posición conocida.

5.2 *Conversión de TTX a texto AI5*

5.2.1 *Conversión de formato*

Un TTX se convierte en texto AI5 adoptando la orientación vertical y un máximo de 77 caracteres por línea (una línea se puede construir colocando 72 caracteres a la derecha del margen izquierdo y 5 caracteres adicionales a la izquierda del margen izquierdo). La información teletex en la orientación horizontal provocará una pérdida de información.

Un TTX se convierte directamente en un texto AI5 si el número de caracteres gráficos de la línea TTX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de texto AI5 y si el número de líneas en el TTX no es mayor que el número de líneas disponibles en una página de texto AI5.

Un par CR-LF de TTX invoca una nueva línea de texto AI5. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea TTX deberá convertirse en el número adecuado de líneas de texto AI5 (con la posible inserción de un par CR-LF de AI5) si el número de caracteres gráficos en una línea TTX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de texto AI5. Cada línea de caracteres de texto AI5 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres de texto AI5. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF del TTX invoca una nueva página de texto AI5.

Una página TTX deberá dividirse en el número adecuado de páginas de texto AI5 si el número de líneas de TTX con conversión de código es mayor que el número de líneas disponibles en una página de texto AI5. Cada página de texto AI5 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página de texto AI5. El número de líneas en un TTX deberá calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

5.2.2 *Conversión de código*

Cada carácter del juego de caracteres de la Recomendación T.61 se convierte en el correspondiente carácter del AI5 suprimiendo el bit b_8. Esta regla de conversión se especifica en el anexo A.

Nota – Otras reglas de conversión para los signos de moneda serán objeto de ulterior estudio.

5.3 *Conversión de TTX a TTX*

Requiere ulterior estudio.

5.4 *Conversión de TTX a FaxG3*

5.4.1 *Conversión de formato*

Un texto TTX se convierte directamente en un FaxG3 si el número de caracteres gráficos de la línea TTX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres FaxG3 y si el número de líneas en el TTX no es mayor que el número de líneas disponibles en una página FaxG3.

Un par CR-LF de TTX invoca una nueva línea de caracteres FaxG3. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea de TTX deberá convertirse en el número adecuado de líneas de caracteres FaxG3 (con la posible inserción de un par CR-LF de TTX), si el número de caracteres gráficos en una línea TTX con conversión de código es mayor que el número de caracteres gráficos disponibles en una línea de caracteres FaxG3. Cada línea de caracteres FaxG3 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres FaxG3. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF de TTX invoca una nueva página FaxG3.

Una página TTX deberá dividirse en el número adecuado de páginas FaxG3 (con la posible inserción de un par CR-FF de TTX) si el número de líneas TTX con conversión de código es mayor que el número de líneas disponibles en una página FaxG3. Cada página FaxG3 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página FaxG3. El número de líneas en un TTX deberá calcularse tras la inserción de cuantos pares CR-LF de TTX hagan falta.

La imaginización de caracteres en FaxG3 será conforme a la Recomendación T.351. No obstante, el empleo de las figuras de la Recomendación T.351 correspondientes a las opciones de TTX requiere ulterior estudio.

5.4.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

5.5 *Conversión de TTX a G4 Clase 1*

5.5.1 *Conversión de formato*

Un texto TTX se convierte directamente en un G4 Clase 1 si el número de caracteres gráficos de la línea TTX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1 y si el número de líneas en el TTX no es mayor que el número de líneas disponibles en una página G4 Clase 1.

Un par CR-LF de TTX invoca una nueva línea de caracteres G4 Clase 1. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea TTX deberá convertirse en el número adecuado de líneas de caracteres G4 Clase 1 (con la posible inserción de un par CR-LF de TTX) si el número de caracteres gráficos en una línea TTX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea de caracteres G4 Clase 1. Cada línea de caracteres G4 Clase 1 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres G4 Clase 1. La terminación de la línea al final de una palabra requiere ulterior estudio.

Un par CR-FF de TTX invoca una nueva página G4 Clase 1.

Una página TTX deberá dividirse en el número adecuado de páginas G4 Clase 1 (con la posible inserción de un par CR-FF de TTX) si el número de líneas TTX con conversión de código es mayor que el número de líneas disponibles en una página G4 Clase 1. Cada página G4 Clase 1 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página G4 Clase 1. El número de líneas en un TTX deberá calcularse tras la inserción de cuantos pares CR-LF de TTX sean necesarios.

La imaginización de caracteres en G4 Clase 1 será conforme a la Recomendación T.351. No obstante, el empleo de las figuras de la Recomendación T.351 correspondientes a las opciones de TTX requiere ulterior estudio.

5.5.2 *Conversión de código*

Esta regla de conversión se define en el anexo A. La reproducción de caracteres es una opción nacional.

5.6 *Conversión de TTX a videotex*

5.6.1 *Conversión de formato*

Un TTX se convierte en un videotex adoptando la orientación vertical y un máximo de 77 caracteres por línea (una línea se puede construir colocando 72 caracteres a la derecha del margen izquierdo y 5 caracteres adicionales a la izquierda del margen izquierdo). La información teletex en la orientación horizontal provocará una pérdida de información.

Nota – Los caracteres de control BS (5 como máximo) al comienzo de una línea TTX desplazan la primera posición de carácter lógico de todas las líneas videotex hacia la izquierda, según el número de BS. Esto permite aumentar la longitud de la línea en 5 caracteres. Ha de añadirse un número apropiado de espacios al comienzo de cada línea videotex, para asegurar que todas las líneas videotex empiecen en la primera posición lógica determinada por la línea que tiene el BS máximo al comienzo de la línea TTX.

Un TTX se convierte directamente en un videotex si el número de caracteres gráficos de la línea TTX con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea videotex y si el número de líneas en el TTX no es mayor que el número de líneas disponibles en una página videotex.

Un par CR-LF de TTX invoca una nueva línea videotex. Si no hay un LF asociado con un CR, se puede insertar un LF después del CR.

Una línea TTX deberá convertirse en el número adecuado de líneas videotex (con la posible inserción de un par APD-APR de la Recomendación T.101) si el número de caracteres gráficos en una línea TTX con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea videotex. Cada línea de caracteres videotex dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de caracteres videotex. La terminación de una línea al final de una palabra requiere ulterior estudio.

Un par CR-FF de TTX invoca una nueva página videotex.

Una página TTX deberá dividirse en el número adecuado de páginas videotex (con la posible inserción de una CS de la Recomendación T.101) si el número de líneas TTX con conversión de código es mayor que el número de líneas disponibles en una página videotex. Cada página videotex dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página videotex. El número de páginas TTX deberá calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Por definición, no se considera pérdida de información la conversión de una línea TTX en una línea videotex, ni la conversión de una página TTX en una o varias páginas videotex, comenzando cada página TTX con una nueva página videotex.

5.6.2 *Conversión de código*

La regla de conversión se especifica en el anexo A.

5.7 *Conversión de TTX a voz*

Requiere ulterior estudio.

5.8 *Conversión de TTX a modo mixto*

5.8.1 *Conversión de formato*

Requiere ulterior estudio.

5.8.2 *Conversión de código*

No es necesaria. En modo mixto se admite la cadena T.61.

6 Conversión desde FaxG3

6.1 *Conversión de FaxG3 a FaxG3*

Requiere ulterior estudio.

6.2 *Conversión de FaxG3 a G4 Clase 1*

Requiere ulterior estudio.

6.3 *Conversión de FaxG3 a modo mixto*

Requiere ulterior estudio.

7 Conversión desde G4 Clase 1

7.1 *Conversión de G4 Clase 1 a FaxG3*

Requiere ulterior estudio.

7.2 *Conversión de G4 Clase 1 a G4 Clase 1*

Requiere ulterior estudio.

7.3 *Conversión de G4 Clase 1 a modo mixto*

Requiere ulterior estudio.

8 Conversión desde videotex

8.1 *Conversión de videotex a TLX*

8.1.1 *Conversión de formato*

Un videotex se convierte directamente en un TLX si el número de caracteres gráficos de la línea videotex con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea TLX.

Un par APD-APR de la Recomendación T.101 invoca una nueva línea TLX. Si no hay un APR asociado con un APD, se puede insertar un APR después del APD.

Una línea videotex deberá convertirse en el número adecuado de líneas TLX (con la posible inserción de un par CR-LF del ATI2) si el número de caracteres gráficos en una línea videotex con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea TLX. Cada línea TLX dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea TLX. La terminación de una línea al final de una palabra requiere ulterior estudio.

Una CS de la Recomendación T.101 se convierte en un par CR-LF del ATI2, con la adición facultativa de hasta 3 líneas en blanco.

8.1.2 *Conversión de código*

La regla de conversión se especifica en el anexo A.

8.2 *Conversión de videotex a texto AI5*

8.2.1 *Conversión de formato*

Un videotex se convierte directamente en un texto AI5 si el número de caracteres gráficos de la línea videotex, con conversión de código no es mayor que el número máximo de caracteres gráficos disponibles en una línea de texto AI5 y si el número de líneas en el videotex no es mayor que el número de líneas disponibles en una página de texto AI5.

Un par APD-APR de la Recomendación T.101 invoca una nueva línea de texto AI5. Si no hay un APR asociado con un APD, se puede insertar un APR después del APD.

Una línea videotex deberá convertirse en el número adecuado de líneas de texto AI5 (con la posible inserción de un par CR-LF del AI5) si el número de caracteres gráficos en una línea videotex con conversión de código es mayor que el número máximo de caracteres gráficos en una línea de texto AI5. Cada línea de texto AI5 dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea de texto AI5. La terminación de una línea al final de una palabra requiere ulterior estudio.

Un CS de la Recomendación T.101 invoca una nueva página de texto AI5 o, alternativamente, 3 líneas en blanco si la siguiente página videotex puede ser reproducida completamente en la misma página de texto AI5.

Una página videotex deberá dividirse en el número adecuado de páginas de texto AI5 (con la posible inserción de un par CR-FF del AI5) si el número de líneas videotex con conversión de código es mayor que el número de líneas disponibles en una página de texto AI5. Cada página de texto AI5 dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página de texto AI5. El número de líneas en un videotex deberá calcularse tras la inserción de cuantos pares CR-LF del AI5 sean necesarios.

Por definición, no se considera pérdida de información la conversión de una línea videotex en una línea de texto AI5, ni la conversión de varias páginas videotex en una página de texto AI5, comenzando cada página de texto AI5 con una nueva página videotex.

8.2.2 *Conversión de código*

La regla de conversión se especifica en el anexo A.

8.3 *Conversión de videotex a TTX*

8.3.1 *Conversión de formato*

Un videotex se convierte directamente en un TTX si el número de caracteres gráficos de la línea videotex con conversión de código no es mayor que el número máximo de líneas disponibles en una página TTX y si el número de líneas en el videotex no es mayor que el número de líneas disponibles en una página TTX.

Un par APD-APR de la Recomendación T.101 invoca una nueva línea TTX. Si no hay un APR asociado a un APD, se puede insertar un APR después del APD.

Una línea videotex deberá convertirse en el número adecuado de líneas TTX (con la posible inserción de un par CR-LF de TTX) si el número de caracteres gráficos en una línea videotex con conversión de código es mayor que el número máximo de caracteres gráficos disponibles en una línea TTX. Cada línea TTX dividida (excepto la última) puede contener el número máximo de caracteres gráficos disponibles para la línea TTX. La terminación de una línea al final de una palabra requiere ulterior estudio.

Un CS de la Recomendación T.101 invoca una nueva página TTX o, alternativamente, 3 líneas en blanco si la siguiente página videotex puede ser representada por completo en la misma página TTX.

Una página videotex deberá dividirse en el número adecuado de páginas TTX (con la posible inserción de un par CR-FF de TTX) si el número de líneas videotex con conversión de código es mayor que el número de líneas disponibles en una página TTX. Cada página TTX dividida (excepto la última) puede contener el número máximo de líneas disponibles para la página TTX. El número de líneas en un videotex deberá calcularse tras la inserción de cuantos pares CR-LF de TTX sean necesarios.

Por definición, no se considera pérdida de información la conversión de una línea videotex en una línea TTX, ni la conversión de varias páginas videotex en una página TTX comenzando cada página TTX, con una nueva página videotex.

8.3.2 *Conversión de código*

La regla de conversión se especifica en el anexo A.

8.4 *Conversión de videotex a FaxG3*

Requiere ulterior estudio.

8.5 *Conversión de videotex A G4 Clase 1*

Requiere ulterior estudio.

8.6 *Conversión de videotex a videotex*

Requiere ulterior estudio.

8.7 *Conversión de videotex a voz*

Requiere ulterior estudio.

8.8 *Conversión de videotex a modo mixto*

Requiere ulterior estudio.

9 Conversión desde voz

9.1 *Conversión de voz a voz*

Requiere ulterior estudio.

10 Conversión desde modo mixto

10.1 *Conversión de modo mixto a TLX*

Requiere ulterior estudio.

10.2 *Conversión de modo mixto a texto AI5*

Requiere ulterior estudio.

10.3 *Conversión de modo mixto a TTX*

Requiere ulterior estudio.

10.4 *Conversión de modo mixto a FaxG3*

Requiere ulterior estudio.

10.5 *Conversión de modo mixto a G4 Clase 1*

Requiere ulterior estudio.

10.6 *Conversión de modo mixto a videotex*

Requiere ulterior estudio.

10.7 *Conversión de modo mixto a voz*

Requiere ulterior estudio.

10.8 *Conversión de modo mixto a modo mixto*

Requiere ulterior estudio.

ANEXO A

(a la Recomendación X.408)

Tablas de conversión de código

A.1 *Introducción*

Este anexo se elaboró con el fin de describir las reglas de conversión de código para la utilización del tratamiento de mensajes de una manera concisa y coherente.

A.2 *Premisas*

A.2.1 *Referencias*

a) cuadros 1/S.18 y 2/S.18 (Reglas)

b) cuadros 1/T.50 al 9/T.50 y 11/T.50 (Símbolo y descripción)

c) figuras 1/T.51 y 2/T.51, cuadros 1/T.51, 2/T.51, 4/T.51 y 5/T.51 (Símbolo y descripción)

d) cuadro C-1/T.60 (Reglas)

e) los § 3.2 y 3.3 de la Recomendación T.61 (Símbolo e identificación)

f) figuras 2/T.61 y 3/T.61, cuadros 1/T.61 y 2/T.61 y figuras B-1/T.61 y C-1/T.61 (Símbolo)

g) Recomendación T.100 (Identificación)

h) Recomendación X.408 (1984) (Reglas)

A.2.2 *Estructura de las tablas*

A.2.2.1 *Introducción*

Las tablas están divididas en DOS columnas:

a) JUEGO DE REFERENCIA

b) JUEGO CONVERTIDO

Un par del JUEGO DE REFERENCIA y una subcolumna en la columna JUEGO CONVERTIDO forman la definición de la regla de conversión de código para el tipo de información codificada referenciado como una salida.

Las tablas se han construido de acuerdo con las premisas que se describen más adelante. La ampliación de las tablas requiere ulterior estudio.

A.2.2.2 *JUEGO DE REFERENCIA*

El JUEGO DE REFERENCIA es una colección de las formas gráficas visibles finales (por ejemplo, impresas o presentadas en una pantalla) de caracteres. Con este juego NO se pretende presentar un nuevo juego de caracteres para su implantación en cualquier otro lugar.

Respecto a los caracteres de control, la visibilidad del carácter podría no constituir un criterio para su inclusión en el JUEGO DE REFERENCIA. Se incluyen todos los controles de que se dispone, para mostrar si la finalidad del carácter de control en cuestión se mantiene tras la conversión.

Nota – Es posible que la utilización de un carácter de control difiera de un tipo a otro. Ello puede dar lugar a que tengamos que ocuparnos primero de las secuencias de escape definidas en ISO 2022, y después de la conversión de caracteres. Esto requiere ulterior estudio.

Esta columna se facilita para el juego de caracteres de referencia. Se trata de un juego conceptual, en el que puede figurar cualquier carácter imaginable. Es completamente independiente de la codificación particular de caracteres individuales. Se indican no obstante 3 excepciones con respecto a los caracteres «acento circunflejo» «acento grave» y «tilde» del AI5, por razones de tipo histórico y técnico.

Se asignan los mismos números de identificación a los símbolos (# y ¤), cuya codificación difiere de un tipo a otro.

Las cuestiones relativas a la autoridad de registro y mantenimiento del JUEGO DE REFERENCIA, se dejan para ulterior estudio.

La columna comprende tres subcolumnas:

a) *Identificación:* Se indican en ella los números de identificación de los caracteres, expresados como múltiplos sucesivos de 10, y también el código de identificación utilizado en la Recomendación T.61, si está disponible. Los números 0 a 999 se asignarán a los caracteres de control, y de 1000 en adelante, a los caracteres gráficos.

b) *Denominación o descripción:* Descripción concisa de los caracteres.

c) *Símbolo:* Símbolo conocido de cada carácter.

A.2.2.3 *Columna «JUEGO CONVERTIDO»*

Esta columna comprende varias subcolumnas. Cada subcolumna define uno o más caracteres correspondientes a ese JUEGO DE REFERENCIA.

Es posible que en la conversión de un tipo a otro, se utilicen algunas partes de la regla de conversión de código. Por ejemplo, en la conversión de télex a teletex, no hace falta utilizar los caracteres de número superior a 2000.

Existen, en principio, cinco columnas, para los siguientes tipos de información codificada:

a) teletex (designado por T.61);

b) texto AI5 (designado por VIRAI5);

c) télex (designado por ATI2);

d) FaxG3 y G4 Clase 1 (designado por facsímil);

e) videotex (designado por videotex).

A.2.3 *Empleo de otras normas*

Para aplicaciones de tratamiento de mensajes, se utilizará la tabla de conversión siempre que sea posible. La tabla de conversión no está destinada a reemplazar a las normas internacionales existentes referentes a las conversiones para aplicaciones distintas de las de tratamiento de mensajes.

La regla fundamental para el empleo de las tablas de conversión es que las conversiones definidas en las mismas se obtienen a partir de las representaciones básicas, en caracteres, de los códigos, tal como aparecen en las normas internacionales pertinentes. Para la presente versión de la Recomendación X.408, pueden utilizarse representaciones alternativas, pero requieren ulterior estudio.

Cuando haya conversiones alternativas definidas en Recomendaciones existentes, la X.408 no deberá limitar las opciones. A continuación se muestran algunos ejemplos de conversiones alternativas:

a) La conversión ATI2 → AI5 definida en la Recomendación S.18 tiene conversiones alternativas tales como:

   El carácter * del AI5, puede convertirse en el carácter ? o en caracteres (?) del ATI2.

b) La conversión ATI2 → T.61 definida en la Recomendación T.60 tiene conversiones alternativas tales como:

   El carácter A del ATI2 puede convertirse en el carácter A o en el carácter a de T.61.

Obsérvese que la conversión de un carácter gráfico a varios caracteres gráficos puede utilizarse donde convenga, como opción nacional.

A.3 *Convenios*

a) Casillas de Símb. y N.° en blanco en las columnas de «JUEGO CONVERTIDO», significan que no se proporciona esa conversión (es decir, NO convertible).

b) UE significa «ulterior estudio».

c) Desc. significa «DESCARTADO».

d) No debe interpretarse que los símbolos de los caracteres de control imprimen los símbolos literalmente. Se hacen figurar sólo como información de referencia. La finalidad es que debe mantenerse la semántica de esos caracteres, definidos en otras partes. Véase el § A.2.2.2.

A.4 *Notas*

ⓐ Este carácter se utiliza únicamente para accionar el transmisor automático de indicativo del equipo correspondiente en el servicio público internacional.

ⓑ Estos caracteres no se atribuyen en el plano internacional.

ⓒ Estos caracteres no tienen función correspondiente en otros tipos de información codificada. El equipo de conversión acciona los caracteres apropiados de cambio y descarte.

ⓓ La clasificación de las funciones de control con números inferiores a 1000 requiere ulterior estudio.

CUADRO A-1/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
0		Nulo	NUL	desc.		NUL	0	?	1310	desc.		NUL	0
10		Comienzo de encabezamiento	SOH	desc.		SOH	10	?	1310	desc.		desc.	
20		Comienzo de texto	STX	desc.		STX	20	?	1310	desc.		desc.	
30		Fin de texto	ETX	desc.		ETX	30	?	1310	desc.		desc.	
40		Fin de transmisión	EOT	desc.		EOT	40	?	1310	desc.		desc.	
50		Pregunta	ENQ	desc.		ENQ	50	WRU ⓐ	600	desc.		ENQ	50
60		Acuse de recibo	ACK	desc.		ACK	60	?	1310	desc.		desc.	
70		Timbre	BEL	desc.		BEL	70	BEL	70	desc.		desc.	
80	CF10	Retroceso de un espacio	BS	BS	80	BS	80	?	1310	BS	80	APB	800
90		Tabulación horizontal	HT	desc.		HT	90	?	1310	desc.		desc.	
100	CF12	Cambio de renglón	LF	LF	100	LF	100	LF	100	LF	100	APD	820
110		Tabulación vertical	VT	desc.		VT	110	?	1310	desc.		desc.	
120	CF14	Página siguiente	FF	CR,FF	130,120	FF	120	CR,LF	130,100	CR,FF	130,120	CS	840
130	CF15	Retroceso del carro	CR	CR	130	CR	130	CR	130	CR	130	APR	850
140		Fuera de código	SO	desc.		SO	140	?	1310	desc.		UE	
150		En código	SI	desc.		SI	150	?	1310	desc.		UE	
160		Escape de enlace de datos	DLE	desc.		DLE	160	?	1310	desc.		desc.	
170		Control de dispositivo uno	DC1	desc.		DC1	170	?	1310	desc.		desc.	
180		Control de dispositivo dos	DC2	desc.		DC2	180	?	1310	desc.		desc.	
190		Control de dispositivo tres	DC3	desc.		DC3	190	?	1310	desc.		desc.	

CUADRO A-2/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
200		Control de dispositivo cuatro	DC4	desc.		DC4	200	?	1310	desc.		desc.	
210		Acuse de recibo negativo	NAK	desc.		NAK	210	?	1310	desc.		desc.	
220		Síncrono en reposo	SYN	desc.		SYN	220	?	1310	desc.		desc.	
230		Fin de bloque de texto	ETB	desc.		ETB	230	?	1310	desc.		desc.	
240		Anulación	CAN	desc.		CAN	240	?	1310	desc.		CAN	240
250		Fin del medio físico	EM	desc.		EM	250	?	1310	desc.		desc.	
260	CM02	Carácter de sustitución	SUB	SUB	260	SUB	260	?	1310	UE		UE	
270	CE03	Escape	ESC	ESC	270	ESC	270	?	1310	UE		UE	
280		Separador de información cuatro	IS4	desc.		IS4	280	?	1310	desc.		desc.	
290		Separador de información tres	IS3	desc.		IS3	290	?	1310	desc.		desc.	
300		Separador de información dos	IS2	desc.		IS2	300	?	1310	desc.		desc.	
310		Separador de información uno	IS1	desc.		IS1	310	?	1310	desc.		desc.	
320													
330													
340													
350													
360													
370													
380													
390													

CUADRO A-3/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
400	CE07	Cambio con enclavamiento cero	LS0	LS0	400	UE		UE		UE		UE	
410	CE08	Cambio con enclavamiento uno	LS1	LS1	410	UE		UE		UE		UE	
420	CE09	Cambio con enclavamiento uno derecho	LS1R	LS1R	420	UE		UE		UE		UE	
430	CE10	Cambio con enclavamiento dos	LS2	LS2	430	UE		UE		UE		UE	
440	CE11	Cambio con enclavamiento dos derecho	LS2R	LS2R	440	UE		UE		UE		UE	
450	CE12	Cambio con enclavamiento tres	LS3	LS3	450	UE		UE		UE		UE	
460	CE13	Cambio con enclavamiento tres derecho	LS3R	LS3R	460	UE		UE		UE		UE	
470													
480													
490													
500													
510													
520	CE04	Cambio individual dos	SS2	SS2	520	UE		UE		UE		UE	
530	CE05	Cambio individual tres	SS3	SS3	530	UE		UE		UE		UE	
540													
550													
560													
570													
580													
590													

CUADRO A-4/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
600		¿CON QUIÉN COMUNICO? ⓐ	WRU	desc.		desc.		WRU	600	desc.		desc.	
610		Uso nacional ⓑ		desc.		desc.				desc.		desc.	
620		Uso nacional ⓑ		desc.		desc.				desc.		desc.	
630		Uso nacional ⓑ		desc.		desc.				desc.		desc.	
640													
650		Cambio a letras ⓒ	LS	desc.		desc.		LS	650	desc.		desc.	
660		Cambio a cifras ⓒ	FS	desc.		desc.		UE	660	desc.		desc.	
670		Todos espacios: Nulo	NU	desc.		desc.		NU	670	desc.		desc.	
680													
690	CF16	Descenso parcial de renglón	PLD	PLD	690	desc.		desc.		desc.		desc.	
700	CF17	Ascenso parcial de renglón	PLU	PLU	700	desc.		desc.		desc.		desc.	
710	CP06	Introductor de secuencia de control	CSI	CSI	710	UE		desc.		desc.		UE	
720	CF20	Cambio de renglón inverso	RLF	RLF	720	desc.		desc.		desc.		desc.	
730	CP01	Selección de formato de página	PFS	PFS	730	desc.		desc.		desc.		desc.	
740	CP03	Selección de reproducción gráfica	SGR	SGR	740	desc.		desc.		desc.		desc.	
750	CP04	Selección del espaciamiento horizontal	SHS	SHS	750	desc.		desc.		desc.		desc.	
760	CP05	Selección del espaciamiento vertical	SVS	SVS	760	desc.		desc.		desc.		desc.	
770	CP06	Selección del sentido de presentación	SPD	SPD	770	desc.		desc.		desc.		desc.	
780	CP07	Modificación de tamaño gráfico	GSM	GSM	780	desc.		desc.		desc.		desc.	
790	CM04	Identificación de subrepertorio gráfico	IGS	IGS	790	desc.		desc.		desc.		desc.	

ARCHIVES U.I.T. GENÈVE

CUADRO A-5/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
800		Retroceso de la posición activa	APB	BS	80	BS	80	?	1310	UE		APB	800
810		Avance de la posición activa	APF	UE		UE		?	1310	UE		APF	810
820		Descenso de la posición activa	APD	LF	100	LF	100	LF	100	UE		APD	820
830		Ascenso de la posición activa	APU	UE		UE		?	1310	UE		APU	830
840		Borrado de la pantalla	CS	FF	120	FF	120	CR,LF	130,100	UE		CS	840
850		Retorno de la posición activa (al comienzo de línea)	APR	CR	130	CR	130	CR	130	UE		APR	850
860													
870													
880													
890													
900													
910													
920													
930													
940													
950													
960													
970													
980													
990													

CUADRO A-6/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción ⓓ	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
1000	SP01	Espacio	SP	SP	1000	SP	1000	SP	1000	SP	1000	SP	1000
1010	SP02	Signo de admiración (final)	!	!	1010	!	1010	?	1310	!	1010	!	1010
1020	SP04	Comillas	"	"	1020	"	1020	?	1310	"	1020	"	1020
1030													
1040													
1050	SM02	Signo de tanto por ciento	%	%	1050	%	1050	?	1310	%	1050	%	1050
1060	SM03	Y comercial	&	&	1060	&	1060	?	1310	&	1060	&	1060
1070	SP05	Apóstrofo	'	'	1070	'	1070	'	1070	'	1070	'	1070
1080	SP06	Paréntesis izquierdo	(	(	1080	(	1080	(	1080	(	1080	(	1080
1090	SP07	Paréntesis derecho	)	)	1090	)	1090	)	1090	)	1090	)	1090
1100	SM04	Asterisco	*	*	1100	*	1100	?	1310	*	1100	*	1100
1110	SA01	Signo más	+	+	1110	+	1110	+	1110	+	1110	+	1110
1120	SP08	Coma	,	,	1120	,	1120	,	1120	,	1120	,	1120
1130	SP10	Guión o signo menos	–	–	1130	–	1130	–	1130	–	1130	–	1130
1140	SP11	Punto	.	.	1140	.	1140	.	1140	.	1140	.	1140
1150	SP12	Barra oblicua	/	/	1150	/	1150	/	1150	/	1150	/	1150
1160	ND10	Cifra 0	0	0	1160	0	1160	0	1160	0	1160	0	1160
1170	ND01	Cifra 1	1	1	1170	1	1170	1	1170	1	1170	1	1170
1180	ND02	Cifra 2	2	2	1180	2	1180	2	1180	2	1180	2	1180
1190	ND03	Cifra 3	3	3	1190	3	1190	3	1190	3	1190	3	1190

CUADRO A-7/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
1200	ND04	Cifra 4	4	4	1200	4	1200	4	1200	4	1200	4	1200
1210	ND05	Cifra 5	5	5	1210	5	1210	5	1210	5	1210	5	1210
1220	ND06	Cifra 6	6	6	1220	6	1220	6	1220	6	1220	6	1220
1230	ND07	Cifra 7	7	7	1230	7	1230	7	1230	7	1230	7	1230
1240	ND08	Cifra 8	8	8	1240	8	1240	8	1240	8	1240	8	1240
1250	ND09	Cifra 9	9	9	1250	9	1250	9	1250	9	1250	9	1250
1260	SP13	Dos puntos	:	:	1260	:	1260	:	1260	:	1260	:	1260
1270	SP14	Punto y coma	;	;	1270	;	1270	?	1310	;	1270	;	1270
1280	SA03	Signo menor que	<	<	1280	<	1280	?	1310	<	1280	<	1280
1290	SA04	Signo igual	=	=	1290	=	1290	=	1290	=	1290	=	1290
1300	SA05	Signo mayor que	>	>	1300	>	1300	?	1310	>	1300	>	1300
1310	SP15	Signo de interrogación	?	?	1310	?	1310	?	1310	?	1310	?	1310
1320	SM05	a comercial	@	@	1320	@	1320	?	1310	@	1320	@	1320
1330	LA02	A mayúscula	A	A	1330	A	1330	A	1330	A	1330	A	1330
1340	LB02	B mayúscula	B	B	1340	B	1340	B	1340	B	1340	B	1340
1350	LC02	C mayúscula	C	C	1350	C	1350	C	1350	C	1350	C	1350
1360	LD02	D mayúscula	D	D	1360	D	1360	D	1360	D	1360	D	1360
1370	LE02	E mayúscula	E	E	1370	E	1370	E	1370	E	1370	E	1370
1380	LF02	F mayúscula	F	F	1380	F	1380	F	1380	F	1380	F	1380
1390	LG02	G mayúscula	G	G	1390	G	1390	G	1390	G	1390	G	1390

CUADRO A-8/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
1400	LH02	H mayúscula	H	H	1400	H	1400	H	1400	H	1400	H	1400
1410	LI02	I mayúscula	I	I	1410	I	1410	I	1410	I	1410	I	1410
1420	LJ02	J mayúscula	J	J	1420	J	1420	J	1420	J	1420	J	1420
1430	LK02	K mayúscula	K	K	1430	K	1430	K	1430	K	1430	K	1430
1440	LL02	L mayúscula	L	L	1440	L	1440	L	1440	L	1440	L	1440
1450	LM02	M mayúscula	M	M	1450	M	1450	M	1450	M	1450	M	1450
1460	LN02	N mayúscula	N	N	1460	N	1460	N	1460	N	1460	N	1460
1470	LO02	O mayúscula	O	O	1470	O	1470	O	1470	O	1470	O	1470
1480	LP02	P mayúscula	P	P	1480	P	1480	P	1480	P	1480	P	1480
1490	LQ02	Q mayúscula	Q	Q	1490	Q	1490	Q	1490	Q	1490	Q	1490
1500	LR02	R mayúscula	R	R	1500	R	1500	R	1500	R	1500	R	1500
1510	LS02	S mayúscula	S	S	1510	S	1510	S	1510	S	1510	S	1510
1520	LT02	T mayúscula	T	T	1520	T	1520	T	1520	T	1520	T	1520
1530	LU02	U mayúscula	U	U	1530	U	1530	U	1530	U	1530	U	1530
1540	LV02	V mayúscula	V	V	1540	V	1540	V	1540	V	1540	V	1540
1550	LW02	W mayúscula	W	W	1550	W	1550	W	1550	W	1550	W	1550
1560	LX02	X mayúscula	X	X	1560	X	1560	X	1560	X	1560	X	1560
1570	LY02	Y mayúscula	Y	Y	1570	Y	1570	Y	1570	Y	1570	Y	1570
1580	LZ02	Z mayúscula	Z	Z	1580	Z	1580	Z	1580	Z	1580	Z	1580
1590	SM06	Corchete izquierdo	[	[	1590	[	1590	?	1310	[	1590	[	1590

CUADRO A-9/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
1600		Barra oblicua inversa	\	?	1310	\	1600	?	1310	\	1600	?	1310
1610	SM08	Corchete derecho	]	]	1610	]	1610	?	1310	]	1610	]	1610
1620		Acento circunflejo (AI N.° 5)	^	UE		^	1620	?	1310	^	1620	UE	
1630	SP09	Línea baja (o de subrayado)	_	_	1630	_	1630	?	1310	_	1630	_	1630
1640		Acento grave (AI N.° 5)	`	UE		`	1640	?	1310	`	1640	UE	
1650	LA01	a minúscula	a	a	1650	a	1650	A	1330	a	1650	a	1650
1660	LB01	b minúscula	b	b	1660	b	1660	B	1340	b	1660	b	1660
1670	LC01	c minúscula	c	c	1670	c	1670	C	1350	c	1670	c	1670
1680	LD01	d minúscula	d	d	1680	d	1680	D	1360	d	1680	d	1680
1690	LE01	e minúscula	e	e	1690	e	1690	E	1370	e	1690	e	1690
1700	LF01	f minúscula	f	f	1700	f	1700	F	1380	f	1700	f	1700
1710	LG01	g minúscula	g	g	1710	g	1710	G	1390	g	1710	g	1710
1720	LH01	h minúscula	h	h	1720	h	1720	H	1400	h	1720	h	1720
1730	LI01	i minúscula	i	i	1730	i	1730	I	1410	i	1730	i	1730
1740	LJ01	j minúscula	j	j	1740	j	1740	J	1420	j	1740	j	1740
1750	LK01	k minúscula	k	k	1750	k	1750	K	1430	k	1750	k	1750
1760	LL01	l minúscula	l	l	1760	l	1760	L	1440	l	1760	l	1760
1770	LM01	m minúscula	m	m	1770	m	1770	M	1450	m	1770	m	1770
1780	LN01	n minúscula	n	n	1780	n	1780	N	1460	n	1780	n	1780
1790	LO01	o minúscula	o	o	1790	o	1790	O	1470	o	1790	o	1790

CUADRO A-10/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
1800	LP01	p minúscula	p	p	1800	p	1800	P	1480	p	1800	p	1800
1810	LQ01	q minúscula	q	q	1810	q	1810	Q	1490	q	1810	q	1810
1820	LR01	r minúscula	r	r	1820	r	1820	R	1500	r	1820	r	1820
1830	LS01	s minúscula	s	s	1830	s	1830	S	1510	s	1830	s	1830
1840	LT01	t minúscula	t	t	1840	t	1840	T	1520	t	1840	t	1840
1850	LU01	u minúscula	u	u	1850	u	1850	U	1530	u	1850	u	1850
1860	LV01	v minúscula	v	v	1860	v	1860	V	1540	v	1860	v	1860
1870	LW01	w minúscula	w	w	1870	w	1870	W	1550	w	1870	w	1870
1880	LX01	x minúscula	x	x	1880	x	1880	X	1560	x	1880	x	1880
1890	LY01	y minúscula	y	y	1890	y	1890	Y	1570	y	1890	y	1890
1900	LZ01	z minúscula	z	z	1900	z	1900	Z	1580	z	1900	z	1900
1910		Llave izquierda	{	<	1280	{	1910	?	1310	{	1910	<	1280
1920	SM13	Barra vertical	|	|	1920	|	1920	?	1310	|	1920	|	1920
1930		Llave derecha	}	>	1300	}	1930	?	1310	}	1930	>	1300
1940		Línea alta AI N.° 5	¯	UE		¯	1940	?	1310	¯	1940	UE	
1950		Supresión	DEL	desc.		DEL	1950	desc.		DEL	1950	desc.	
1960													
1970													
1980													
1990													

CUADRO A-11/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
2000													
2010	SP03	Signo de admiración (inicial)	¡	¡	2010	?	1310	?	1310	¡	2010	¡	2010
2020	SC04	Signo de centavo	¢	¢	2020	¤	2080	?	1310	¢	2020	¢	2020
2030	SC02	Signo de libra	£	£	2030	¤	2080	?	1310	£	2030	£	2030
2040	SC03	Signo de dólar	$	$	2040	¤	2080	?	1310	$	2040	$	2040
2050	SC05	Signo de yen	¥	¥	2050	¤	2080	?	1310	¥	2050	¥	2050
2060	SM01	Signo de número	#	#	2060	#	2060	?	1310	#	2060	#	2060
2070	SM24	Signo de párrafo	§	§	2070	?	1310	?	1310	§	2070	§	2070
2080	SC01	Signo de moneda	¤	¤	2080	¤	2080	?	1310	¤	2080	¤	2080
2090	SP19	Comilla individual izquierda	‘	′	1070	′	1070	′	1070	′	1070	′	1070
2100	SP21	Doble comilla izquierda	“	″	1020	″	1020	?	1310	″	1020	″	1020
2110	SP17	Comillas angulares izquierdas	«	«	2110	<	1280	?	1310	«	2110	«	2110
2120	SM30	Flecha hacia la izquierda	←	?	1310	?	1310	?	1310	?	1310	?	1310
2130	SM32	Flecha hacia arriba	↑	?	1310	?	1310	?	1310	?	1310	?	1310
2140	SM31	Flecha hacia la derecha	→	?	1310	?	1310	?	1310	?	1310	?	1310
2150	SM33	Flecha hacia abajo	↓	?	1310	?	1310	?	1310	?	1310	?	1310
2160	SM19	Signo de grado	°	°	2160	?	1310	?	1310	°	2160	°	2160
2170	SA02	Signo más/menos	±	±	2170	?	1310	?	1310	±	2170	±	2170
2180	NS02	Superíndice 2	$\square^2$	$\square^2$	2180	?	1310	?	1310	$\square^2$	2180	$\square^2$	2180
2190	NS03	Superíndice 3	$\square^3$	$\square^3$	2190	?	1310	?	1310	$\square^3$	2190	$\square^3$	2190

CUADRO A-12/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
2200	SA07	Signo de multiplicación	×	×	2200	?	1310	?	1310	×	2200	×	2200
2210	SM17	Signo de micro	µ	µ	2210	?	1310	?	1310	µ	2210	µ	2210
2220	SM25	Signo de calderón	¶	¶	2220	?	1310	?	1310	¶	2220	¶	2220
2230	SM26	Punto central	·	·	2230	?	1310	?	1310	·	2230	·	2230
2240	SA06	Signo de división	÷	÷	2240	?	1310	?	1310	÷	2240	÷	2240
2250	SP20	Comilla individual derecha	'	'	1070	'	1070	'	1070	'	1070	'	1070
2260	SP22	Doble comilla derecha	"	"	1020	"	1020	?	1310	"	1020	"	1020
2270	SP18	Comillas angulares derechas	»	»	2270	>	1300	?	1310	»	2270	»	2270
2280	NF04	Fracción un quarto	¼	¼	2280	?	1310	?	1310	¼	2280	¼	2280
2290	NF01	Fracción un medio	½	½	2290	?	1310	?	1310	½	2290	½	2290
2300	NF05	Fracción tres cuartos	¾	¾	2300	?	1310	?	1310	¾	2300	¾	2300
2310	SP16	Signo de interrogación (inicial)	¿	¿	2310	?	1310	?	1310	¿	2310	¿	2310
2320													
2330	SD13	Acento grave	`	`	2330	?	1310	?	1310	`	2330	`	2330
2340	SD11	Acento agudo	´	´	2340	?	1310	?	1310	´	2340	´	2340
2350	SD15	Acento circunflejo	^	^	2350	?	1310	?	1310	^	2350	^	2350
2360	SD19	Tilde	~	~	2360	?	1310	?	1310	~	2360	~	2360
2370	SD31	Signo de vocal larga (macrón)	-	-	2370	?	1310	?	1310	-	2370	-	2370
2380	SD23	Signo de vocal breve	˘	˘	2380	?	1310	?	1310	˘	2380	˘	2380
2390	SD29	Punto	.	.	2390	?	1310	?	1310	.	2390	.	2390

CUADRO A-13/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
2400	SD17	Diéresis o signo de umlaut	¨	¨	2400	?	1310	?	1310	¨	2400	¨	2400
2410													
2420	SD27	Cero volado (o acento sueco)	°	°	2420	?	1310	?	1310	°	2420	°	2420
2430	SD41	Cedilla	¸	¸	2430	?	1310	?	1310	¸	2430	¸	2430
2440													
2450	SD25	Doble acento agudo	˝	˝	2450	?	1310	?	1310	˝	2450	˝	2450
2460	SD43	Ogonek	˛	˛	2460	?	1310	?	1310	˛	2460	˛	2460
2470	SD21	Caron	ˇ	ˇ	2470	?	1310	?	1310	ˇ	2470	ˇ	2470
2480	SM12	Barra horizontal	–	?	1310	?	1310	?	1310	–	2480	–	2480
2490		Superíndice 1	□[1]	?	1310	?	1310	?	1310	□[1]	2490	□[1]	2490
2500		Signo registrado	®	?	1310	?	1310	?	1310	®	2500	®	2500
2510		Signo de derechos de autor	©	?	1310	?	1310	?	1310	©	2510	©	2510
2520		Signo de marca registrada	TM	?	1310	?	1310	?	1310	TM	2520	TM	2520
2530		Nota musical	♪	?	1310	?	1310	?	1310	♪	2530	♪	2530
2540													
2550													
2560													
2570													
2580													
2590													

CUADRO A-14/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
2600		Fracción un octavo	1/8	?	1310	?	1310	?	1310	1/8	2600	1/8	2600
2610		Fracción tres octavos	3/8	?	1310	?	1310	?	1310	3/8	2610	3/8	2610
2620		Fracción cinco octavos	5/8	?	1310	?	1310	?	1310	5/8	2620	5/8	2620
2630		Fracción siete octavos	7/8	?	1310	?	1310	?	1310	7/8	2630	7/8	2630
2640	SM18	Signo de ohmio	Ω	Ω	2640	?	1310	?	1310	Ω	2640	Ω	2640
2650	LA52	Diptongo Æ en mayúscula	Æ	Æ	2650	?	1310	?	1310	Æ	2650	Æ	2650
2660	LD62	D con trazo	Đ	Đ	2660	?	1310	?	1310	Đ	2660	Đ	2660
2670	SM21	Indicador ordinal, femenino	a	a	2670	?	1310	?	1310	a	2670	a	2670
2680	LH62	H mayúscula con trazo	Ħ	Ħ	2680	?	1310	?	1310	Ħ	2680	Ħ	2680
2690													
2700	LI52	Ligadura IJ en mayúscula	IJ	IJ	2700	?	1310	?	1310	IJ	2700	IJ	2700
2710	LL64	L mayúscula con punto central	Ŀ	Ŀ	2710	?	1310	?	1310	Ŀ	2710	Ŀ	2710
2720	LL62	L mayúscula con barra	Ł	Ł	2720	?	1310	?	1310	Ł	2720	Ł	2720
2730	LO62	O mayúscula con barra	Ø	Ø	2730	?	1310	?	1310	Ø	2730	Ø	2730
2740	LO52	Ligadura Œ mayúscula	Œ	Œ	2740	?	1310	?	1310	Œ	2740	Œ	2740
2750	SM20	Indicador ordinal, masculino	o	o	2750	?	1310	?	1310	o	2750	o	2750
2760	LT64	Thorn mayúscula, islandesa	Þ	Þ	2760	?	1310	?	1310	Þ	2760	Þ	2760
2770	LT62	T mayúscula con trazo	Ŧ	Ŧ	2770	?	1310	?	1310	Ŧ	2770	Ŧ	2770
2780	LN62	Eng mayúscula, lapona	ŋ	ŋ	2780	?	1310	?	1310	ŋ	2780	ŋ	2780
2790	LN63	n minúscula con apóstrofo	ŉ	ŉ	2790	?	1310	?	1310	ŉ	2790	ŉ	2790

CUADRO A-15/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
2800	LK61	k minúscula, groenlandesa	ĸ	ĸ	2800	?	1310	?	1310	ĸ	2800	ĸ	2800
2810	LA51	Diptongo æ en minúscula	æ	æ	2810	?	1310	?	1310	æ	2810	æ	2810
2820	LD61	d minúscula con trazo	đ	đ	2820	?	1310	?	1310	đ	2820	đ	2820
2830	LD63	eth islandesa, minúscula	ð	ð	2830	?	1310	?	1310	ð	2830	ð	2830
2840	LH61	h minúscula con trazo	ħ	ħ	2840	?	1310	?	1310	ħ	2840	ħ	2840
2850	LI61	i minúscula sin punto	ı	ı	2850	?	1310	?	1310	ı	2850	ı	2850
2860	LI51	Ligadura ij en minúscula	ij	ij	2860	?	1310	?	1310	ij	2860	ij	2860
2870	LL63	l minúscula con punto central	l·	l·	2870	?	1310	?	1310	l·	2870	l·	2870
2880	LL61	l minúscula con trazo	ł	ł	2880	?	1310	?	1310	ł	2880	ł	2880
2890	LO61	o minúscula con barra	ø	ø	2890	?	1310	?	1310	ø	2890	ø	2890
2900	LO51	Ligadura œ en minúscula	œ	œ	2900	?	1310	?	1310	œ	2900	œ	2900
2910	LS61	Doble s alemana, minúscula	β	β	2910	?	1310	?	1310	β	2910	β	2910
2920	LT63	Thorn minúscula, islandesa	þ	þ	2920	?	1310	?	1310	þ	2920	þ	2920
2930	LT61	t minúscula con trazo	ŧ	ŧ	2930	?	1310	?	1310	ŧ	2930	ŧ	2930
2940	LN61	Eng minúscula, lapona	ŋ	ŋ	2940	?	1310	?	1310	ŋ	2940	ŋ	2940
2950													
2960													
2970													
2980													
2990													

CUADRO A-16/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
3000	LA11	a minúscula con acento agudo	á	á	3000	a	1650	A	1330	á	3000	á	3000
3010	LA12	A mayúscula con acento agudo	Á	Á	3010	A	1330	A	1330	Á	3010	Á	3010
3020	LA13	a minúscula con acento grave	à	à	3020	a	1650	A	1330	à	3020	à	3020
3030	LA14	A mayúscula con acento grave	À	À	3030	A	1330	A	1330	À	3030	À	3030
3040	LA15	a minúscula con acento circunflejo	â	â	3040	a	1650	A	1330	â	3040	â	3040
3050	LA16	A mayúscula con acento circunflejo	Â	Â	3050	A	1330	A	1330	Â	3050	Â	3050
3060	LA17	a minúscula con diéresis o signo de umlaut	ä	ä	3060	a	1650	A	1330	ä	3060	ä	3060
3070	LA18	A mayúscula con diéresis o signo de umlaut	Ä	Ä	3070	A	1330	A	1330	Ä	3070	Ä	3070
3080	LA19	a minúscula con tilde	ã	ã	3080	a	1650	A	1330	ã	3080	ã	3080
3090	LA20	A mayúscula con tilde	Ã	Ã	3090	A	1330	A	1330	Ã	3090	Ã	3090
3100	LA23	a minúscula con signo de vocal breve	ă	ă	3100	a	1650	A	1330	ă	3100	ă	3100
3110	LA24	A mayúscula con signo de vocal breve	Ă	Ă	3110	A	1330	A	1330	Ă	3110	Ă	3110
3120	LA27	a minúscula con cero volado (o acento sueco)	å	å	3120	a	1650	A	1330	å	3120	å	3120
3130	LA28	A mayúscula con cero volado (o acento sueco)	Å	Å	3130	A	1330	A	1330	Å	3130	Å	3130
3140	LA31	a minúscula con signo de vocal larga (macrón)	ā	ā	3140	a	1650	A	1330	ā	3140	ā	3140
3150	LA32	A mayúscula con signo de vocal larga (macrón)	Ā	Ā	3150	A	1330	A	1330	Ā	3150	Ā	3150
3160	LA43	a minúscula con ogonek	ą	ą	3160	a	1650	A	1330	ą	3160	ą	3160
3170	LA44	A mayúscula con ogonek	Ą	Ą	3170	A	1330	A	1330	Ą	3170	Ą	3170
3180	LC11	c minúscula con acento agudo	ć	ć	3180	c	1670	C	1350	ć	3180	ć	3180
3190	LC12	C mayúscula con acento agudo	Ć	Ć	3190	C	1350	C	1350	Ć	3190	Ć	3190

CUADRO A-17/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
3200	LC15	c minúscula con acento circunflejo	ĉ	ĉ	3200	c	1670	C	1350	ĉ	3200	ĉ	3200
3210	LC16	C mayúscula con acento circunflejo	Ĉ	Ĉ	3210	C	1350	C	1350	Ĉ	3210	Ĉ	3210
3220	LC21	c minúscula con caron	č	č	3220	c	1670	C	1350	č	3220	č	3220
3230	LC22	C mayúscula con caron	Č	Č	3230	C	1350	C	1350	Č	3230	Č	3230
3240	LC29	c minúscula con punto superior	ċ	ċ	3240	c	1670	C	1350	ċ	3240	ċ	3240
3250	LC30	C mayúscula con punto superior	Ċ	Ċ	3250	C	1350	C	1350	Ċ	3250	Ċ	3250
3260	LC41	c minúscula con cedilla	ç	ç	3260	c	1670	C	1350	ç	3260	ç	3260
3270	LC42	C mayúscula con cedilla	Ç	Ç	3270	C	1350	C	1350	Ç	3270	Ç	3270
3280	LD21	d minúscula con caron	ď	ď	3280	d	1680	D	1360	ď	3280	ď	3280
3290	LD22	D mayúscula con caron	Ď	Ď	3290	D	1360	D	1360	Ď	3290	Ď	3290
3300	LE11	e minúscula con acento agudo	é	é	3300	e	1690	E	1370	é	3300	é	3300
3310	LE12	E mayúscula con acento agudo	É	É	3310	E	1370	E	1370	É	3310	Ê	3310
3320	LE13	e minúscula con acento grave	è	è	3320	e	1690	E	1370	è	3320	è	3320
3330	LE14	E mayúscula con acento grave	È	È	3330	E	1370	E	1370	È	3330	È	3330
3340	LE15	e minúscula con acento circunflejo	ê	ê	3340	e	1690	E	1370	ê	3340	ê	3340
3350	LE16	E mayúscula con acento circunflejo	Ê	Ê	3350	E	1370	E	1370	Ê	3350	Ê	3350
3360	LE17	e minúscula con diéresis o signo de umlaut	ë	ë	3360	e	1690	E	1370	ë	3360	ë	3360
3370	LE18	E mayúscula con diéresis o signo de umlaut	Ë	Ë	3370	E	1370	E	1370	Ë	3370	Ë	3370
3380	LE21	e minúscula con caron	ě	ě	3380	e	1690	E	1370	ě	3380	ě	3380
3390	LE22	E mayúscula con caron	Ě	Ě	3390	E	1370	E	1370	Ě	3390	Ě	3390

CUADRO A-18/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
3400	LE29	e minúscula con punto superior	ė	ė	3400	e	1690	E	1370	ė	3400	ė	3400
3410	LE30	E mayúscula con punto superior	Ė	Ė	3410	E	1370	E	1370	Ė	3410	Ė	3410
3420	LE31	e minúscula con signo de vocal larga (macrón)	ē	ē	3420	e	1690	E	1370	ē	3420	ē	3420
3430	LE32	E mayúscula con signo de vocal larga (macrón)	Ē	Ē	3430	E	1370	E	1370	Ē	3430	Ē	3430
3440	LE43	e minúscula con ogonek	ę	ę	3440	e	1690	E	1370	ę	3440	ę	3440
3450	LE44	E mayúscula con ogonek	Ę	Ę	3450	E	1370	E	1370	Ę	3450	Ę	3450
3460	LG11	g minúscula con acento agudo	ǵ	ǵ	3460	g	1710	G	1390	ǵ	3460	ǵ	3460
3470	LG15	g minúscula con acento circunflejo	ĝ	ĝ	3470	g	1710	G	1390	ĝ	3470	ĝ	3470
3480	LG16	G mayúscula con acento circunflejo	Ĝ	Ĝ	3480	G	1390	G	1390	Ĝ	3480	Ĝ	3480
3490	LG23	g minúscula con signo de vocal breve	ğ	ğ	3490	g	1710	G	1390	ğ	3490	ğ	3490
3500	LG24	G mayúscula con signo de vocal breve	Ğ	Ğ	3500	G	1390	G	1390	Ğ	3500	Ğ	3500
3510	LG29	g minúscula con punto superior	ġ	ġ	3510	g	1710	G	1390	ġ	3510	ġ	3510
3520	LG30	G mayúscula con punto superior	Ġ	Ġ	3520	G	1390	G	1390	Ġ	3520	Ġ	3520
3530	LG42	G mayúscula con cedilla	Ģ	Ģ	3530	G	1390	G	1390	Ģ	3530	Ģ	3530
3540	LH15	h minúscula con acento circunflejo	ĥ	ĥ	3540	h	1720	H	1400	ĥ	3540	ĥ	3540
3550	LH16	H mayúscula con acento circunflejo	Ĥ	Ĥ	3550	H	1400	H	1400	Ĥ	3550	Ĥ	3550
3560	LI11	i minúscula con acento agudo	í	í	3560	i	1730	I	1410	í	3560	í	3560
3570	LI12	I mayúscula con acento agudo	Í	Í	3570	I	1410	I	1410	Í	3570	Í	3570
3580	LI13	i minúscula con acento grave	ì	ì	3580	i	1730	I	1410	ì	3580	ì	3580
3590	LI14	I mayúscula con acento grave	Ì	Ì	3590	I	1410	I	1410	Ì	3590	Ì	3590

CUADRO A-19/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
3600	LI15	i minúscula con acento circunflejo	î	î	3600	i	1730	I	1410	î	3600	î	3600
3610	LI16	I mayúscula con acento circunflejo	Î	Î	3610	I	1410	I	1410	Î	3610	Î	3610
3620	LI17	i minúscula con diéresis o signo de umlaut	ï	ï	3620	i	1730	I	1410	ï	3620	ï	3620
3630	LI18	I mayúscula con diéresis o signo de umlaut	Ï	Ï	3630	I	1410	I	1410	Ï	3630	Ï	3630
3640	LI19	i minúscula con tilde	ĩ	ĩ	3640	i	1730	I	1410	ĩ	3640	ĩ	3640
3650	LI20	I mayúscula con tilde	Ĩ	Ĩ	3650	I	1410	I	1410	Ĩ	3650	Ĩ	3650
3660	LI30	I mayúscula con punto superior	İ	İ	3660	I	1410	I	1410	İ	3660	İ	3660
3670	LI31	i minúscula con signo de vocal larga (macrón)	ī	ī	3670	i	1730	I	1410	ī	3670	ī	3670
3680	LI32	I mayúscula con signo de vocal larga (macrón)	Ī	Ī	3680	I	1410	I	1410	Ī	3680	Ī	3680
3690	LI43	i minúscula con ogonek	į	į	3690	i	1730	I	1410	į	3690	į	3690
3700	LI44	I mayúscula con ogonek	Į	Į	3700	I	1410	I	1410	Į	3700	Į	3700
3710	LJ15	j minúscula con acento circunflejo	ĵ	ĵ	3710	j	1740	J	1420	ĵ	3710	ĵ	3710
3720	LJ16	J mayúscula con acento circunflejo	Ĵ	Ĵ	3720	J	1420	J	1420	Ĵ	3720	Ĵ	3720
3730	LK41	k minúscula con cedilla	ķ	ķ	3730	k	1750	K	1430	ķ	3730	ķ	3730
3740	LK42	K mayúscula con cedilla	Ķ	Ķ	3740	K	1430	K	1430	Ķ	3740	Ķ	3740
3750	LL11	l minúscula con acento agudo	ĺ	ĺ	3750	l	1760	L	1440	ĺ	3750	ĺ	3750
3760	LL12	L mayúscula con acento agudo	Ĺ	Ĺ	3760	L	1440	L	1440	Ĺ	3760	Ĺ	3760
3770	LL21	l minúscula con caron	ľ	ľ	3770	l	1760	L	1440	ľ	3770	ľ	3770
3780	LL22	L mayúscula con caron	Ľ	Ľ	3780	L	1440	L	1440	Ľ	3780	Ľ	3780
3790	LN11	n minúscula con acento agudo	ń	ń	3790	n	1780	N	1460	ń	3790	ń	3790

CUADRO A-20/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
3800	LN12	N mayúscula con acento agudo	Ń	Ń	3800	N	1460	N	1460	Ń	3800	Ń	3800
3810	LN19	n minúscula con tilde (eñe minúscula española)	ñ	ñ	3810	n	1780	N	1460	ñ	3810	ñ	3810
3820	LN20	N mayúscula con tilde (eñe mayúscula española)	Ñ	Ñ	3820	N	1460	N	1460	Ñ	3820	Ñ	3820
3830	LN21	n minúscula con caron	ň	ň	3830	n	1780	N	1460	ň	3830	ň	3830
3840	LN22	N mayúscula con caron	Ň	Ň	3840	N	1460	N	1460	Ň	3840	Ň	3840
3850	LN41	n minúscula con cedilla	ņ	ņ	3850	n	1780	N	1460	ņ	3850	ņ	3850
3860	LN42	N mayúscula con cedilla	Ņ	Ņ	3860	N	1460	N	1460	Ņ	3860	Ņ	3860
3870	LO11	o minúscula con acento agudo	ó	ó	3870	o	1790	O	1470	ó	3870	ó	3870
3880	LO12	O mayúscula con acento agudo	Ó	Ó	3880	O	1470	O	1470	Ó	3880	Ó	3880
3890	LO13	o minúscula con acento grave	ò	ò	3890	o	1790	O	1470	ò	3890	ò	3890
3900	LO14	O mayúscula con acento grave	Ò	Ò	3900	O	1470	O	1470	Ò	3900	Ò	3900
3910	LO15	o minúscula con acento circunflejo	ô	ô	3910	o	1790	O	1470	ô	3910	ô	3910
3920	LO16	O mayúscula con acento circunflejo	Ô	Ô	3920	O	1470	O	1470	Ô	3920	Ô	3920
3930	LO17	o minúscula con diéresis o signo de umlaut	ö	ö	3930	o	1790	O	1470	ö	3930	ö	3930
3940	LO18	O mayúscula con diéresis o signo de umlaut	Ö	Ö	3940	O	1470	O	1470	Ö	3940	Ö	3940
3950	LO19	o minúscula con tilde	õ	õ	3950	o	1790	O	1470	õ	3950	õ	3950
3960	LO20	O mayúscula con tilde	Õ	Õ	3960	O	1470	O	1470	Õ	3960	Õ	3960
3970	LO25	o minúscula con doble acente agudo	ő	ő	3970	o	1790	O	1470	ő	3970	ő	3970
3980	LO26	O mayúscula con doble acente agudo	Ő	Ő	3980	O	1470	O	1470	Ő	3980	Õ	3980
3990	LO31	o minúscula con signo de vocal larga (macrón)	ō	ō	3990	o	1790	O	1470	ō	3990	ō	3990

CUADRO A-21/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
4000	LO32	O mayúscula con signo de vocal larga (macrón)	Ō	Ō	4000	O	1470	O	1470	Ō	4000	Ō	4000
4010	LR11	r minúscula con acento agudo	ŕ	ŕ	4010	r	1820	R	1500	ŕ	4010	ŕ	4010
4020	LR12	R mayúscula con acento agudo	Ŕ	Ŕ	4020	R	1500	R	1500	Ŕ	4020	Ŕ	4020
4030	LR21	r minúscula con caron	ř	ř	4030	r	1820	R	1500	ř	4030	ř	4030
4040	LR22	R mayúscula con caron	Ř	Ř	4040	R	1500	R	1500	Ř	4040	Ř	4040
4050	LR41	r minúscula con cedilla	ŗ	ŗ	4050	r	1820	R	1500	ŗ	4050	ŗ	4050
4060	LR42	R mayúscula con cedilla	Ŗ	Ŗ	4060	R	1500	R	1500	Ŗ	4060	Ŗ	4060
4070	LS11	s minúscula con acento agudo	ś	ś	4070	s	1830	S	1510	ś	4070	ś	4070
4080	LS12	S mayúscula con acento agudo	Ś	Ś	4080	S	1510	S	1510	Ś	4080	Ś	4080
4090	LS15	s minúscula con acento circunflejo	ŝ	ŝ	4090	s	1830	S	1510	ŝ	4090	ŝ	4090
4100	LS16	S mayúscula con acento circunflejo	Ŝ	Ŝ	4100	S	1510	S	1510	Ŝ	4100	Ŝ	4100
4110	LS21	s minúscula con caron	š	š	4110	s	1830	S	1510	š	4110	š	4110
4120	LS22	S mayúscula con caron	Š	Š	4120	S	1510	S	1510	Š	4120	Š	4120
4130	LS41	s minúscula con cedilla	ş	ş	4130	s	1830	S	1510	ş	4130	ş	4130
4140	LS42	S mayúscula con cedilla	Ş	Ş	4140	S	1510	S	1510	Ş	4140	Ş	4140
4150	LT21	t minúscula con caron	ť	ť	4150	t	1840	T	1520	ť	4150	ť	4150
4160	LT22	T mayúscula con caron	Ť	Ť	4160	T	1520	T	1520	Ť	4160	Ť	4160
4170	LT41	t minúscula con cedilla	ţ	ţ	4170	t	1840	T	1520	ţ	4170	ţ	4170
4180	LT42	T mayúscula con cedilla	Ţ	Ţ	4180	T	1520	T	1520	Ţ	4180	Ţ	4180
4190	LU11	u minúscula con acento agudo	ú	ú	4190	u	1850	U	1530	ú	4190	ú	4190

CUADRO A-22/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.°				Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°	Símbolo	N.°
4200	LU12	U mayúscula con acento agudo	Ú	Ú	4200	U	1530	U	1530	Ú	4200	Ú	4200
4210	LU13	u minúscula con acento grave	ù	ù	4210	u	1850	U	1530	ù	4210	ù	4210
4220	LU14	U mayúscula con acento grave	Ù	Ù	4220	U	1530	U	1530	Ù	4220	Ù	4220
4230	LU15	u minúscula con acento circunflejo	û	û	4230	u	1850	U	1530	û	4230	û	4230
4240	LU16	U mayúscula con acento circunflejo	Û	Û	4240	U	1530	U	1530	Û	4240	Û	4240
4250	LU17	u minúscula con diéresis o signo de umlaut	ü	ü	4250	u	1850	U	1530	ü	4250	ü	4250
4260	LU18	U mayúscula con diéresis o signo de umlaut	Ü	Ü	4260	U	1530	U	1530	Ü	4260	Ü	4260
4270	LU19	u minúscula con tilde	ũ	ũ	4270	u	1850	U	1530	ũ	4270	ũ	4270
4280	LU20	U mayúscula con tilde	Ũ	Ũ	4280	U	1530	U	1530	Ũ	4280	Ũ	4280
4290	LU23	u minúscula con signo de vocal breve	ŭ	ŭ	4290	u	1850	U	1530	ŭ	4290	ŭ	4290
4300	LU24	U mayúscula con signo de vocal breve	Ŭ	Ŭ	4300	U	1530	U	1530	Ŭ	4300	Ŭ	4300
4310	LU25	u minúscula con doble acento agudo	ű	ű	4310	u	1850	U	1530	ű	4310	ű	4310
4320	LU26	U mayúscula con doble acento agudo	Ű	Ű	4320	U	1530	U	1530	Ű	4320	Ű	4320
4330	LU27	u minúscula con cero volado (o acento sueco)	ů	ů	4330	u	1850	U	1530	ů	4330	ů	4330
4340	LU28	U mayúscula con cero volado (o acento sueco)	Ů	Ů	4340	U	1530	U	1530	Ů	4340	Ů	4340
4350	LU31	u minúscula con signo de vocal larga (macrón)	ū	ū	4350	u	1850	U	1530	ū	4350	ū	4350
4360	LU32	U mayúscula con signo de vocal larga (macrón)	Ū	Ū	4360	U	1530	U	1530	Ū	4360	Ū	4360
4370	LU43	u minúscula con ogonek	ų	ų	4370	u	1850	U	1530	ų	4370	ų	4370
4380	LU44	U mayúscula con ogonek	Ų	Ų	4380	U	1530	U	1530	Ų	4380	Ų	4380
4390	LW15	w minúscula con acento circunflejo	ŵ	ŵ	4390	w	1870	W	1550	ŵ	4390	ŵ	4390

CUADRO A-23/X.408

JUEGO DE REFERENCIA				JUEGO CONVERTIDO									
Identificación		Denominación o descripción	Símbolo	T.61		VIRAI5		ATI2		Facsímil		Videotex	
N.º				Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º	Símbolo	N.º
4400	LW16	W mayúscula avec acento circunflejo	Ŵ	Ŵ	4400	W	1550	W	1550	Ŵ	4400	Ŵ	4400
4410	LY11	y minúscula con acento agudo	ý	ý	4410	y	1890	Y	1570	ý	4410	ý	4410
4420	LY12	Y mayúscula con acento agudo	Ý	Ý	4420	Y	1570	Y	1570	Ý	4420	Ý	4420
4430	LY15	y minúscula con acento circunflejo	ŷ	ŷ	4430	y	1890	Y	1570	ŷ	4430	ŷ	4430
4440	LY16	Y mayúscula con acento circunflejo	Ŷ	Ŷ	4440	Y	1570	Y	1570	Ŷ	4440	Ŷ	4440
4450	LY17	y minúscula con diéresis o signo de umlaut	ÿ	ÿ	4450	y	1890	Y	1570	ÿ	4450	ÿ	4450
4460	LY18	Y mayúscula con diéresis o signo de umlaut	Ÿ	Ÿ	4460	Y	1570	Y	1570	Ÿ	4460	Ÿ	4460
4470	LZ11	z minúscula con acento agudo	ź	ź	4470	z	1900	Z	1580	ź	4470	ź	4470
4480	LZ12	Z mayúscula con acento agudo	Ź	Ź	4480	Z	1580	Z	1580	Ź	4480	Ź	4480
4490	LZ21	z minúscula con caron	ž	ž	4490	z	1900	Z	1580	ž	4490	ž	4490
4500	LZ22	Z mayúscula con caron	Ž	Ž	4500	Z	1580	Z	1580	Ž	4500	Ž	4500
4510	LZ29	z minúscula con punto superior	ż	ż	4510	z	1900	Z	1580	ż	4510	ż	4510
4520	LZ30	Z mayúscula con punto superior	Ż	Ż	4520	Z	1580	Z	1580	Ż	4520	Ż	4520
4530													
4540													
4550													
4560													
4570													
4580													
4590													

ANEXO B

(a la Recomendación X.408)

Abreviaturas

En esta Recomendación se utilizan las siguientes abreviaturas:

AI	Alfabeto Internacional
APD	Descenso de la posición activa
APR	Retroceso de la posición activa hasta el comienzo de línea
ATI	Alfabeto Telegráfico Internacional
BS	Retroceso
CR	Retorno del carro
CS	Borrado de la pantalla
FaxG3	Tipo facsímil del Grupo 3
FF	Página siguiente
G3	Grupo 3
G4	Grupo 4
HT	Tabulación horizontal
IGS	Identificación de subrepertorio gráfico
ISA	Interconexión de sistemas abiertos
LF	Cambio de renglón
PFS	Selección de formato de página
PLD	Descenso parcial de renglón
PLU	Ascenso parcial de renglón
RLF	Cambio de renglón inverso
SGR	Selección de reproducción gráfica
SHS	Selección del espaciamiento horizontal
SP	Espacio
STM	Sistema de tratamiento de mensajes
SUB	Carácter de sustitución
SVS	Selección del espaciamiento vertical
TLX	Télex
TTX	Teletex
UE	Ulterior estudio
VT	Tabulación vertical

SISTEMAS DE TRATAMIENTO DE MENSAJES: SISTEMA DE TRANSFERENCIA DE MENSAJES: DEFINICIÓN DEL SERVICIO ABSTRACTO Y PROCEDIMIENTOS [1]

(Málaga-Torremolinos, 1984; modificada en Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión, controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) la necesidad de transferir y almacenar mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexion de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT;

(e) que las Recomendaciones de la serie X.500 definen los sistemas de guía;

(f) que los sistemas de tratamiento de mensajes se definen en una serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419; y

(g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

(1) que el servicio abstracto del sistema de transferencia de mensajes (STRM) se define en la sección 2;

(2) que el servicio abstracto del agente de transferencia de mensajes ATM se define en la sección 3;

(3) que los procedimientos ejecutados por los agentes de transferencia de mensajes (ATM) para garantizar el correcto funcionamiento distribuido del sistema de transferencia de mensajes se definen en la sección 4.

ÍNDICE

SECCIÓN 1 – *Introducción*

0 Introducción

1 Campo de aplicación

2 Referencias

3 Definiciones

4 Abreviaturas

5 Convenios

[1] La Recomendación X.411 y la Norma ISO 10021-4 [Information Processing Systems – Text Communication – MOTIS – Message Transfer System – Abstract Service Definition and Procedures] han sido desarrollados en estrecha colaboración, y armonizados en sus aspectos técnicos, salvo por lo que se refiere a las diferencias señaladas en el anexo C.

SECCIÓN 2 – *Servicio abstracto del sistema de transferencia de mensajes*

6 Modelo del sistema de transferencia de mensajes

7 Visión de conjunto del servicio abstracto del sistema de transferencia de mensajes

8 Definición del servicio abstracto del sistema de transferencia de mensajes

9 Definición de la sintaxis abstracta del sistema de transferencia de mensajes

SECCIÓN 3 – *Servicio abstracto de agente de transferencia de mensajes*

10 Modelo perfeccionado del sistema de transferencia de mensajes

11 Visión de conjunto del servicio abstracto del agente de transferencia de mensajes

12 Definición del servicio abstracto de agente de transferencia de mensajes

13 Definición de la sintaxis abstracta de agente de transferencia de mensajes

SECCIÓN 4 – *Procedimientos de funcionamiento distribuido del STRM*

14 Procedimientos de funcionamiento distribuido del STRM

Anexo A – Definición de referencia de los identificadores de objetos del STRM

Anexo B – Definición de referencia de los límites superiores de los parámetros del STRM

Anexo C – Diferencias entre la Norma ISO/CEI y la Recomendación del CCITT

SECCIÓN 1 – INTRODUCCIÓN

0 Introducción

Esta Recomendación forma parte de un conjunto de Recomendaciones que definen el tratamiento de mensajes en un entorno distribuido de sistemas abiertos.

El tratamiento de mensajes facilita el intercambio de mensajes entre usuarios sobre la base de un almacenamiento y retransmisión. Un mensaje remitido por un usuario (el *originador*) se transfiere a través del sistema de transferencia de mensajes (STRM) y se entrega a uno o más usuarios (los *destinatarios*).

El STRM consta de un cierto número de agentes de transferencia de mensajes (ATM), que transfieren mensajes y los entregan a los destinatarios deseados.

Esta Recomendación ha sido desarrollada conjuntamente por el CCITT y la ISO. El documento equivalente de ISO es el ISO 10021-4.

1 Campo de aplicación

Esta Recomendación define el servicio abstracto proporcionado por el STRM (servicio abstracto de STRM), y especifica los procedimientos que deben realizar los ATM para garantizar un funcionamiento distribuido correcto del STRM.

La Recomendación X.402 identifica otras Recomendaciones que definen otros aspectos de los sistemas de tratamiento de mensajes.

El acceso al servicio abstracto de STRM definido en esta Recomendación puede ser facilitado por el protocolo de acceso (P3) del STRM, definido en la Recomendación X.419. El funcionamiento distribuido del STRM definido en esta Recomendación puede garantizarse mediante la utilización del protocolo de transferencia del STRM (P1) también definido en la Recomendación X.419.

La sección 2 de esta Recomendación define el servicio abstracto del STRM. El § 6, describe el modelo de sistema de transferencia de mensajes. El § 7, proporciona una visión de conjunto del servicio abstracto del STRM. El § 8, define la semántica de los parámetros del servicio abstracto del STRM. El § 9 define la sintaxis-abstracta del servicio abstracto del STRM.

La sección 3 de esta Recomendación define el servicio abstracto del ATM. El § 10, perfecciona el modelo de STRM, presentado inicialmente en el § 6, para mostrar que el STRM incluye un cierto número de ATM que interfuncionan entre sí para prestar el servicio abstracto del STRM. El § 11, proporciona una visión de conjunto del servicio abstracto de ATM. El § 12, define la semántica de los parámetros del servicio abstracto de ATM. El § 13, define la sintaxis abstracta del servicio abstracto de ATM.

La sección 4 de esta Recomendación especifica los procedimientos realizados por los ATM para garantizar el funcionamieno distribuido correcto del STRM.

El anexo A proporciona una definición de referencia de los identificadores de objetos del STRM citados en los módulos NSA.1 del texto de esta Recomendación.

El anexo B proporciona una definición de referencia de los límites superiores de las limitaciones de tamaño impuestas sobre los tipos de datos de longitud variable definidos en los módulos de NSA.1 del texto de esta Recomendación.

El anexo C identifica las diferencias técnicas entre las versiones ISO/CEI y del CCITT de la presente Recomendación y de la publicación 10021-4 de ISO/CEI.

2 Referencias

Las referencias se enumeran en la Recomendación X.402.

3 Definiciones

Las definiciones se encuentran en la Recomendación X.402.

4 Abreviaturas

Las abreviaturas se enumeran en la Recomendación X.402.

5 Convenios

Esta Recomendación utiliza los convenios descriptivos descritos a continuación.

5.1 *Términos*

A lo largo de esta Recomendación, la redacción de los términos definidos y los nombres y valores de los parámetros del servicio abstracto de STRM y del servicio abstracto de ATM, a menos que sean nombres propios, comienzan con una letra minúscula y se unen con un guión de la siguiente forma: término-definido. Los nombres propios comienzan con una letra mayúscula (en el texto inglés) y no se unen mediante guión. En los § 8 y 12, los nombres y los valores de los parámetros del servicio abstracto de STRM y del servicio abstracto de ATM se escriben en negrita.

5.2 *Presencia de parámetros*

En los cuadros de los parámetros de los § 8 y 12, la presencia de cada parámetro se califica de la siguiente forma:

- Obligatorio (O): Parámetro obligatorio que debe existir siempre.
- Facultativo (F): Argumento facultativo que debe existir a discreción del invocador de la operación-abstracta; un resultado faculativo existirá a discreción del ejecutor de la operación-abstracta.
- Condicional (C): Debe existir un parámetro condicional según se define en la [Recomendación/norma internacional].

Cuando existe un parámetro condicional, debido a una cierta acción del STRM sobre el mensaje, sonda o informe, éste se define explícitamente. La presencia de otros parámetros condicionales depende de la presencia de estos parámetros en otras operaciones-abstractas (por ejemplo, la presencia de un argumento condicional de la operación abstracta de transferencia-mensaje depende de la presencia del mismo argumento facultativo en la correspondiente operación-abstracta de remisión-mensaje).

5.3 *Definiciones de sintaxis abstracta*

Esta Recomendación define la sintaxis-abstracta del servicio abstracto de STRM y del servicio abstracto de ATM utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208 y los convenios de definición del servicio abstracto definidos en la Recomendacion X.208 y los convenios de definición indicados en la Recomendación X.407.

Cuando se introducen cambios en los protocolos definidos en la Recomendación X.411 (1984) del CCITT, éstos se señalan en las definiciones de sintaxis abstracta subrayándolos.

6 Modelo del sistema de transferencia de mensajes

El tratamiento de mensajes facilita el intercambio de mensajes entre usuarios, sobre la base de un almacenamiento y retransmisión. A través de un sistema de transferencia de mensajes se transfiere un mensaje remitido por un usuario (el *originador*) y se entrega a uno o más usuarios (los *destinatarios*).

Se describe el STRM utilizando un modelo abstracto – el servicio abstracto de STRM – para definir los servicios prestados por el STRM en su conjunto.

El STRM se modela como un *objeto*, cuyo comportamiento global puede describirse sin hacer referencia a su estructura interna. Los servicios prestados por el objeto del STRM se encuentran disponibles en los *puertos*. Un tipo de puerto representa una visión particular de los servicios proporcionados por el objeto del STRM.

También se modela un usuario del STRM como un objeto que contiene los servicios prestados por el STRM a través de un puerto *emparejado* con un puerto del STRM del mismo tipo.

Un tipo de puerto corresponde a un conjunto de *operaciones-abstractas* que pueden tener lugar en un puerto; aquellas que puede realizar el objeto del STRM (invocado por el objeto del usuario-STRM), y aquellas que puede invocar el objeto de STRM (realizados por el objeto del usuario-STRM).

Un puerto puede ser simétrico, en cuyo caso el objeto del STRM puede invocar igualmente el conjunto de operaciones realizadas por el objeto del STRM, y viceversa. Por el contrario, el puerto puede ser asimétrico en cuyo caso el objeto se denomina *suministrador* o *consumidor* en relación con el tipo de puerto. Los términos *suministrador* y *consumidor* se utilizan únicamente para distinguir entre los papeles de un par de puertos que invocan o realizan operaciones. La asignación de los términos es generalmente intuitiva cuando un objeto proporciona un servicio utilizado por otro objeto; el objeto del servicio (por ejemplo, STRM) se considera generalmente como el *suministrador*, y el objeto del usuario (por ejemplo, un objeto del usuario-STRM) se considera generalmente como *consumidor*.

Antes de que los objetos puedan invocar operaciones sobre otros, deben ligarse a una *asociación* abstracta. La ligazón de una asociación entre objetos establece una relación entre los objetos que dura hasta que se libera la asociación. El iniciador de la asociación es quien libera siempre la asociación. La ligazón de una asociación establece las *credenciales* de los objetos que interaccionan, el *contexto-aplicación* y el *contexto-seguridad* de la asociación. El *contexto-aplicación* de una asociación puede ser uno o más tipos del puerto emparejado entre los dos objetos.

El modelo presentado es abstracto. Es decir, un observador exterior no siempre puede identificar las fronteras entre los objetos, o decidir el momento o los medios para la realización de las operaciones. Sin embargo, en ciertos casos el modelo abstracto puede ser realizado. Por ejemplo, una pareja de objetos que comunican a través de puertos emparejados puede colocarse en diferentes sistemas abiertos. En este caso, la frontera entre los objetos resulta visible, se exponen los puertos, y las operaciones pueden proporcionarse como casos de comunicación ISA.

El objeto del STRM admite puertos de tres tipos diferentes: un puerto-remisión, un puerto-entrega y un puerto-administración.

Un puerto-remisión permite a un usuario-STRM remitir mensajes al STRM para su transferencia y entrega a uno o más usuarios-STRM destinatarios, y sondear la aptitud del STRM para entregar un mensaje-tema.

Un puerto-entrega permite a un usuario STRM aceptar la entrega de mensajes del STRM, y aceptar informes sobre la entrega o no-entrega de mensajes y de sondas.

Un puerto-administración permite a un usuario-STRM modificar los parámetros a largo plazo contenidos en el STRM asociados con la entrega de mensajes, y permite al STRM o al usuario-STRM cambiar las *credenciales* con otro.

Un mensaje remitido por un usuario-STRM a través de un puerto-remisión se entregará normalmente a uno o más usuarios-STRM destinatarios a través de puertos-entrega. Los usuarios-STRM originadores pueden elegir la posibilidad de recibir notificación de la entrega o no entrega de un mensaje a través de su puerto-entrega.

La figura 1/X.411 presenta un modelo del sistema de transferencia de mensajes (STRM).

El § 7 proporciona una visión de conjunto del servicio abstracto de STRM.

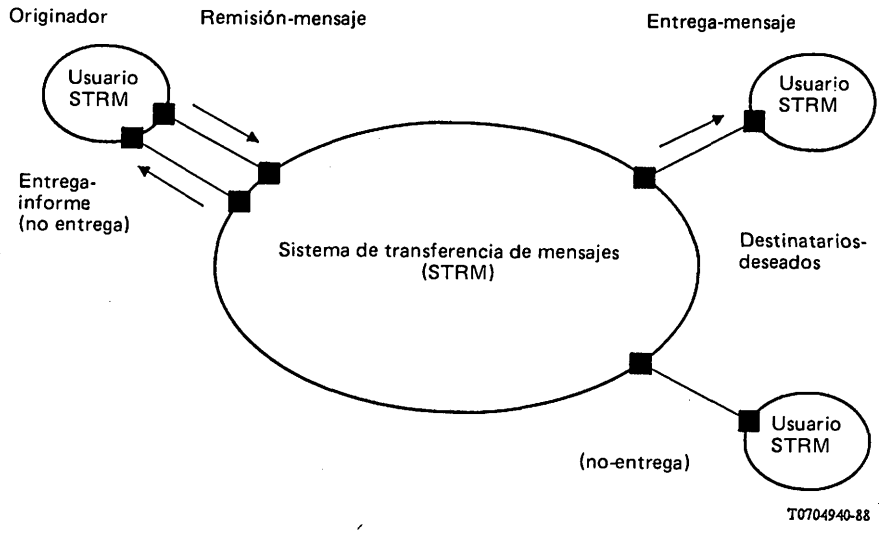


FIGURA 1/X.411

Modelo del servicio de transferencia de mensajes

7 Visión de conjunto del servicio abstracto del sistema de transferencia de mensajes

Esta Recomendación define los servicios siguientes que componen el servicio abstracto de STRM:

Vinculación y desvinculación STRM

a) vinculación-STRM

b) desvinculación-STRM

Operaciones abstractas en el puerto de remisión

c) remisión-mensajes

d) remisión-sonda

e) cancelación-entrega-diferida

f) control-remisión

Operaciones abstractas en el puerto de entrega

g) entrega-mensajes

h) entrega-informes

i) control-entrega

Operaciones abstractas en el puerto de administración

j) registro

k) cambio-credenciales.

7.1 *Vinculación y desvinculación al STRM*

La **vinculación-STRM** permite al usuario-STRM establecer una asociación con el STRM, o al STRM establecer una asociación con el usuario STRM. Otras operaciones-abstractas distintas de las de vinculación-STRM pueden invocarse únicamente en el contexto de una asociación establecida.

La **desvinculación-STRM** permite la liberación de una asociación establecida por el iniciador de la asociación.

7.2 *Puerta de remisión*

La operación-abstracta **remisión-mensaje** permite a un usuario-STRM remitir un mensaje al STRM para su transferencia y entrega a uno o más usuarios-STRM destinatarios.

La operación-abstracta **remisión-sonda** permite a un usuario-STRM remitir una sonda para determinar si podría transferirse y entregarse un mensaje a uno o más usuarios STRM, si éste fuera presentado.

La operación-abstracta **cancelación-entrega-diferida** permite a un usuario-STRM solicitar la cancelación de un mensaje previamente remitido (para entrega-diferida) mediante la invocación de la operación abstracta remisión-mensaje.

La operación-abstracta **control-remisión** permite al STRM limitar la utilización por parte del usuario de las operaciones-abstractas puerto-remisión.

Las operaciones-abstractas **remisión-mensaje** y **remisión-sonda** pueden provocar la invocación subsiguiente de la operación-abstracta entrega-informe por parte del STRM.

7.3 *Puerto de entrega*

La operación-abstracta **entrega-mensaje** permite al STRM entregar un mensaje al usuario-STRM.

La operación-abstracta **entrega-Informe** permite al STRM acusar recibo al usuario-STRM en relación con el resultado de la invocación previa de las operaciones-abstractas remisión-mensaje o remisión-sonda. Para la operación abstracta remisión-mensaje, la operación abstracta entrega-informe indica la entrega o no entrega del mensaje presentado. Para la operación-abstracta remisión-sonda, la operación-abstracta entrega-informe indica si podría entregarse o no un mensaje en el caso de que éste se presentara. La operación-abstracta entrega-informe puede también transportar una notificación entrega-física por un SEF.

La operación-abstracta **control-entrega** permite a un usuario-STRM limitar la utilización de las operaciones-abstractas puerto-entrega por parte del STRM.

7.4 *Puerto de administración*

La operación-abstracta **registro** permite a un usuario-STRM cambiar los parámetros a largo plazo del usuario-STRM contenidos en el STRM, asociados a la entrega de un mensaje.

La operación abstracta **cambio-credenciales** permite a un usuario-STRM cambiar sus **credenciales** con el STRM y al STRM cambiar sus **credenciales** con el usuario-STRM.

8 Definición del servicio abstracto del sistema de transferencia de mensajes

En este punto, se define la semántica de los parámetros del servicio abstracto del STRM.

El § 8.1 define la vinculación-STRM y la desvinculación-STRM. El § 8.2 define el puerto-remisión. El § 8.3 define el puerto-entrega. El § 8.4 define el puerto-administración. El § 8.5 define algunos tipos de parámetros comunes.

La sintaxis-abstracta del servicio abstracto del STRM se define en el § 9.

8.1 *Vinculación-STRM y desvinculación-STRM*

En este punto se definen las operaciones vinculación-STRM y desvinculación-STRM utilizadas para establecer y liberar asociaciones entre un usuario-STRM y el STRM.

8.1.1 *Vinculación-abstracta y desvinculación-abstracta*

En este punto se definen las operaciones siguientes: vinculación-abstracta y desvinculación-abstracta;

a) vinculación-STRM
b) desvinculación-STRM.

8.1.1.1 *Vinculación-STRM*

La vinculación-STRM permite a un usuario-STRM establecer una asociación con el STRM, o al STRM establecer una asociación con un usuario-STRM.

La vinculación-STRM establece las **credenciales** de un usuario-STRM y permite al usuario-STRM interaccionar, y establece el **contexto-aplicación** y el **contexto-seguridad** de la asociación. Únicamente el iniciador puede liberar esta asociación (utilizando la desvinculación-STRM).

Pueden invocarse otras operaciones-abstractas diferentes de la vinculación-STRM en el contexto de una asociación establecida.

La consecución con éxito de vinculación-STRM significa el establecimiento de una asociación.

La interrupción de vinculación-STRM debido a un error-vinculación indica que no se ha establecido una asociación.

8.1.1.1.1 *Argumentos*

El cuadro 1/X.411 enumera los argumentos de vinculación-STRM, y para cada argumento califica su presencia e indica el punto donde se define el argumento.

CUADRO 1/X.411

Argumentos de vinculación-STRM

Argumento	Presencia	Punto
Argumentos de vinculación		
Nombre-iniciador	O	8.1.1.1.1.1
Credenciales-iniciador	O	8.1.1.1.1.2
Contexto-seguridad	F	8.1.1.1.1.3
Mensajes-esperando	F	8.1.1.1.1.4

8.1.1.1.1.1 *Nombre-iniciador*

Este argumento contiene un nombre para el iniciador de la asociación. Debe ser generado por el iniciador de la asociación.

Si el iniciador es un usuario-STRM, el nombre es el **nombre-O/D** del usuario-STRM, que está inscrito en el STRM (véase el § 8.4.1.1.1.1). El **nombre-iniciador** contiene la **dirección-O/D** y puede contener también opcionalmente el **nombre-guía**, del usuario-STRM, (**Dirección-O/D-y-nombre-guía- facultativo**). Para seguridad en la mensajería, cuando interviene una MM el **nombre-iniciador** puede también indicar si el iniciador es un AU o una MM.

Si el iniciador es el STRM (o un ATM – véase el § 11), el nombre es un **nombre-ATM**, que conoce el usuario-STRM.

8.1.1.1.1.2 *Credenciales-iniciador*

Este argumento contiene las **credenciales** del iniciador de la asociación. Debe ser generado por el iniciador de la asociación.

Las **credenciales-iniciador** pueden utilizarse por el respondedor para autenticar la identidad del iniciador (véase Recomendación X.509).

Si se utiliza únicamente una autenticación-simple, las **credenciales-iniciador** consisten en una **contraseña** simple asociada al **nombre-iniciador**.

Si se utiliza una autenticación-fuerte, las **credenciales-iniciador** comprenden un **testigo-vinculación-iniciador** y de forma opcional un **certificado-iniciador**.

El **testigo-vinculación-iniciador** es un **testigo** generado por el iniciador de la asociación. Si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**, los **datos-firmados** incluyen un **número-aleatorio**. Los **datos-cifrados** de un **testigo-asimétrico** pueden utilizarse para transportar información-sobre-seguridad secreta (por ejemplo, una o más claves-cifrado-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-iniciador**.

El **certificado-iniciador** es un **certificado** del iniciador de la asociación, generado por una fuente de confianza (por ejemplo, autoridad-certificación). Puede suministrarse por el iniciador de la asociación, si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**. El **certificado-iniciador** puede utilizarse para transportar una copia verificada de la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del iniciador de la asociación. La clave-cifrado-pública-asimétrica puede utilizarse por el respondedor para calcular el **testigo-vinculación-respondedor**. Si se sabe que el respondedor dispone o tiene acceso al **certificado** del iniciador (por ejemplo, a través de la operación-abstracta de cambiar-credenciales, o a través de la guía), puede omitirse el **certificado-iniciador**.

8.1.1.1.1.3 *Contexto-seguridad*

Este argumento identifica el **contexto-seguridad** con el que el iniciador de la asociación propone funcionar. Puede generarse por el iniciador de la asociación.

El **contexto-seguridad** incluye una o más **etiquetas-seguridad** que definen la sensibilidad de las interacciones que pueden producirse entre el usuario-STRM y el STRM a lo largo de la duración de la asociación, en línea con la política- seguridad en vigor. El **contexto-seguridad** debe ser uno entre los autorizados por las **etiquetas-seguridad-usuario** registradas del usuario-STRM y por las **etiquetas-seguridad** asociadas al ATM del STRM.

Una vez establecido, el **contexto-seguridad** del puerto-remisión y del puerto-entrega puede restringirse transitoriamente utilizando las operaciones-abstractas de control-remisión (véase el § 8.2.1.4.5) y de control-entrega (véase el § 8.3.1.3.1.7), respectivamente.

Si no se establecen los **contextos-seguridad** entre el usuario-STRM y el STRM, la sensibilidad de las interacciones que pueden producirse entre el usuario-STRM y el STRM pueden dejarse a la discreción del invocador de una operación-abstracta.

8.1.1.1.1.4 *Mensajes-esperando*

Este argumento indica el número de mensajes y el número total de octetos que esperan para ser entregados por el STRM al usuario-STRM, para cada **prioridad**. Puede generarse por el iniciador de la asociación.

Este argumento estará únicamente presente cuando el STRM inicie una asociación con un usuario-STRM, y cuando un usuario-STRM se abone al elemento-de-servicio retención de entrega (definido en la Recomendación X.400).

8.1.1.1.2 *Resultados*

El cuadro 2/X.411 enumera los resultados de vinculación-STRM, y para cada resultado califica su presencia e indica el punto donde se define el resultado.

CUADRO 2/X.411

Resultados de vinculación-STRM

Resultado	Presencia	Punto
Resultado de vinculación		
Nombre-respondedor	O	8.1.1.1.2.1
Credenciales-respondedor	O	8.1.1.1.2.2
Mensajes-esperando	F	8.1.1.1.2.3

8.1.1.1.2.1 *Nombre-respondedor*

Este argumento contiene un nombre para el respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

Si el respondedor es un usuario-SRTM, el nombre es el **nombre-O/D** del usuario-STRM, que se inscribe con el SRTM (véase el § 8.4.1.1.1.1). El **nombre-respondedor** contendrá la **dirección-O/D** y puede contener también de forma opcional el **nombre-guía**, del usuario-STRM (**dirección-O/D-y-nombre-opcional-guía**). Para seguridad en la mensajería, cuando interviene una MM el **nombre-respondedor** puede también indicar si el respondedor es un AU o una MM.

Si el respondedor es el STRM (o un ATM – véase el § 11), el nombre es un **nombre-ATM**, que conoce el usuario-STRM.

8.1.1.1.2.2 *Credenciales-respondedor*

Este argumento contiene las **credenciales** del respondedor de la asociación. Debe ser generado por el respondedor de la asociación.

Las **credenciales-respondedor** pueden utilizarse por el iniciador para autenticar la identidad del respondedor (véase Recomendación X.509).

Si se utiliza únicamente la autenticación-simple, las **credenciales-respondedor** incluyen una **contraseña** simple asociada al **nombre-respondedor**.

Si se utiliza una autenticación-fuerte, las **credenciales-respondedor** constan de un **testigo-vinculación-respondedor**. El **testigo-vinculación-respondedor** es un testigo generado por el respondedor de la asociación. El **testigo-vinculación-respondedor** debe ser del mismo tipo que el **testigo-vinculación-iniciador**. Si el **testigo-vinculación-respondedor** es un **testigo-asimétrico**, los datos firmados constan de un **número-aleatorio** (que puede estar relacionado con el **número-aleatorio** suministrado en el **testigo-vinculación-iniciador**). Los **datos-cifrados** de un **testigo asimétrico** pueden utilizarse para transportar información-sobre-seguridad secreta (por ejemplo, una o más claves-cifrado-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-respondedor**.

8.1.1.1.2.3 *Mensajes esperando*

Este argumento indica el número de mensajes y el número total de octetos que esperan para ser entregados por el STRM al usuario-STRM, para cada **prioridad**. Puede generarse por el respondedor de la asociación.

Este argumento debe estar únicamente presente cuando el STRM conteste a una asociación iniciada por un usuario-STRM, y cuando un usuario-STRM se abone al elemento-de-servicio retención de entrega (véase Recomendación X.400).

8.1.1.1.3 *Errores-vinculación*

Los errores-vinculación que pueden interrumpir la vinculación-STRM se definen en el § 8.1.2.

8.1.1.2 *Desvinculación-STRM*

La desvinculación-STRM permite liberar una asociación establecida por el iniciador de la asociación.

8.1.1.2.1 *Argumentos*

La desvinculación-STRM no tiene argumentos.

8.1.1.2.2 *Resultados*

La desvinculación-STRM devuelve un resultado vacío como indicación de la liberación de la asociación.

8.1.1.2.3 *Errores-desvinculación*

No existen errores-desvinculación que puedan interrumpir la desvinculación-STRM.

8.1.2 *Errores-vinculación*

En este punto se definen los siguientes errores-vinculación:

a) error-autenticación
b) ocupado
c) modo-diálogo-inaceptable
d) contexto-seguridad-inaceptable

8.1.2.1 *Error-autenticación*

El error-vinculación de error-autenticación notifica que no puede establecerse una asociación debido a un error de autenticación; las **credenciales** del iniciador no son aceptables o están indebidamente especificadas.

El error-vinculación de error-autenticación no tiene parámetros.

8.1.2.2 *Ocupado*

El error-vinculación ocupado notifica que una asociación no puede establecerse porque el respondedor está ocupado.

El error-vinculación-ocupado no tiene parámetros.

8.1.2.3 *Modo-diálogo-inaceptable*

Un error-vinculación de modo-diálogo-inaceptable notifica que el modo-diálogo propuesto por el iniciador de la asociación es inaceptable para el respondedor (véase Recomendación X.419).

El error-vinculación de diálogo-inaceptable no tiene parámetros.

8.1.2.4 *Contexto-seguridad-inaceptable*

Un error-vinculación de contexto-seguridad-inaceptable notifica que el **contexto-seguridad** propuesto por el iniciador de la asociación resulta inaceptable para el respondedor.

El error-vinculación de contexto-seguridad-inaceptable no tiene parámetros.

8.2 *Puerto de remisión*

En este punto se definen las operaciones-abstractas y los errores abstractos que se producen en el puerto de remisión.

8.2.1 *Operación abstracta*

En este punto se definen las siguientes operaciones abstractas en el puerto de depósito:

a) remisión-mensaje
b) remisión-sonda
c) cancelación-entrega-diferida
d) control-remisión.

8.2.1.1 *Remisión-mensaje*

La operación abstracta remisión-mensaje permite al usuario-STRM remitir un mensaje al STRM para su transferencia y entrega a uno o más usuarios-STRM destinatarios.

La ejecución satisfactoria de la operación abstracta significa que el STRM ha aceptado la responsabilidad del mensaje (pero no que se haya entregado ya los destinatarios deseados).

La interrupción de la operación-abstracta por un error-abstracto indica que el STRM no puede asumir la responsabilidad del mensaje.

8.2.1.1.1 *Argumentos*

El cuadro 3/X.411 enumera los argumentos de la operación abstracta remisión-mensaje, y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

8.2.1.1.1.1 *Nombre-originador*

Este argumento contiene el **nombre-O/D** del originador del mensaje. Se debe generar por el usuario-STRM originador.

El **nombre-originador** contiene el **nombre-O/D** de un originador individual, es decir no debe contener el **nombre-O/D** de una LD.

8.2.1.1.1.2 *Nombre-destinatario*

Este argumento contiene el **nombre-O/D** de un destinatario del mensaje. Se debe generar por el originador del mensaje. Se debe especificar un valor diferente de este argumento para cada destinatario del mensaje.

El **nombre-destinatario** contiene el **nombre-O/D** de un destinatario individual o de una LD.

8.2.1.1.1.3 *Destinatario-alternativo-autorizado*

Este argumento indica si puede entregarse el mensaje a un destinatario alternativo asignado por el DG-destinatario, si el **nombre-destinatario** no identifica un usuario-STRM. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **destinatario-alternativo-autorizado** o **destinatario-alternativo-prohibido**.

CUADRO 3/X.411

Argumentos de remisión-mensaje

Argumento	Presencia	Punto
Argumento del originador		
Nombre-originador	O	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	O	8.2.1.1.1.2
Destinatario-alternativo-autorizado	F	8.2.1.1.1.3
Reasignación-destinatario-prohibida	F	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	F	8.2.1.1.1.5
Ampliación-LD-prohibida	F	8.2.1.1.1.6
Revelación de destinatarios	F	8.2.1.1.1.7
Argumento de prioridad		
Prioridad	F	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	F	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	F	8.2.1.1.1.10
Conversión-explícita	F	8.2.1.1.1.11
Argumentos de tiempo de entrega		
Tiempo-entrega-diferida	F	8.2.1.1.1.12
Último-tiempo-entrega	F	8.2.1.1.1.13
Argumento de método de entrega		
Método-entrega-solicitado	F	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	F	8.2.1.1.1.15
Petición-dirección-envío-físico	F	8.2.1.1.1.16
Modos-entrega-física	F	8.2.1.1.1.17
Tipo-correo-certificado	F	8.2.1.1.1.18
Número-destinatario-para-aviso	F	8.2.1.1.1.19
Atributos-reproducción-física	F	8.2.1.1.1.20
Dirección-devolución-originador	F	8.2.1.1.1.21
Argumentos de petición de informes		
Petición-informe-originador	O	8.2.1.1.1.22
Petición-devolución-contenido	F	8.2.1.1.1.23
Petición-informe-entrega-física	F	8.2.1.1.1.24
Argumentos de seguridad		
Certificado-originador	F	8.2.1.1.1.25
Testigo-mensaje	F	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	F	8.2.1.1.1.27
Verificación-integridad-contenido	F	8.2.1.1.1.28
Verificación-autenticación-mensaje-origen	F	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	F	8.2.1.1.1.30
Petición-prueba-de-remisión	F	8.2.1.1.1.31
Petición-prueba-de-entrega	F	8.2.1.1.1.32
Argumentos de contenido		
Tipos-información-codificada-originales	F	8.2.1.1.1.33
Tipo-contenido	O	8.2.1.1.1.34
Identificador-contenido	F	8.2.1.1.1.35
Correlador-contenido	F	8.2.1.1.1.36
Contenido	O	8.2.1.1.1.37

Si este argumento tiene el valor **destinatario-alternativo-autorizado** y el **nombre-destinatario** (especificado por el originador del mensaje, o añadido por una ampliación-LD, o substituido mediante una nueva dirección por el **destinatario-alternativo-asignado-destinatario** o por el **destinatario-alternativo-solicitado-originador**, o presente mediante una combinación de una nueva dirección y una ampliación) no identifica a un usuario STRM, el mensaje puede redirigirse hacia un destinatario alternativo asignado por el DG-destinatario para recibir dichos mensajes. Si el DG-destinatario no ha asignado ninguno de estos destinatarios-alternativos, o si este argumento tiene el valor **destinatario-alternativo-prohibido**, se generará un informe de no entrega.

En ausencia de este argumento se supondrá por defecto **destinatario-alternativo-prohibido**.

8.2.1.1.1.4 *Reasignación-destinatario-prohibida*

Este argumento indica si el mensaje puede reasignarse a un **destinatario-alternativo-asignado-destinatario** registrado por el destinatario-deseado. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **reasignación-destinatario-prohibida** o **reasignación-destinatario-autorizada**.

Si este argumento tiene el valor **reasignación-destinatario-autorizada** y el destinatario-deseado ha registrado un **destinatario-alternativo-asignado-destinatario**, el mensaje se redireccionará hacia el **destinatario-alternativo-asignado-destinatario**.

Si este argumento tiene el valor **reasignación-destinatario-prohibida** y el destinatario-deseado ha registrado un **destinatario-alternativo-asignado-destinatario**, entonces si el originador del mensaje ha especificado **destinatario-alternativo-solicitado-originador** se redirigirá el mensaje hacia el **destinatario-alternativo-solicitado-originador**, o si el originador del mensaje no ha especificado un **destinatario-alternativo-solicitado-originador**, se generará un informe de no-entrega.

En ausencia de este argumento, se supondrá por defecto **reasignación-destinatario-autorizada**.

8.2.1.1.1.5 *Destinatario-alternativo-solicitado-originador*

Este argumento contiene el **nombre-O/D** del destinatario alternativo solicitado por el originador del mensaje. Puede generarse por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

El **destinatario-alternativo-solicitado-originador** contiene el **nombre-O/D** de un destinatario-alternativo individual o LD.

Si este argumento está presente y no resulta posible la entrega del mensaje al **nombre-destinatario** (especificado por el originador del mensaje, o añadido por una ampliación-LD, o substituido mediante una nueva dirección por el **destinatario-alternativo-asignado-destinatario**), el mensaje se debe redirigir al **destinatario-alternativo-solicitado-originador** especificado por este argumento.

Si el originador del mensaje ha especificado un **destinatario-alternativo-solicitado-originador**, el mensaje será redirigido a ese destinatario alternativo con preferencia a uno asignado por el DG-destinatario.

8.2.1.1.1.6 *Ampliación-LD prohibida*

Este argumento indica si se producirá una ampliación-LD dentro del STRM para cualquier **nombre-destinatario** que designe una LD. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **ampliación-LD prohibida** o **ampliación-LD autorizada**.

En ausencia de este argumento se supondrá por defecto **ampliación-LD autorizada**.

8.2.1.1.1.7 *Revelación-de-destinatarios*

Este argumento indica si debe indicarse el **nombre-destinatario** de todos los destinatarios a cada usuario-STRM destinatario al entregar el mensaje. Puede generarse por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **revelación-de-destinatarios-autorizada** o **revelación-de-destinatarios-prohibida**.

En ausencia de este argumento se supondrá por defecto **revelación-de-destinatarios-prohibida**.

8.2.1.1.1.8 *Prioridad*

Este argumento especifica la prioridad relativa del mensaje: **normal, no-urgente** o **urgente**. Puede generarse por el originador del mensaje.

En ausencia de este argumento se supondrá por defecto una **prioridad normal**.

8.2.1.1.1.9 *Conversión-implícita-prohibida*

Este argumento indica si puede realizarse una conversión implícita del **contenido** del mensaje. Puede generarse por el originador del mensaje.

Este argumento puede tener los siguientes valores: **conversión-implícita-prohibida** o **conversión-implícita-autorizada**.

En ausencia de este argumento, se supondrá por defecto **conversión-implícita-autorizada**.

Véase igualmente el § 8.2.1.1.1.10.

8.2.1.1.1.10 *Conversión-con-pérdida-prohibida*

Este argumento indica si puede realizarse una conversión o conversiones del **tipo-información-codificada** del **contenido** del mensaje, en el caso de que dicha conversión o conversiones pueden dar lugar a una pérdida de información. La pérdida de información se define en la Recomendación X.408. Puede generarse por el originador del mensaje.

Este argumento puede tener los siguientes valores: **conversión-con-pérdida-prohibida** o **conversión-con-pérdida-autorizada**.

En ausencia de este argumento se supondrá por defecto **conversión-con- pérdida-autorizada**.

El efecto combinado de los argumentos de **conversión-implícita-prohibida** y de **conversión-con-pérdida-prohibida** se refiere únicamente a las conversiones-implícitas y se define en el cuadro 4/X.411.

CUADRO 4/X.411

Efecto combinado de los argumentos de conversión

Conversión implícita	Conversión con pérdida	Efecto combinado
autorizada	con-pérdida-autorizada	autorizado
autorizada	con-pérdida-prohibida	con-pérdida-prohibida
prohibida	con-pérdida-autorizada	prohibido
prohibida	con-pérdida-prohibida	prohibido

8.2.1.1.1.11 *Conversión explícita*

Este argumento indica el tipo de conversión del **contenido** del mensaje solicitado explícitamente por el originador para el destinatario. Puede generarse por el originador del mensaje. Puede especificarse un valor diferente de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **no-conversión-explícita, ai5-texto-a-teletex, teletex-a-télex, télex-a-texto-ai5, télex-a-teletex, télex-a-g4-clase-1, télex-a-videotex, texto-ai5-a-télex, télex-a-facsímil-g3, texto-ai5-a-facsímil-g3, texto-ai5-a-g4-clase-1, texto-ai5-a-videotex, teletex-a-texto-ai5, teletex-a-facsímil-g3, teletex-a-g4-clase-1, teletex-a-videotex, videotex-a-télex, videotex-a-texto-ai5** o **videotex-a-télex**. Pueden definirse otros tipos de **conversión explícita** en versiones futuras de esta Recomendación. La **conversión-explícita** se debe realizar conforme a lo especificado en la Recomendación X.408.

En ausencia de este argumento se supondrá por defecto **no-conversión-explícita**.

Nota – Cuando se especifica la **conversión-explícita** para una LD de destinatarios, ésta se aplica a todos los miembros de la LD.

8.2.1.1.1.12 *Tiempo-entrega-diferida*

Este argumento especifica el **tiempo** antes del cual no debería entregarse el mensaje al destinatario o destinatarios. Puede generarse por el originador del mensaje.

8.2.1.1.1.13 *Último-tiempo-entrega*

Este argumento contiene el **tiempo** después del cual no debería entregarse el mensaje al destinatario o destinatarios. Puede generarse por el originador del mensaje.

El tratamiento de la no entrega debido al **último-tiempo-entrega** se describe en el § 14.3.2.4.

8.2.1.1.1.14 *Método-entrega-solicitado*

Este argumento indica el método solicitado de entrega del mensaje al destinatario. Puede generarse por el originador del mensaje. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno o más de los siguientes valores: **cualquier-método-entrega**, **entrega-STM**, **entrega-física**, **entrega-télex**, **entrega-teletex**, **entrega-facsímil-g3**, **entrega-facsímil-g4**, **entrega-terminal-ai5**, **entrega-videotex**, o **entrega telefónica**.

Si se especifica más de un valor de este argumento para un destinatario, se supondrá que la secuencia de valores implica un orden de preferencia del originador respecto de los métodos-entrega.

En ausencia de este argumento, se supondrá por defecto **cualquier-método-entrega**.

Si el **nombre-destinatario** generado por el originador del mensaje contiene un **nombre-guía** pero omite una **dirección-O/D**, el STRM puede utilizar el **método-entrega-solicitado** como una indicación de la forma de **dirección O/D** en que el STRM debería transformar **el nombre-guía** (por ejemplo utilizando la guía). Si no puede encontrarse una forma de **dirección-O/D** adecuada al **método-entrega-solicitado**, se debe devolver al originador del mensaje un error-abstracto **destinatario-impropiamente-especificado**.

Si el **nombre-destinatario** generado por el originador del mensaje contiene una **dirección-O/D** con una forma no adecuada para el **método-entrega-solicitado**, se debe devolver al originador del mensaje un informe-no-entrega.

Si el **método-entrega-solicitado** suministrado-originador entra en conflicto con el método-entrega preferido del destinatario (por ejemplo registrado en la guía en el atributo método-entrega-preferido-stm), el **método-entrega-solicitado** del originador tiene preferencia. Si el **método-entrega-solicitado** entra en conflicto con los requisitos de conversión del originador (véanse los § 8.2.1.1.1.9 a 8.2.1.1.1.11) se debe devolver un informe de no-entrega al originador del mensaje.

8.2.1.1.1.15 *Envío-físico-prohibido*

Este argumento indica si está prohibido el envío-físico de un mensaje. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los siguientes valores: **envío-físico-autorizado**, o **envío-físico-prohibido**.

En ausencia de este argumento se supondrá por defecto **envío-físico-autorizado**.

8.2.1.1.1.16 *Petición-dirección-envío-físico*

Este argumento indica si debe devolverse en un informe la dirección-envío-físico del destinatario. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los siguientes valores: **dirección-envío-físico-solicitada**, o **dirección-envío-físico-no-solicitada**.

En ausencia de este argumento se supondrá por defecto **dirección-envío-físico-no-solicitada**.

Se puede solicitar una dirección de envío físico cuando el envío físico esté prohibido o permitido (véase el § 8.2.1.1.1.15).

8.2.1.1.1.17 *Modos-entrega-física*

Este argumento indica el modo de entrega-física al destinatario que ha de utilizarse. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **correo-ordinario, urgente, entrega-inmediata, retirada-ventanilla, retirada-ventanilla-con-aviso-telefónico, retirada-ventanilla-con-aviso-télex, retirada-ventanilla-con-aviso-teletex,** o **entrega-burofax.**

Obsérvese que la **entrega-burofax** comprende todos los modos de entrega del A al H definidos en la Recomendación F.170, es decir A – Entrega Regular, B – Urgente, C – Entrega Inmediata, D – Retirada en ventanilla, E – Retirada en ventanilla con aviso telefónico, F – Telefax, G – Retirada en ventanilla con aviso télex, y H – Retirada en ventanilla con aviso teletex.

En ausencia de este argumento, se supondrá por defecto **correo-ordinario.**

8.2.1.1.1.18 *Tipo-correo-certificado*

Este argumento indica el tipo de correo certificado que ha de utilizarse para entregar físicamente el mensaje al destinatario. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **correo-no-certificado, correo-certificado,** o **correo-certificado-a-dirección-en-persona.**

En ausencia de este argumento se supondrá por defecto **correo-ordinario.**

8.2.1.1.1.19 *Número-destinatario-para-aviso*

Este argumento contiene el número de teléfono, télex o teletex del destinatario, para utilizarlo en combinación con los modos **modo-entrega-física, modo-recogida-oficina-postal-con-aviso** y **modo-entrega-burofax.** Pueden generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una **entrega-física** al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario y el argumento de los **modos-entrega-física** especifica un **modo-entrega-física,** un **modo-recogida-oficina-postal-con-aviso** o un **modo-entrega-burofax.** Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

8.2.1.1.1.20 *Atributos-reproducción-física*

Este argumento indica los **atributos-reproducción-física** del mensaje. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física al destinatario, o si el originador del mensaje proporcionó la **dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **básico.** Tal vez futuras versiones de esta Recomendación definan otros valores de este argumento. Mediante acuerdos bilaterales entre los DG pueden utilizarse otros valores de este argumento.

En ausencia de este argumento se supondrá el valor por defecto **básico.**

8.2.1.1.1.21 *Dirección-devolución-originador*

Este argumento contiene la **dirección-O/D-postal** del originador del mensaje. Se debe generar por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega física a uno o más destinatarios, o si el originador del mensaje proporcionó una o más **direcciones-postales-O/D** de los destinatarios. Puede generarse igualmente por el originador del mensaje si una LD de destinatarios contiene o es probable que contenga uno o más miembros para los cuales se solicita la entrega-física.

La **dirección-devolución-originador** contendrá la **dirección-postal-O/D** de cada originador (**dirección-O/D**), es decir no contendrá ni el **nombre-guía** de un originador ni el **nombre-guía** de una LD.

8.2.1.1.1.22 *Petición-informe-originador*

Este argumento indica la categoría de informe solicitada por el originador del mensaje. Se debe generar por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes:

- **no-informe**: el originador del mensaje solicita la supresión de los informes de no-entrega;
- **informe-no-entrega**: se devuelve un informe únicamente en el caso de no-entrega;
- **informe**: se devuelve un informe en el caso de entrega o de no-entrega.

Obsérvese que el valor de este argumento puede cambiarse en un punto-ampliación de LD. Dicho cambio puede afectar al número y tipo de informe que el originador del mensaje puede recibir sobre la entrega a una LD.

8.2.1.1.1.23 *Petición-devolución-contenido*

Este argumento indica si el **contenido** del mensaje debe devolverse con cualquier informe-no-entrega. Se puede generar por el originador del mensaje.

Este argumento puede tener uno de los valores siguientes: **devolución-contenido-solicitada** o **devolución-contenido-no-solicitada**.

En ausencia de este argumento, se supondrá por defecto **devolución- contenido-no-solicitada**.

Obsérvese que la supresión de los informes-no-entrega por el originador del mensaje (véase el § 8.2.1.1.1.22) tiene preferencia sobre una petición de devolución del **contenido**.

Obsérvese que en el caso de informes-no-entrega entregados al propietario de una LD (véase el § 8.3.1.2.1.4), el **contenido** del mensaje no estará presente.

8.2.1.1.1.24 *Petición-informe-entrega-física*

Este argumento indica el tipo de informe-entrega-física solicitado por el originador del mensaje. Puede generarse por el originador del mensaje si el argumento **método-entrega-solicitado** especifica que se necesita una entrega-física al destinatario, o si el originador del mensaje proporcionó **la dirección-postal-O/D** del destinatario. Puede especificarse un valor distinto de este argumento para cada uno de los destinatarios del mensaje.

Este argumento puede tener uno de los valores siguientes: **devolución-de-correo-inentregable-por-SEF**, **devolución-de-notificación-por-SEF**, **devolución-de-notificación-por-STM** o **devolución-de-notificación-por-STM-y-SEF**.

En ausencia de este argumento, se supondrá por defecto **devolución-de-correo-inentregable-por-SEF**.

8.2.1.1.1.25 *Certificado-originador*

Este argumento contiene el **certificado** del originador del mensaje. Se debe generar por una fuente de confianza (por ejemplo autoridad de certificación), y puede suministrarse por el originador del mensaje.

El **certificado-originador** puede utilizarse para transportar una copia verificada de la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del originador del mensaje.

La clave-cifrado-pública-asimétrica puede ser utilizada por los destinatarios del mensaje para validar el **distintivo-mensaje**, si se utiliza un **distintivo-asimétrico**.

La clave-encripción-pública-asimétrica puede igualmente utilizarse por los destinatarios del mensaje, y cualquier ATM a través del cual se transfiere un mensaje para validar la **comprobación-autenticación-origen-mensaje**.

8.2.1.1.1.26 *Testigo-mensaje*

Este argumento contiene el **testigo** asociado al mensaje. Puede generarse por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

Si el **testigo-mensaje** es un **testigo-asimétrico**, los **datos-firmados** pueden incluir:

- cualquiera de los siguientes argumentos: el **identificador-algoritmo-confidencialidad-contenido**, la **verificación-integridad-contenido**, la **etiqueta-seguridad-mensaje**, y la **prueba-de-petición-entrega**; y
- **un número-secuencia-mensaje**, que identifique la posición del mensaje en una secuencia de mensajes del originador al destinatario al que se refiere el **testigo-mensaje** (para proporcionar el elemento-de-servicio de integridad de secuencia de mensajes, definido en la Recomendación X.400.)

Si el **testigo-mensaje** es un **testigo-asimétrico**, los **datos-cifrados** pueden incluir:

- una **clave-confidencialidad-contenido**: clave-encripción simétrica utilizada con el **identificador-algoritmo-confidencialidad-contenido** por el originador del mensaje para cifrar el **contenido** del mensaje y por el destinatario del mensaje para descifrar el **contenido** del mensaje; y/o
- la **verificación-integridad-contenido**: puede incluirse en los **datos-cifrados**, en vez de en los **datos-firmados**, si se requiere confidencialidad de la **verificación-integridad-contenido** y/o si la **etiqueta-seguridad-mensaje** se incluye en los **datos-cifrados** (para confidencialidad de la **etiqueta-seguridad-mensaje**) y debe mantenerse la asociación entre la **verificación-integridad-contenido** y la **etiqueta-seguridad-mensaje**;
- la **etiqueta-seguridad-mensaje**: puede incluirse en los **datos-cifrados**, en vez de en los **datos-firmados**, si se requiere confidencialidad de la **etiqueta-seguridad-mensaje**;
- una **clave-integridad-contenido**: clave-encripción-simétrica utilizada con el **identificador-algoritmo-integridad-contenido**, por el originador del mensaje para calcular la **verificación-integridad-contenido**; y por el destinatario para validar la **verificación-integridad-contenido**;
- un **número-secuencia-mensaje**: definido para los **datos-firmados** anteriormente, pero que puede incluirse en los **datos-encriptados** si se requiere confidencialidad de la secuencia.

Si el **testigo-mensaje** es un **testigo-asimétrico** y los **datos-firmados** del **testigo-mensaje** incluyen la **verificación-integridad-contenido**, el **testigo-mensaje** proporciona el no-repudio-del-origen del **contenido** del mensaje (elemento-de-servicio de no repudio del origen, definido en la Recomendación X.400). Si los **datos-firmados** del **distintivo-mensaje** incluyen tanto la **integridad-verificación-contenido** como la **etiqueta-seguridad-mensaje**, el **testigo-mensaje** proporciona una prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el **contenido** del mensaje.

8.2.1.1.1.27 *Identificador-algoritmo-confidencialidad-contenido*

Este argumento contiene un **identificador-algoritmo**, que identifica el algoritmo utilizado por el originador del mensaje para cifrar el **contenido** del mensaje (para proporcionar el elemento-de-servicio confidencialidad de contenido definido en la Recomendación X.400). Puede generarse por el originador del mensaje.

El algoritmo puede utilizarse por el destinatario o destinatarios del mensaje para descifrar el **contenido** del mensaje.

El algoritmo de confidencialidad-contenido puede ser un algoritmo-cifrado-simétrico o asimétrico.

Si se utiliza un algoritmo-cifrado-simétrico, la **clave-confidencialidad-contenido** utilizada para cifrar el **contenido** del mensaje, y que el destinatario puede utilizar para descifrar el **contenido** del mensaje, puede deducirse del **distintivo-mensaje** enviado con el mensaje. Como alternativa, puede distribuirse por algún otro medio la **clave-confidencialidad-contenido**.

Si se utiliza un algoritmo-cifrado-asimétrico, la clave-cifrado-pública asimétrica del destinatario deseado puede ser utilizada por el originador del mensaje para descifrar el **contenido** del mensaje. El destinatario puede utilizar la clave-cifrado-asimétrica-secreta del destinatario para descifrar el **contenido** del mensaje. Obsérvese que si se utiliza un algoritmo-cifrado-asimétrico, el mensaje puede dirigirse únicamente a un único destinatario, o a un conjunto de destinatarios que compartan la misma pareja de claves-cifrado-asimétricas.

8.2.1.1.1.28 *Verificación-integridad-contenido*

Este argumento proporciona al destinatario o destinatarios del mensaje los medios para validar que no se ha modificado el **contenido** del mensaje (para proporcionar el elemento-de-servicio integridad de contenido definido en la Recomendación X.400). Puede ser generado por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

La **verificación-integridad-contenido** permite validar la integridad-contenido destinatario por cada destinatario utilizando un algoritmo-cifrado-simétrico-asimétrico. Obsérvese que la **verificación-autenticación-origen-mensaje** proporciona los medios para validar la integridad-contenido mensaje por mensaje utilizando un algoritmo-cifrado-asimétrico.

La **verificación-integridad-contenido** puede incluirse en los **datos-firmados** o en los **datos-cifrados** del **distintivo-mensaje** para permitir el no-repudio-del-origen del **contenido** del mensaje, y la prueba de asociación entre la **etiqueta-seguridad-mensaje** y el **contenido** del mensaje.

La **verificación-integridad-contenido** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-integridad-contenido** (un **identificador-algoritmo**).

La **verificación-integridad-contenido** contiene el **identificador-algoritmo-integridad-contenido**, y una función cifrada (por ejemplo una versión resumida o desmenuzada) del **identificador-algoritmo-integridad-contenido** y del **contenido** del mensaje. Obsérvese que la **verificación-integridad-contenido** se calcula utilizando el **contenido** del mensaje claro (es decir sin cifrar).

El algoritmo-integridad-contenido puede ser un algoritmo-cifrado- simétrico o asimétrico. Obsérvese que la utilización de un algoritmo-cifrado- simétrico puede permitir una compresión y cifrado simultáneos del **contenido** del mensaje.

Si se utiliza un algoritmo-cifrado-simétrico, la **clave-integridad-contenido** utilizada para calcular la **verificación-integridad-contenido**, y que puede utilizar el destinatario para validar la **verificación-integridad- contenido**, puede deducirse del **distintivo-mensaje** enviado con el mensaje. Como alternativa, la **clave-integridad-contenido** puede distribuirse por varios otros procedimientos.

Si se utiliza un algoritmo-cifrado-asimétrico, la clave-cifrado-asimétrica-secreta del originador puede utilizarse por el originador del mensaje para calcular la **verificación-integridad-contenido**. El destinatario puede utilizar la clave-encripción-pública-asimétrica del originador (**clave-pública-sujeto**) deducida del **certificado-originador** para validar la **verificación-integridad-contenido**.

8.2.1.1.1.29 *Verificación-autenticación-origen-mensaje*

Este argumento proporciona al destinatario o destinatarios del mensaje, y a cualquier ATM a través del cual se transfiera un mensaje, los medios para autenticar el origen del mensaje (para proporcionar el elemento-de-servicio autenticación de origen de mensaje definido en la Recomendación X.400). Puede generarse por el identificador del mensaje.

La **verificación-autenticación-origen-mensaje** proporciona la prueba del origen del mensaje (autenticación del origen del mensaje), garantía de que el **contenido** del mensaje no ha sido modificado (el elemento-de-servicio integridad de contenido definido en la Recomendación X.400), y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el mensaje.

La **verificación-autenticación-origen-mensaje** se calcula utilizando el algoritmo (algoritmo-cifrado-asimétrico y función-desmenuzar) identificada por el **identificador-algoritmo-autenticación-origen-mensaje** (un **identificador-algoritmo**).

La **verificación-autenticación-origen-mensaje** contiene el **identificador-algoritmo-autenticación-origen-mensaje**, y una versión cifrada, desmenuzada del **identificador-algoritmo-autenticación-origen-mensaje**, el **contenido** del mensaje, el **identificador-contenido** y la **etiqueta-seguridad-mensaje**. Se incluyen componentes facultativos en la **verificación-autenticación-origen-mensaje** si están presentes en el mensaje.

Si se utiliza igualmente la confidencialidad-contenido (véase el § 8.2.1.1.1.27), se calcula **verificación-autenticación-origen-mensaje** utilizando la versión cifrada del **cotenido** del mensaje (para permitir que la **verificación-autenticación-origen-mensaje** sea validada por otro que no sea el destinatario-deseado (por ejemplo por un ATM) sin comprometer la confidencialidad del **contenido** del mensaje). Obsérvese que si la versión clara (es decir sin cifrar) del **contenido** del mensaje se utiliza para calcular la **verificación-autenticación-origen-mensaje**, ésta facilita la autenticación del origen del mensaje y el no repudio del origen del **contenido** del mensaje (firma), definidos en la Recomendación X.400. Sin embargo, si se utiliza la versión cifrada del **contenido** del mensaje, la **verificación-autenticación-origen-mensaje** facilita la autenticación del origen del mensaje, pero no el no repudio del origen del **contenido** del mensaje.

El originador del mensaje puede calcular **verificación-autentificación-origen-mensaje** utilizando la clave-cifrado-secreta-asimétrica del originador. La **verificación-autenticación-origen-mensaje** puede validarse por el destinatario o destinatarios del mensaje, y por cualquier ATM a través del cual se transfiere el mensaje, utilizando la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del originador del mensaje deducida a partir del **certificado-originador**.

Futuras versiones de esta Recomendación pueden definir otras formas de **verificación-autenticación-origen-mensaje** (por ejemplo basadas en técnicas-cifrado-simétricas) que pueden ser utilizadas por los ATM a través de los cuales se transfiere el mensaje para autenticar el origen del mensaje.

8.2.1.1.1.30 *Etiqueta-seguridad-mensaje*

Este argumento asocia una **etiqueta-seguridad** al mensaje (o sonda). Puede ser generado por el originador del mensaje (o sonda), en línea con la política-seguridad en vigor.

La **etiqueta-seguridad-mensaje** de un informe será la misma que la **etiqueta-seguridad-mensaje** del mensaje sujeto (o sonda-).

Si se asignan **etiquetas-seguridad** a los usuarios-STRM, a los ATM y a otros objetos del STM, el tratamiento, por estos objetos, de mensajes, sondas e informes que transportan **etiquetas-seguridad-mensaje** puede determinarse por la política-seguridad en vigor. Si no se asignan **etiquetas-seguridad** a los usuarios STRM, a los ATM y a otros objetos del STM, el tratamiento, por estos objetos, de los mensajes, sondas e informes que transportan **etiquetas-seguridad-mensaje** puede ser discrecional.

Si establecen **contextos-seguridad** entre el originador y un ATM (el ATM-que-origina) del STRM (véanse los § 8.1.1.1.1.3 y 8.2.1.4.1.5), la **etiqueta-seguridad-mensaje** que puede asignar el originador a un mensaje (o sonda) puede determinarse por el **contexto-seguridad** (contexto-seguridad-remisión), en línea con la política-seguridad en vigor. Si no se establecen **contextos-seguridad** entre el originador y el ATM-que-origina, la asignación de una **etiqueta-seguridad-mensaje** a un mensaje (o sonda) puede quedar a la discreción del originador.

Si se establecen **contextos-seguridad** entre dos ATM (véase el § 12.1.1.1.1.3), la transferencia de mensajes, sondas o informes entre los ATM puede determinarse por las **etiquetas-seguridad-mensaje** de los mensajes, sondas o informes, y el **contexto-seguridad**, en línea con la política-seguridad en vigor. Si no se establecen **contextos-seguridad** entre los ATM, la transferencia de mensajes, sondas e informes puede quedar a la discreción del emisor.

Si se establecen **contextos-seguridad** entre un usuario-STRM y un ATM (ATM-que-entrega) del STRM (véanse los § 8.1.1.1.1.3 y 8.3.1.3.1.7), la entrega de mensajes e informes puede determinarse por las **etiquetas-seguridad-mensaje** de los mensajes e informes y el **contexto-seguridad** (contexto-seguridad-entrega), en línea con la política-seguridad en vigor. Si las **etiquetas-seguridad-usuario** registradas del destinatario autorizan la **etiqueta-seguridad-mensaje** de un mensaje o informe, pero el **contexto-seguridad** corriente del destinatario (contexto-seguridad-entrega) no la autoriza, entonces al ATM-que-entrega puede retener-para-entrega. Si no se establecen los **contextos-seguridad** entre los usuarios STRM y el ATM-que-entrega, la entrega de mensajes e informes puede realizarse a discreción del ATM-que-entrega.

8.2.1.1.1.31 *Petición-prueba-de-remisión*

Este argumento indica si el originador del mensaje solicita la **prueba-de-remisión** (para proporcionar el elemento-de-servicio prueba de remisión) definida en la Recomendación X.400 del mensaje al STRM. Puede ser generado por el originador del mensaje.

Este argumento puede tener uno de los siguientes valores: **prueba-de-remisión-solicitada** o **prueba-de-remisión-no-solicitada**.

En ausencia de este argumento se supondrá que el valor por defecto es **prueba-de-remisión-no-solicitada**.

8.2.1.1.1.32 *Petición de prueba-de-entrega*

Este argumento indica si el originador del mensaje solicita **prueba-de-entrega** (para proporcionar el elemento-de-servicio prueba de entrega) definida en la Recomendación X.400 del mensaje al destinatario. Puede ser generado por el originador del mensaje. Puede especificarse un valor distinto de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno de los siguientes valores: **prueba-de-entrega-solicitada** o **prueba-de-entrega-no-solicitada**.

En ausencia de este argumento se supondrá que el valor por defecto es **prueba-de-entrega-no-solicitada**.

8.2.1.1.1.33 *Tipos-información-codificada-originales*

Este argumento identifica los **tipos-información-codificada** originales del **contenido** del mensaje. Puede generarse por el originador del mensaje.

La ausencia de este argumento indica que los **tipos-de-información-codificada-originales** del **contenido** del mensaje están **sin especificar**.

8.2.1.1.1.34 *Tipo-contenido*

Este argumento identifica el tipo de **contenido** del mensaje. Será generado por el originador del mensaje. El **tipo-contenido** será o incorporado o ampliado.

Un **tipo-contenido** incorporado puede tener uno de los siguientes valores:

- **sin identificar**: designa un **tipo-contenido** sin identificar y sin limitación; la utilización de este **tipo-contenido sin identificar** constituye un acuerdo bilateral entre usuarios STRM;
- **externo**: designa un **tipo-contenido** que se reserva para el interfuncionamiento entre sistemas 1988 y sistemas 1984 (véase la Recomendación X.419);
- **mensajería-interpersonal-1984**: identifica el **tipo-contenido** de la **mensajería-interpersonal-1984** definido en la Recomendación X.420;

- **mensajería-interpersonal-1988**: identifica el **tipo-contenido** de la **mensajería-interpersonal-1988** definido en la Recomendación X.420;
- un valor específico de un **tipo-contenido** ampliado definido en esta Recomendación es **sobre-interior**: **tipo-contenido-ampliado** que es un mensaje en sí mismo (sobre y contenido), para ser enviado por el destinatario indicado en el sobre-exterior a los indicados en el sobre-interior. El tipo del **contenido** OCTET STRING es una **UDPA-STRM** codificada utilizando las reglas de codificación básica de la NSA.1. [Obsérvese que el sobre-interior y el contenido pueden protegerse introduciendo seguridad en el **contenido** del sobre-exterior utilizando los argumentos de seguridad (véanse los § 8.2.1.1.1.25 y 8.2.1.1.1.32).]

Pueden definirse otros **tipos-contenido-ampliado** normalizados en futuras versiones de esta Recomendación. Pueden utilizarse otros valores de este argumento mediante acuerdos bilaterales entre usuarios-STRM.

8.2.1.1.1.35 *Identificador-contenido*

Este argumento contiene un identificador del **contenido** del mensaje. Puede generarse por el originador del mensaje.

El **identificador-contenido** puede ser entregado al destinatario o destinatarios del mensaje, y devuelto al originador con algún informe o informes. Este argumento no es alterado por el STRM.

8.2.1.1.1.36 *Correlador-contenido*

Este argumento contiene información que permite al originador del mensaje efectuar la correlación del **contenido** del mensaje. Puede generarse por el originador del mensaje.

El **correlador-contenido** no puede ser entregado al destinatario o destinatarios del mensaje, pero se devuelve al originador con algún informe o informes. Este argumento no debe ser modificado o suprimido por otro que no sea el originador del mensaje.

8.2.1.1.1.37 *Contenido*

Este argumento contiene la información del mensaje que se pretende transportar al destinatario o destinatarios. Será generado por el originador del mensaje.

Excepto cuando se realiza una conversión, el STRM no modifica el **contenido** del mensaje; al contrario éste pasa de forma transparente a través de él.

El **contenido** puede ser cifrado para asegurar su confidencialidad (véase el § 8.2.1.1.1.27).

El **contenido** puede ser un **contenido-externo**. El **contenido** es un **contenido-externo** cuando el argumento del **tipo-contenido** tiene el valor **externo**. Cuando el **contenido** es un **contenido-externo**, se especifica el **tipo-contenido-externo** mediante el identificador del objeto de **contenido-externo**. Un **contenido-externo** puede utilizarse para transportar un **sobre-interior** (véase el § 8.2.1.1.1.34), o para el interfuncionamiento entre sistemas 1988 y sistemas 1984 (véase la Recomendación X.419).

8.2.1.1.2 *Resultados*

El cuadro 5/X.411 enumera los resultados de la operación-abstracta remisión-mensaje, y para cada resultado califica su presencia e identifica el punto en la que se define el resultado.

CUADRO 5/X.411

Resultados de la operación-abstracta remisión-mensaje

Resultado	Presencia	Punto
Identificador-remisión-mensaje	O	8.2.1.1.2.1
Tiempo-remisión-mensaje	O	8.2.1.1.2.2
Certificado-ATM-que-origina	F	8.2.1.1.2.3
Prueba-de-remisión	C	8.2.1.1.2.4
Identificador-contenido	C	8.2.1.1.1.35

8.2.1.1.2.1 *Identificador-remisión-mensaje*

Este resultado contiene un **identificador-STRM** que identifica inequívocamente la remisión-mensaje. Debe ser generado por el STRM.

El STRM proporciona el **identificador-remisión-mensaje** al notificar, al usuario-STRM, la entrega o la no-entrega del mensaje, a través de la operación abstracta entrega-informe.

El usuario-STRM proporciona el **identificador-remisión-mensaje** al cancelar un mensaje cuya entrega estaba diferida, a través de la operación-abstracta cancelación-entrega-diferida.

8.2.1.1.2.2 *Tiempo-remisión-mensaje*

Este resultado indica el **tiempo** en que el STRM acepta la responsabilidad del mensaje. Debe ser generado por el STRM.

8.2.1.1.2.3 *Certificado-ATM-que-origina*

Este resultado contiene el **certificado** del ATM en el que se ha depositado el mensaje (ATM-que-origina). Debe ser generado por una fuente de confianza (por ejemplo una autoridad-certificación), y puede suministrarse por el ATM-que-origina, si el originador del mensaje solicitó una **prueba-de-remisión** (véase el § 8.2.1.1.1.31) y se utiliza un algoritmo-cifrado-asimétrico para calcular la **prueba-de-remisión**.

Puede utilizarse el **certificado-ATM-que-origina** para enviar al originador del mensaje una copia verificada de la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del ATM-que-origina.

El originador del mensaje puede utilizar la clave-cifrado-pública-asimétrica de los ATM-que-originan para validar la **prueba-de-remisión**.

8.2.1.1.2.4 *Prueba-de-remisión*

Este resultado proporciona al originador del mensaje la prueba de remisión del mensaje al STRM (para proporcionar el elemento-de-servicio prueba de remisión definido en la Recomendación X.400). En función del algoritmo-cifrado utilizado y de la política de seguridad en vigor, este argumento puede proporcionar igualmente el elemento-de-servicio no Repudio de remisión (definido en la Recomendación X.400). Debe ser generado por el ATM-que- origina del STRM, si el originador del mensaje solicitó la **prueba-de-remisión** (véase el § 8.2.1.1.1.31).

Se calcula la **prueba-de-remisión** utilizando el algoritmo identificado por el **identificador-algoritmo-prueba-de-remisión** (un **algoritmo-identificador**).

La **prueba-de-remisión** contiene el **identificador-algoritmo-prueba-de-remisión**, y una función cifrada (por ejemplo una versión comprimida o desmenuzada) del **identificador-algoritmo-prueba-de-remisión**, los argumentos del mensaje remitido (véase el § 8.2.1.1.1), y el **identificador-remisión-mensaje** y el **tiempo-remisión-mensaje**. En la **prueba-de-remisión** se incluyen los componentes facultativos si están presentes en el mensaje.

Obsérvese que la recepción de este resultado proporciona al originador del mensaje la prueba de remisión del mensaje. La no-recepción de este resultado no proporciona ni la prueba de remisión ni la prueba de no-remisión (a menos que se utilicen un enlace seguro y una funcionalidad de confianza).

Si se utiliza un algoritmo-cifrado-asimétrico, el ATM-que-origina puede calcular la **prueba-de-remisión**, utilizando la clave-cifrado-asimétrica-secreta del ATM-que-origina. El originador del mensaje puede validar la **prueba-de-remisión** utilizando la clave-cifrado-pública-asimétrica del ATM-que-origina (**clave-pública-sujeto**) deducida del **certificado-ATM-que-origina**. Puede proporcionarse igualmente una **prueba-de-remisión** para el no-Repudio de remisión.

Si se utiliza un algoritmo-cifrado-simétrico, la clave cifrado-simétrica que el ATM-que-origina utilizó para calcular la **prueba-de-remisión**, y que el originador puede utilizar para validar la **prueba-de-remisión**, puede deducirse a partir de los **testigos-vinculación** (véanse los § 8.1.1.1.1.3 y 8.1.1.1.2.2) intercambiados al iniciar la asociación. Como alternativa, la clave-cifrado-simétrica utilizada para la **prueba-de-remisión** puede intercambiarse por algún otro procedimiento. Obsérvese que si se utiliza un algoritmo-cifrado-simétrico, la **prueba-de-remisión** únicamente puede proporcionar el no Repudio de la remisión si la política-seguridad en vigor proporciona la intervención de una tercera parte que actúe como notario.

8.2.1.1.3 *Errores-abstractos*

El cuadro 6/X.411 enumera los errores abstractos que pueden interrumpir la operación-abstracta remisión-mensaje, y para cada error abstracto identifica el punto donde se define el error-abstracto.

CUADRO 6/X.411

Errores-abstractos de remisión-mensaje

Error-abstracto	Punto
Control-remisión-violado	8.2.2.1
Elemento-de-servicio-no-abonado	8.2.2.2
Originador-inválido	8.2.2.4
Destinatario-indebidamente-especificado	8.2.2.5
Petición-incoherente	8.2.2.7
Error-seguridad	8.2.2.8
Función-crítica-no-admitida	8.2.2.9
Error-vinculación-distante	8.2.2.10

8.2.1.2 *Remisión-sonda*

La operación-abstracta remisión-sonda permite a un usuario-STRM remitir una sonda para determinar si podría transferirse y entregarse un mensaje (mensaje-sujeto) a uno o más usuarios-STRM destinatarios, si éste se presentara.

El éxito de una sonda no garantiza que un mensaje remitido posteriormente pueda ser realmente entregado, sino más bien que en el momento actual el destinatario es válido y el mensaje no tropezaría con obstáculos importantes para la entrega.

Para cualesquiera **nombres-destinatarios** que designe una LD, la operación-abstracta remisión-sonda determina si se produciría una ampliación de la LD especificada (pero no LD anidadas).

Para cualesquiera **nombres-destinatarios** para los cuales se produciría un redireccionamiento, la operación-abstracta remisión-sonda determina si podría transferirse y entregarse el mensaje al destinatario-alternativo.

El usuario-STRM suministra la mayoría de los argumentos utilizados para la remisión-mensaje y la longitud del contenido del mensaje-sujeto. La operación abstracta remisión-sonda no culmina con la entrega a los destinatarios deseados del mensaje-sujeto, sino que establece si probablemente lo haría la operación-abstracta remisión-mensaje.

La ejecución satisfactoria de la operación-abstracta significa que el STRM ha aceptado hacerse cargo de la sonda (pero no que la haya llevado a cabo todavía).

La interrupción de la operación-abstracta por un error-abstracto indica que el STRM no puede hacerse cargo de la sonda.

8.2.1.2.1 *Argumentos*

El cuadro 7/X.411 enumera los argumentos de la operación-abstracta remisión-sonda, y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

8.2.1.2.1.1 *Verificación-autenticación-origen-sonda*

Este argumento proporciona a cualquier ATM a través del cual se transfiere la sonda, los medios para autenticar el origen de la sonda (proporcionar el elemento-de-servicio autenticación del origen de la sonda definido en la Recomendación X.400). Puede generarse por el originador de la sonda.

La **verificación-autenticación-origen-sonda** proporciona la prueba del origen de la sonda (autenticación del origen de la sonda), y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el **identificador-contenido** del mensaje-sujeto.

La **verificación-autenticación-origen-sonda** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-autenticación-origen-sonda** (un **identificador-algoritmo**).

CUADRO 7/X.411

Argumentos de remisión-sonda

Argumento	Presencia	Punto
Argumento del originador		
Nombre-originador	O	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	O	8.2.1.1.1.2
Destinatario-alternativo-autorizado	F	8.2.1.1.1.3
Reasignación-destinatario-prohibida	F	8.2.1.1.1.4
Destinatario-alternativo-solicitado	F	8.2.1.1.1.5
Ampliación-DL-prohibida	F	8.2.1.1.1.6
Argumentos de conversión		
Conversión-implícita-prohibida	F	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	F	8.2.1.1.1.10
Conversión-explícita	F	8.2.1.1.1.11
Argumento de método de entrega		
Método-entrega-solicitado	F	8.2.1.1.1.14
Argumento de entrega física		
Atributos-reproducción-física	F	8.2.1.1.1.20
Argumento de petición de informes		
Petición-informe-originador	O	8.2.1.1.1.22
Argumentos de seguridad		
Certificado-originador	F	8.2.1.1.1.25
Comprobación-autenticación-origen-sonda	F	8.2.1.2.1.1
Etiqueta-seguridad-mensaje	F	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-original	F	8.2.1.1.1.33
Tipo-contenido	O	8.2.1.1.1.34
Identificador-contenido	F	8.2.1.1.1.35
Correlador-contenido	F	8.2.1.1.1.36
Longitud-contenido	F	8.2.1.2.1.2

La **verificación-autenticación-origen-sonda** contiene el **identificador-algoritmo-autenticación-origen-sonda**, y una versión cifrada asimétricamente, desmenuzada del **identificador-algoritmo-autenticación-origen-sonda**, el **identificador-contenido** y la **etiqueta-seguridad-mensaje** del mensaje-sujeto. En la **verificación-autenticación-origen-sonda** se incluyen componentes facultativos si éstos están presentes en la sonda.

El originador de la sonda puede calcular la **verificación-autenticación-origen-sonda** utilizando la clave-cifrado-secreta-asimétrica del originador. La **verificación-autenticación-origen-sonda** puede validarse por cualquier ATM a través del cual se transfiere el mensaje, utilizando la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del originador del mensaje deducida a partir del **certificado-originador**.

Futuras versiones de esta Recomendación pueden definir otras formas de **verificación-autenticación-origen-sonda** (por ejemplo, basadas en técnicas-cifrado-simétricas) que pueden ser utilizadas por los ATM a través de los cuales se transfiere el mensaje para autenticar el origen de la sonda.

8.2.1.2.1.2 *Longitud-contenido*

Este argumento especifica la longitud, en octetos, del **contenido** del mensaje-sujeto. Puede generarse por el originador de la sonda.

8.2.1.2.2 *Resultados*

El cuadro 8/X.411 enumera los resultados de la operación-abstracta remisión-sonda, y para cada resultado califica su presencia e identifica el punto donde se define el resultado.

CUADRO 8/X.411

Resultados de remisión-sonda

Resultado	Presencia	Punto
Identificador-remisión-sonda	O	8.2.1.2.2.1
Tiempo-remisión-sonda	O	8.2.1.2.2.2
Identificador-contenido	C	8.2.1.1.1.35

8.2.1.2.2.1 *Identificador-remisión-sonda*

Este resultado contiene un **identificador-STRM** que identifica de forma inequívoca la remisión-sonda. Debe ser generado por el STRM.

El STRM proporciona el **identificador-remisión-sonda**, al notificar al usuario-STRM, de su capacidad o incapacidad para entregar el mensaje-sujeto, a través de la operación-abstracta de entrega-informe.

8.2.1.2.2.2 *Tiempo-remisión-sonda*

Este resultado indica el **tiempo** en que el STRM acepta la responsabilidad de la sonda. Debe ser generado por el STRM.

8.2.1.2.3 *Errores abstractos*

El cuadro 9/X.411 enumera los errores abstractos que pueden interrumpir la operación-abstracta remisión-sonda, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 9/X.411

Errores-abstractos de remisión-sonda

Error-abstracto	Punto
Control-remisión-violado	8.2.2.1
Elemento-de-servicio-no-abonado	8.2.2.2
Originador-inválido	8.2.2.4
Destinatario-indebidamente-especificado	8.2.2.5
Petición-incoherente	8.2.2.7
Error-seguridad	8.2.2.8
Función-crítica-no-admitida	8.2.2.9
Error-vinculación-distante	8.2.2.10

8.2.1.3 *Cancelación-entrega-diferida*

La operación-abstracta cancelación-entrega-diferida permite a un usuario-STRM abortar la entrega-diferida de un mensaje previamente remitido a través de la operación-abstracta remisión-mensaje.

El usuario-STRM identifica el mensaje cuya entrega debe cancelarse mediante el **identificador-remisión-mensaje** devuelto por el STRM como resultado de una invocación previa de la operación-abstracta remisión-mensaje.

La ejecución satisfactoria de la operación-abstracta significa que el STRM ha cancelado la entrega-diferida del mensaje.

La interrupción de la operación-abstracta por un error-abstracto indica que la entrega-diferida del mensaje no puede cancelarse. La entrega-diferida de un mensaje no puede cancelarse si el mensaje ya ha progresado para su entrega y/o transferencia dentro del STRM. El STRM puede rehusar el cancelar la entrega-diferida de un mensaje, si el STRM proporcionó al originador del mensaje la **prueba-de-remisión**.

8.2.1.3.1 *Argumentos*

El cuadro 10/X.411 enumera los argumentos de la operación-abstracta cancelación-entrega-diferida y, para cada argumento califica la presencia e identifica el punto donde se define el argumento.

CUADRO 10/X.411

Argumentos de cancelación entrega-diferida

Argumento	Presencia	Punto
Argumento de remisión		
Identificador-remisión-mensaje	O	8.2.1.3.1.1

8.2.1.3.1.1 *Identificador-remisión-mensaje*

Este argumento contiene el **identificador-remisión-mensaje** del mensaje cuya entrega diferida debe ser cancelada. Debe ser suministrado por el usuario-STRM.

El STRM devuelve el **identificador-remisión-mensaje** (un **identificador-STRM**) como resultado de una invocación previa de la operación-abstracta remisión-mensaje (véase el § 8.2.1.1.2.1), cuando se presentó el mensaje para entrega-diferida.

8.2.1.3.2 *Resultados*

La operación-abstracta cancelación-entrega-diferida devuelve un resultado vacío como indicación de éxito.

8.2.1.3.3 *Errores-abstractos*

El cuadro 11/X.411 enumera los errores abstractos que pueden interrumpir la operación-abstracta cancelación-entrega-diferida, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 11/X.411

Errores-abstractos de cancelación-entrega-diferida

Error-abstracto	Punto
Cancelación-entrega-diferida-rechazada	8.2.2.3
Identificador-remisión-mensaje-inválido	8.2.2.6
Error-vinculación-distante	8.2.2.10

8.2.1.4 *Control-remisión*

La operación-abstracta control-remisión permite al STRM limitar transitoriamente las operaciones-abstractas puerto-remisión que puede invocar el usuario-STRM, y los mensajes que el usuario-STRM puede remitir al STRM a través de la operación-abstracta remisión-mensaje.

El usuario-STRM debe retener hasta un tiempo posterior, en vez de abandonar, las operaciones-abstractas y los mensajes prohibidos actualmente.

La ejecución satisfactoria de la operación-abstracta significa que los controles especificados están actualmente en vigor. Estos controles sobreseen cualquier otro en vigor, y permanecen vigentes hasta que se libera la asociación o el STRM reinvoca la operación-abstracta control-remisión.

La operación-abstracta devuelve una indicación de cualquier operación-abstracta que pudiera invocar el usuario-STRM, o cualquier tipo de mensaje que el usuario-STRM pudiera remitir, a no ser por los controles que prevalecen.

8.2.1.4.1 *Argumentos*

El cuadro 12/X.411 enumera los argumentos de la operación-abstracta control-remisión, y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

CUADRO 12/X.411

Argumentos de control-remisión

Argumento	Presencia	Punto
Argumentos de control-remisión		
Limitación	F	8.2.1.4.1.1
Operaciones-admisibles	F	8.2.1.4.1.2
Prioridad-inferior-admisible	F	8.2.1.4.1.3
Longitud-contenido-máxima-admisible	F	8.2.1.4.1.4
Contexto-seguridad-admisible	F	8.2.1.4.1.5

8.2.1.4.1.1 *Limitación*

Este argumento indica si los controles sobre las operaciones puerto-remisión deben actualizarse o suprimirse. Puede generarse por el STRM.

Este argumento puede tener uno de los siguientes valores:

- **actualización**: los otros argumentos actualizan los controles que prevalecen;
- **supresión**: todos los controles deben suprimirse; los otros argumentos deben ignorarse.

En ausencia de este argumento, se supondrá el valor por defecto de **actualización**.

8.2.1.4.1.2 *Operaciones-admisibles*

Este argumento indica las operaciones-abstractas que el usuario-STRM puede invocar sobre el STRM. Puede generarse por el STRM.

Este argumento puede tener el valor **autorizado** o **prohibido** para cada uno de los siguientes:

- **remisión-mensaje**: el usuario-STRM puede/no puede invocar la operación-abstracta remisión-mensaje; y
- **remisión-sonda**: el usuario-STRM puede/no puede invocar la operación-abstracta remisión-sonda.

Otras operaciones-abstractas de puerto-remisión no están sujetas a controles, y pueden invocarse en cualquier momento.

En ausencia de este argumento, las operaciones-abstractas que puede invocar el usuario-STRM permanecen sin cambios. Si no estaba en vigor ningún control previo, el usuario-STRM puede invocar tanto la operación-abstracta remisión-mensaje como la operación-abstracta remisión-sonda.

8.2.1.4.1.3 *Prioridad-inferior-admisible*

Este argumento contiene la **prioridad** del mensaje de prioridad más baja que el usuario-STRM debe remitir al STRM a través de la operación-abstracta remisión-mensaje. Puede generarse por el STRM.

Este argumento puede tener uno de los siguientes valores del argumento de **prioridad** de la operación-abstracta de remisión-mensaje: **normal, no urgente** o **urgente.**

En ausencia de este argumento, la **prioridad** del mensaje de prioridad más baja que debe remitir el usuario-STRM al STRM permanece sin modificar. Si no está ningún control previo en vigor, el usuario-STRM puede presentar mensajes de cualquier prioridad.

8.2.1.4.1.4 *Longitud-contenido-máxima-admisible*

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el usuario-STRM debe remitir al STRM a través de la operación-abstracta remisión-mensaje. Puede generarse por el STRM.

En ausencia de este argumento, la **longitud-contenido-máxima-admisible** de un mensaje que el usuario-STRM puede remitir al STRM permanece sin modificar. Si no está en vigor ningún control previo, la longitud del contenido no está explícitamente limitada.

8.2.1.4.1.5 *Contexto-seguridad-admisible*

Este argumento limita de forma transitoria la sensibilidad de las operaciones-abstractas de puerto-remisión (contexto-seguridad-remisión) que el usuario-STRM puede invocar en el STRM. Es una limitación transitoria del **contexto-seguridad** establecido al iniciarse la asociación (véase el § 8.1.1.1.1.3). Puede generarse por el STRM.

El **contexto-seguridad-admisible** consta de una o más **etiquetas-seguridad** del conjunto de **etiquetas-seguridad** establecidas como **contexto-seguridad** al establecerse la asociación.

En ausencia de este argumento, el *contexto-seguridad* de las operaciones-abstractas de puerto-remisión permanence sin modificar.

8.2.1.4.2 *Resultados*

El cuadro 13/X.411 enumera los resultados de la operación-abstracta control-remisión, y para cada resultado califica su presencia e identifica el punto donde se define el resultado.

CUADRO 13/X.411

Resultados de control-remisión

Resultado	Presencia	Punto
Resultados «esperando»		
Operaciones-esperando	F	8.2.1.4.2.1
Mensajes-esperando	F	8.2.1.4.2.2
Tipos-información-codificados-esperando	F	8.2.1.4.2.3
Tipos-contenido-esperando	F	8.2.1.4.2.4

8.2.1.4.2.1 *Operaciones-esperando*

Este resultado indica las operaciones-abstractas que retiene el usuario-STRM y que el usuario-STRM invocaría en el STRM si no fuera por los controles que prevalecen. Puede generarse por el usuario-STRM.

Este resultado puede tener el valor **reteniendo** o **no-reteniendo** para cada uno de los siguientes:

- **remisión-mensaje**: el usuario-STRM está/no está reteniendo mensajes, e invocaría la operación-abstracta remisión-mensaje en el STRM si no fuera por los controles que prevalecen; y
- **remisión-sonda**: el usuario-STRM está/no está reteniendo sondas, e invocaría la operación-abstracta remisión-sonda en el STRM si no fuera por los controles que prevalecen.

En ausencia de este resultado, puede suponerse que el usuario-STRM no está reteniendo ningún mensaje ni ninguna sonda para su remisión al STRM debido a los controles que prevalecen.

8.2.1.4.2.2 *Mensajes-esperando*

Este resultado indica la categoría de los mensajes que el usuario-STRM está reteniendo para su remisión al STRM, y que remitiría a través de la operación-abstracta remisión-mensaje, si no fuera por los controles que prevalecen.

Este resultado puede adoptar uno de los siguientes valores:

- **contenido-largo**: el usuario-STRM ha retenido mensajes para su remisión al STRM que exceden el control de **longitud-contenido-máxima-admisible** actualmente en vigor;
- **baja prioridad**: el usuario-STRM ha retenido mensajes para su remisión al STRM de una **prioridad** inferior al control de **prioridad-inferior-admisible** actualmente en vigor;
- **otras-etiquetas-seguridad**: el usuario-STRM ha retenido mensajes para su remisión al STRM, que transportan **etiquetas-seguridad-mensaje** diferentes de las permitidas por el contexto-seguridad actual.

En ausencia de este resultado, puede suponerse que el usuario-STRM no está reteniendo ningún mensaje ni ninguna sonda para su remisión al STRM debido a los controles de **longitud-contenido-máxima-admisible**, **prioridad-inferior-admisible** o **contexto-seguridad-admisible** actualmente en vigor.

8.2.1.4.2.3 *Tipos-información-codificada-esperando*

Este resultado indica los **tipos-información-codificada** del **contenido** de cualquier mensaje retenido por el usuario-STRM para su remisión al STRM debido a los controles que prevalecen. Puede generarse por el usuario-STRM.

En ausencia de este resultado, los **tipos-información-codificada** de cualquier mensaje retenido por el usuario-STRM para su remisión al STRM están **sin-especificar**.

8.2.1.4.2.4 *Tipos-contenido-esperando*

Este resultado indica los **tipos-contenido** de cualquier mensaje retenido por el usuario-STRM para su remisión al STRM debido a los controles que prevalecen. Puede generarse por el usuario-STRM.

En ausencia de este resultado, los **tipos-contenido** de cualquier mensaje retenido por el usuario-STRM para su remisión al STRM están **sin-especificar**.

8.2.1.4.3 *Errores-abstractos*

El cuadro 14/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta control-remisión, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 14/X.411

Errores-abstractos de control-remisión

Error-seguridad	Punto
Error-seguridad	8.2.2.8
Error-vinculación-distante	8.2.2.10

8.2.2 *Errores-abstractos*

En este punto se definen los siguientes errores-abstractos de puerto-remisión:

a) control-remisión-violado
b) elemento-de-servicio-no-abonado
c) cancelación-entrega-diferida-rechazada
d) originador-inválido
e) destinatario-indebidamente-especificado
f) identificador-remisión-mensaje-inválido
g) petición-incoherente
h) error-seguridad
i) función-crítica-no-admitida
j) error-vinculación-distante

8.2.2.1 *Control-remisión-violado*

El error-abstracto de control-remisión-violado informa de la violación, por el usuario-STRM, de un control sobre los servicios de puerto-remisión impuestos por el STRM a través del servicio de control-remisión.

El error-abstracto de control-remisión violado no tiene parámetros.

8.2.2.2 *Elemento-de-servicio-no-abonado*

El servicio de elemento-de-servicio-no-abonado informa que la operación-abstracta solicitada no puede ser proporcionada por el STRM porque el usuario-STRM no está abonado a uno de los elementos-de-servicio que la petición requiere.

El error-abstracto de elemento-de-servicio-no-abonado no tiene parámetros.

8.2.2.3 *Cancelación-entrega-diferida-rechazada*

El error-abstracto de cancelación-entrega-diferida-rechazada informa que el STRM no puede cancelar la entrega-diferida de un mensaje, porque el mensaje ya ha progresado para su transferencia y/o entrega o porque el STRM ha proporcionado al originador una **prueba-de-remisión**.

El error-abstracto de cancelación-entrega-diferida-rechazada no tiene parámetros.

8.2.2.4 *Originador-inválido*

El error-abstracto originador-inválido informa que no puede remitirse el mensaje o la sonda porque el originador está incorrectamente identificado.

El error-abstracto originador-inválido no tiene parámetros.

8.2.2.5 *Destinatario-indebidamente-especificado*

El error-abstracto destinatario-indebidamente-especificado informa que no puede remitirse el mensaje o la sonda porque el destinatario o destinatarios están indebidamente especificados.

El error-abstracto destinatario-indebidamente-especificado tiene los siguientes parámetros generados por el STRM:

– **destinatarios-indebidamente-especificados**: **nombres-destinatarios** indebidamente especificados.

8.2.2.6 *Identificador-remisión-mensaje-inválido*

El error-abstracto identificador-remisión-mensaje-inválido informa que no puede cancelarse una entrega-diferida de un mensaje porque el **identificador-remisión-mensaje** es inválido.

El error-abstracto identificador-remisión-mensaje-inválido no tiene parámetros.

8.2.2.7 *Petición-incoherente*

El error-abstracto petición-incoherente informa que la operación-abstracta solicitada no puede ser proporcionada por el STRM porque el usuario-STRM ha realizado una petición-incoherente.

El error-abstracto petición-incoherente no tiene parámetros.

8.2.2.8 *Error-seguridad*

El error-abstracto error-seguridad informa que la operación-abstracta solicitada no puede ser proporcionada por el STRM porque se violaría la política-seguridad en vigor.

El error-abstracto error-seguridad tiene los siguientes parámetros, generados por el STRM:

– **problema-seguridad**: identificador de la causa de violación de la política-seguridad.

8.2.2.9 *Función-crítica-no-admitida*

El error-abstracto función-crítica-no-admitida informa que un argumento de la operación-abstracta ha sido marcado como **crítico-para-remisión** (véase el § 9.1) pero que no está admitido por el STRM.

El error-abstracto función-crítica-no-admitido no tiene parámetros.

8.2.2.10 *Error-vinculación-distante*

El error-abstracto error-vinculación-distante informa que la operación abstracta solicitada no puede ser proporcionada por la MM debido a que ésta no puede vincularse al STRM. Obsérvese que este error-abstracto sólo se produce en casos de remisión indirecta al STRM a través de una MM.

El error-abstracto error-vinculación-distante no tiene parámetros.

8.3 *Puerto de entrega*

En este punto se definen las operaciones-abstractas y los errores-abstractos que ocurren en un puerto-entrega.

8.3.1 *Operaciones-abstractas*

En este punto se definen las siguientes operaciones-abstractas de puerto-entrega:

a) entrega-mensaje
b) entrega-informe
c) control-entrega.

8.3.1.1 *Entrega-mensaje*

La operación-abstracta entrega-mensaje permite que el STRM entregue un mensaje a un usuario-STRM.

El usuario-STRM no debe rehusar la entrega de un mensaje a menos que la entrega viole las limitaciones de control-entrega entonces en vigor.

8.3.1.1.1 *Argumentos*

El cuadro 15/X.411 enumera los argumentos de la operación-abstracta entrega-mensaje y para cada argumento califica la presencia e identifica el punto donde se define el argumento.

8.3.1.1.1.1 *Identificador-entrega-mensaje*

Este argumento contiene un **identificador-STRM** que distingue el mensaje de todos los demás mensajes en el puerto de entrega. Debe ser generado por el STRM y debe tener el mismo valor que el **identificador-remisión-mensaje** suministrado por el originador del mensaje al remitirse el mensaje.

8.3.1.1.1.2 *Tiempo-entrega-mensaje*

Este argumento contiene el **tiempo** en que se produce la entrega y en que el STRM renuncia a su responsabilidad sobre el mensaje. Debe ser generado por el STRM.

En el caso de entrega física, este argumento indica el **tiempo** en que la UAEF ha tomado la responsabilidad de imprimir y entregar posteriormente el mensaje.

El valor de este argumento debe ser el mismo que el valor del **tiempo-entrega-mensaje** indicado al originador del mensaje (véase el § 8.3.1.2.1.8) en el informe-entrega.

8.3.1.1.1.3 *Nombre-este-destinatario*

Este argumento contiene el **nombre-O/D** del destinatario al que se entrega el mensaje. Debe ser generado por el STRM.

El valor de este argumento debe ser el mismo que el valor del argumento **nombre-destinatario-real** indicado al originador del mensaje (véase el § 8.3.1.2.1.2) en un informe-entrega.

El **nombre-este-destinatario** contiene el **nombre-O/D** del destinatario individual, es decir no debe contener el **nombre-O/D** de una LD.

El **nombre-O/D** del destinatario-deseado (si es diferente, y el mensaje ha sido redirigido) está contenido en el argumento **nombre destinatario deseado.**

8.3.1.1.1.4 *Nombre-destinatario-deseado*

Este argumento contiene el **nombre-O/D** del destinatario-deseado del mensaje, si éste ha sido redirigido, y el momento en que se efectuó el redireccionamiento. Puede generarse por el STRM. Puede existir un valor diferente de este argumento para cada ocasión en que se redirige el mensaje.

Este argumento consta de un **nombre-destinatario-deseado-originalmente** y un **nombre-destinatario-deseado.** En la primera ocasión en que se redirige un mensaje tanto el **nombre-destinatario-deseado-originalmente** como el **nombre-destinatario-deseado** contienen el **nombre-destinatario** especificado-originalmente por el originador del mensaje. Las redirecciones subsiguientes causan ulteriores **nombres-destinatarios** que se añadirán a su vez como apéndice a la lista de **nombres-destinatarios-deseados.**

El **nombre-destinatario-deseado** contiene el **nombre-O/D** de un destinatario individual o de un destinatario deseado de una LD, y el momento en que se redirigió el mensaje a un destinatario alternativo.

ARCHIVES U.I.T. GENÈVE

CUADRO 15/X.411

Argumentos de entrega-mensaje

Argumento	Presencia	Punto
Argumentos de entrega		
Identificador-entrega-mensaje	O	8.3.1.1.1.1
Tiempo-entrega-mensaje	O	8.3.1.1.1.2
Tiempo-presentación-mensaje	O	8.2.1.1.2.2
Argumento del originador		
Nombre-originador	O	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-este-destinatario	O	8.3.1.1.1.3
Nombre-destinatario-deseado	C	8.3.1.1.1.4
Motivo-redireccionamiento	C	8.3.1.1.1.5
Otros-nombres-destinatarios	C	8.3.1.1.1.6
Historia-ampliación-LD	C	8.3.1.1.1.7
Argumento de prioridad		
Prioridad	C	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Tipos-información-codificada-convertidos	C	8.3.1.1.1.8
Argumento de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	C	8.2.1.1.1.15
Petición-dirección-envío-físico	C	8.2.1.1.1.16
Modos-entrega-física	C	8.2.1.1.1.17
Tipo-correo-certificado	C	8.2.1.1.1.18
Número-destinatario-para-aviso	C	8.2.1.1.1.19
Atributos-reproducción-física	C	8.2.1.1.1.20
Dirección-devolución-originador	C	8.2.1.1.1.21
Petición-informe-entrega-física	C	8.2.1.1.1.24
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Testigo-mensaje	C	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	C	8.2.1.1.1.27
Verificación-integridad-contenido	C	8.2.1.1.1.28
Verificación-autenticación-origen-mensaje	C	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Petición-prueba-de-entrega	C	8.2.1.1.1.32
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	O	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Contenido	O	8.2.1.1.1.37

8.3.1.1.1.5 *Motivo-redireccionamiento*

Este argumento indica el motivo de que se haya redirigido el mensaje a un destinatario-alternativo. Debe ser generado por el STRM en cada ocasión en que se produce un redireccionamiento. Puede existir un valor diferente de este argumento para cada ocasión en que se redirige el mensaje.

Este argumento puede tener uno de los siguientes valores:

- **destinatario-alternativo-asignado-destinatario**: el destinatario-deseado del mensaje solicitó que se redirigiera el mensaje a un **destinatario-alternativo-asignado-destinatario**; el originador del mensaje no prohibió una reasignación-destinatario (véase el § 8.2.1.1.1.4); el STRM redirige el mensaje al **destinatario-alternativo-asignado-destinatario**;
- **destinatario-alternativo-solicitado-originador**: el mensaje no pudo entregarse al destinatario-deseado o al **destinatario-alternativo-asignado-destinatario** (si está inscrito); el argumento **destinatario-alternativo-solicitado-originador** identificó un destinatario-alternativo solicitado por el originador del mensaje; el STRM redirigió el mensaje al **destinatario-alternativo-solicitado-originador**;
- **destinatario-alternativo-asignado-destinatario-DG**: el argumento **nombre-destinatario** no identificó un usuario-STRM destinatario; el argumento **destinatario-alternativo-autorizado** generado por el originador del mensaje autorizó la entrega a un destinatario-alternativo; el STRM redirigió el mensaje a un destinatario-alternativo asignado por el destinatario-DG para recibir dichos mensajes.

8.3.1.1.1.6 *Otros-nombres-destinatarios*

Este argumento contiene los **nombres-O/D** especificados-originalmente de todos los destinatarios que no sean los identificados por el argumento **nombre-destinatario-deseado-originalmente**, si éste está presente, y el argumento **nombre-este-destinatario**, si el originador del mensaje solicitó la revelación de los otros destinatarios (con el argumento **revelación-de-destinatarios** de la operación-abstracta de remisión-mensaje). Puede generarse por el STRM. Puede existir un valor diferente de este argumento para cada destinatario especificado-originalmente distinto del **nombre-este-destinatario** al cual se entrega el mensaje.

Cada **nombre-otro-destinatario** contiene el **nombre-O/D** de un destinatario individual o de una LD.

8.3.1.1.1.7 *Historia-ampliación-LD*

Este argumento contiene la secuencia de **nombres-O/D** de cualesquiera LD que hayan sido ampliadas para añadir destinatarios a la copia del mensaje entregado al destinatario, y el momento de cada ampliación. Debe ser generado por el STRM si se produjo cualquier ampliación-LD.

8.3.1.1.1.8 *Tipos-información-codificada-convertida*

Este argumento identifica los **tipos-información-codificada** del **contenido** del mensaje después de la conversión, si ésta tuvo lugar. Puede generarse por el STRM.

8.3.1.1.2 *Resultados*

El cuadro 16/X.411 enumera los resultados de la operación-abstracta entrega-mensaje, y para cada resultado, califica su presencia e identifica el punto donde se define el resultado.

CUADRO 16/X.411

Resultado de entrega-mensaje

Resultado	Presencia	Punto
Resultados de prueba de entrega		
Certificado-destinatario	F	8.3.1.1.2.1
Prueba-de-entrega	C	8.3.1.1.2.2

8.3.1.1.2.1 *Certificado-destinatario*

Este argumento contiene el **certificado** del destinatario del mensaje. Debe ser generado por una fuente de confianza (por ejemplo, una autoridad-certificación), y puede ser suministrado por el destinatario del mensaje, si el originador del mensaje solicitó una **prueba-de-entrega** (véase el § 8.2.1.1.1.32) y se utiliza un algoritmo-cifrado-asimétrico para calcular la **prueba-de-entrega**.

Puede utilizarse el **certificado-destinatario** para transportar una copia verificada de la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del destinatario del mensaje.

El originador del mensaje puede utilizar la clave-cifrado-pública-asimétrica del destinatario para validar la **prueba-de-entrega**.

8.3.1.1.2.2 *Prueba-de-entrega*

Este argumento proporciona al originador del mensaje una prueba de que se ha entregado el mensaje al destinatario (para proporcionar el elemento-de-servicio prueba de entrega definido en la Recomendación X.400) en función del algoritmo-cifrado utilizado y de la política-seguridad en vigor. Este argumento puede proporcionar igualmente el elemento-de-servicio no repudio de entrega (definido en la Recomendación X.400). Debe ser generado por el destinatario del mensaje, si el originador del mensaje solicitó una **prueba-de-entrega** (véase el § 8.2.1.1.1.32).

La **prueba-de-entrega** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-prueba-de-entrega** (un **identificador-algoritmo**).

La **prueba-de-entrega** contiene el **identificador-algoritmo-prueba-de-entrega** y una función cifrada (por ejemplo, una versión comprimida o desmenuzada) del **identificador-algoritmo-prueba-de-entrega**, el **tiempo-entrega** y el **nombre-este-destinatario**, el **nombre-destinatario-deseado-originalmente** el **contenido** del mensaje, el **identificador-contenido**, y la **etiqueta-seguridad-mensaje** del mensaje entregado. Se incluyen componentes facultativos en la **prueba-de-entrega** si están presentes en el mensaje entregado. Obsérvese que la **prueba-de-entrega** se calcula utilizando el contenido claro (es decir, sin cifrar) del **contenido** del mensaje.

Obsérvese que la recepción de este argumento proporciona al originador del mensaje una prueba de entrega del mensaje al destinatario. La no-recepción de este argumento no proporciona ni la prueba de entrega ni la prueba de no entrega (a menos que se utilice una ruta segura y una funcionalidad de confianza).

Si se utiliza un algoritmo-cifrado-asimétrico, el destinatario del mensaje puede calcular la **prueba-de-entrega** mediante la clave-cifrado-secreta-asimétrica del destinatario. El originador del mensaje puede validar la **prueba-de-entrega** utilizando la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) deducida del **certificado-destinatario**. Una **prueba-de-entrega** asimétrica puede igualmente proporcionar un no repudio de entrega.

Si se utiliza un algoritmo-simétrico, el destinatario utiliza una clave-cifrado-simétrica para calcular la **prueba-de-entrega**, y el originador para validar la **prueba-de-entrega**. Obsérvese que si se utiliza un algoritmo-cifrado-simétrico entonces la **prueba-de-entrega** puede proporcionar únicamente un no repudio de entrega si la política-seguridad en vigor proporciona la intervención de una tercera parte que actúe como notario. Los procedimientos mediante los cuales se distribuye la clave-cifrado-simétrica no se definen en esta Recomendación.

8.3.1.1.3 *Errores-abstractos*

El cuadro 17/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta entrega-mensaje, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 17/X.411

Errores-abstractos de entrega-mensaje

Error-abstracto	Punto
Control-entrega-violado	8.3.2.1
Error-seguridad	8.3.2.3
Función-crítica-no-admitida	8.3.2.4

8.3.1.2 *Entrega-informe*

La operación-abstracta **entrega-informe** permite que el STRM proporcione el acuse de recibo al usuario-STRM de uno o más resultados de una invocación previa de las operaciones-abstractas remisión-mensaje o remisión-sonda.

Para la operación-abstracta remisión-mensaje, la operación-abstracta entrega-informe indica la entrega o no-entrega del mensaje remitido a uno o más destinatarios.

Para la operación-abstracta remisión-sonda, la operación-abstracta entrega-informe indica si podría entregarse un mensaje o producirse una ampliación-LD, si se remitiera el mensaje.

Una invocación sencilla de la operación-abstracta remisión-mensaje o remisión-sonda puede provocar varias apariciones de la operación abstracta entrega-informe, cubriendo cada una de ellas uno o más destinatarios deseados. Una aparición sencilla de la operación-abstracta entrega-informe puede informar tanto sobre la entrega como la no-entrega a diferentes destinatarios.

Una invocación de la operación-abstracta remisión-mensaje o remisión-sonda por un usuario-STRM puede provocar apariciones de la operación-abstracta entrega-informe a otro usuario-STRM, por ejemplo, informes entregados al propietario de una LD.

El usuario-STRM no debe rehusar aceptar la entrega de un informe a menos que la entrega del informe viole las restricciones del control-entrega entonces en vigor.

8.3.1.2.1 *Argumentos*

El cuadro 18/X.411 enumera los argumentos de la operación-abstracta entrega-informe y para cada argumento califica la presencia e identifica el punto donde se define el argumento.

8.3.1.2.1.1 *Identificador-remisión-sujeto*

Este argumento contiene el **identificador-remisión-mensaje** o el **identificador-remisión-sonda** del sujeto del informe. Debe ser suministrado por el STRM.

8.3.1.2.1.2 *Nombre-destinatario-real*

Este argumento contiene el **nombre-O/D** de un destinatario del mensaje. Debe ser generado por el originador del mensaje, o por el STRM si el mensaje ha sido redirigido. Debe especificarse un valor diferente de este argumento para cada destinatario del sujeto al que se refiere el informe.

En el caso de un informe de entrega, el **nombre-destinatario-real** es el nombre del destinatario real del mensaje y tiene el mismo valor que el argumento de **nombre-este-destinatario** del mensaje entregado. En el caso de un informe-no-entrega, el **nombre-destinatario-real** es el **nombre-O/D** del destinatario al que iba dirigido el mensaje cuando se encontró la razón para no-entrega.

El **nombre-destinatario-real** puede ser un **nombre-destinatario** especificado-originalmente, o el **nombre-O/D** de un destinatario alternativo si se ha redirigido el mensaje. Si se ha redirigido el mensaje, el **nombre-O/D** del destinatario-pretendido está contenido en el argumento de **nombre-destinatario-deseado**.

El **nombre-destinatario-real** contiene el **nombre-O/D** de un destinatario individual o de una LD.

8.3.1.2.1.3 *Originador-e-historia-ampliación-LD*

Este argumento contiene una secuencia de **nombres-O/D** e instantes asociados que documentan la historia del origen del mensaje-sujeto. El primer **nombre-O/D** de la secuencia es el **nombre-O/D** del originador del sujeto, y el resto de la secuencia es una secuencia de **nombres-O/D** de las LD que han sido ampliadas al dirigir el sujeto hacia el destinatario (la última es la misma que la **historia-ampliación-LD**). Debe ser generado por el ATM-que-origina del informe si se ha producido cualquier ampliación-LD en el sujeto.

El **originador-e-historia-ampliación-LD** contiene el **nombre-O/D** del originador del sujeto y de cada una de las LD, y el instante en que se ha producido el suceso asociado.

8.3.1.2.1.4 *Nombre-LD-informador*

Este argumento contiene el **nombre-O/D** de la LD que envió el informe al propietario de la LD. Debe ser generado por un punto-ampliación-LD (un ATM) al enviar un informe al propietario de la LD, en línea con la política-informadora de la LD.

El **nombre-LD-informador** contiene el **nombre-O/D** de la LD que envía el informe.

CUADRO 18/X.411

Argumentos de entrega-informe

Argumento	Presencia	Punto
Argumento de remisión de sujeto		
Identificador-remisión-sujeto	O	8.3.1.2.1.1
Argumentos de destinatario		
Nombre-destinatario-real	O	8.3.1.2.1.2
Nombre-destinatario-deseado	C	8.3.1.1.1.4
Motivo-redireccionamiento	C	8.3.1.1.1.5
Originador-e-historia-ampliación-LD	C	8.3.1.2.1.3
Nombre-LD-informador	C	8.3.1.2.1.4
Argumento de conversión		
Tipos-información-codificada-convertidos	C	8.3.1.2.1.5
Argumentos de información suplementaria		
Información-suplementaria	C	8.3.1.2.1.6
Dirección-envío-físico	C	8.3.1.2.1.7
Argumentos de entrega		
Tiempo-entrega-mensaje	C	8.3.1.2.1.8
Tipo-de-usuario-STRM	C	8.3.1.2.1.9
Argumentos de no-entrega		
Código-motivo-no-entrega	C	8.3.1.2.1.10
Código-diagnóstico-no-entrega	C	8.3.1.2.1.11
Argumentos de seguridad		
Certificado-destinatario	C	8.3.1.1.2.1
Prueba-de-entrega	C	8.3.1.1.2.2
Certificado-ATM-informador	C	8.3.1.2.1.12
Comprobación-autenticación-origen-informe	C	8.3.1.2.1.13
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	C	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido-devuelto	C	8.3.1.2.1.14

8.3.1.2.1.5 *Tipos-información-codificada-convertidos*

Este argumento identifica los **tipos-información-codificada** del **contenido** del mensaje-sujeto después de la conversión, si ésta tuvo lugar. Para un informe sobre un mensaje, este argumento indica los **tipos-información-codificada** reales del **contenido** del mensaje convertido. Para un informe sobre una sonda, este argumento indica los **tipos-información-codificada** que el **contenido** del mensaje-sujeto habría contenido después de la conversión, si se hubiera remitido el mensaje-sujeto. Puede generarse por el STRM. Puede especificarse un valor diferente de este parámetro para cada destinatario del sujeto al que se refiere el informe.

8.3.1.2.1.6 *Información-suplementaria*

Este argumento puede contener información suministrada por el originador del informe, como una cadena imprimible. Puede generarse por el ATM-que-origina del informe o una unidad-acceso asociada. Puede especificarse un valor diferente para cada destinatario deseado del sujeto al que se refiere el informe.

Una unidad-acceso-teletex o una facilidad de conversión teletex-télex pueden utilizar la **información-suplementaria**. Ésta puede contener un acuse de recibo recibido, una duración de transmisión télex, o una nota y mensaje registrado recibido como una cadena imprimible.

Otras unidades-acceso o el ATM-que-origina del propio informe pueden utilizar igualmente la **información-suplementaria**, para transportar información imprimible al originador del mensaje.

8.3.1.2.1.7 *Dirección-envío-físico*

Este argumento contiene la nueva **dirección-O/D-postal** del destinatario-físico del mensaje. Puede generarse por la UAEF asociada al ATM-que-origina del informe, si el originador del mensaje solicitó la dirección-envío-físico del destinatario (véase el § 8.2.1.1.1.16). Puede especificarse un valor diferente de este argumento para cada destinatario deseado del mensaje-sujeto a que se refiere el informe.

8.3.1.2.1.8 *Tiempo-entrega-mensaje*

Este argumento contiene el **tiempo** en que se entregó (o se podría haber entregado) el mensaje-sujeto al usuario-STRM destinatario. Debe ser generado por el STRM si el mensaje fue (o se podría haber) entregado satisfactoriamente. Puede especificarse un valor diferente de este argumento para cada destinatario deseado del sujeto a que se refiere el informe.

En el caso de una entrega física, este argumento indica el **tiempo** en que la UAEF ha asumido la responsabilidad de imprimir y posteriormente entregar el mensaje.

Si se entregó el mensaje-sujeto, el valor de este argumento debe ser el mismo que el valor del argumento del **tiempo-entrega-mensaje** del mensaje entregado (véase el § 8.3.1.1.1.2).

8.3.1.2.1.9 *Tipo-de-usuario-STRM*

Este argumento indica el tipo del usuario-STRM destinatario a quien se entregó (o se podría haber entregado) el mensaje satisfactoriamente. Debe ser generado por el STRM si el mensaje se entregó (o se podría haber entregado) satisfactoriamente. Puede especificarse un valor diferente para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tener uno de los siguientes valores:

- **público**: UA que pertenece a una Administración;
- **privado**: UA que pertenece a alguien distinto de una Administración;
- **mm**: memoria de mensaje;
- **LD**: lista-distribución;
- **UAEF**: unidad-acceso-entrega-física (UAEF);
- **destinatario-físico**: destinatario físico de un SEF;
- **otra**: unidad-acceso de otra categoría.

8.3.1.2.1.10 *Código-motivo-no-entrega*

Este argumento contiene un código que indica el motivo de la entrega fallida de un mensaje-sujeto (o, que en el caso de una sonda, habría fallado). Debe ser generado por el STRM, si el mensaje se entregó (o se hubiera entregado) sin éxito. Puede especificarse un valor diferente de este argumento para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tener uno de los siguientes valores:

- **fallo-transferencia**: indica que, mientras que el STRM intentaba entregar o sondear la entrega del mensaje-sujeto, algún fallo de comunicación le impidió hacerlo;
- **incapaz-de-transferir**: indica que, debido a algún problema con el propio sujeto, el STRM no pudo entregar o sondear la entrega del mensaje-sujeto;
- **conversión-no-realizada**: indica que una conversión necesaria para la entrega del mensaje-sujeto no pudo (o no podría) realizarse;
- **reproducción-física-no-realizada**: indica que el UAEF no pudo reproducir físicamente el mensaje-sujeto;

- **entrega-física-no-realizada**: indica que el SEF no pudo entregar físicamente el mensaje-sujeto;
- **entrega-limitada**: indica que el destinatario está abonado al elemento-de-servicio de entrega-limitada (definido en la Recomendación X.400) que impidió (o impediría) la entrega del mensaje sujeto;
- **operación-guía-infructuosa**: indica que el resultado de una operación de guía solicitada no tuvo éxito.

Pueden especificarse otros **códigos-motivo-no-entrega** en futuras versiones de esta Recomendación.

En el argumento **código-diagnóstico-no-entrega** está contenida otra información adicional sobre la naturaleza del problema que impide la entrega.

8.3.1.2.1.11 *Código-diagnóstico-no-entrega*

Este argumento contiene un código que indica la naturaleza del problema que hizo fracasar la entrega o la sonda de entrega del mensaje-sujeto. El motivo del fallo se indica en el argumento del **código-motivo-no-entrega**. Puede generarse por el STRM si se entregó (o se hubiera entregado) el mensaje sin éxito. Puede especificarse un valor diferente de este argumento para cada destinatario-deseado del sujeto a que se refiere el informe.

Este argumento puede tomar uno de los siguientes valores:

- **nombre-O/D-no-reconocido**: el argumento del **nombre-destinatario** del sujeto no contiene un **nombre-O/D** reconocido por el STRM;
- **nombre-O/D-ambiguo**: el argumento del **nombre-destinatario** del sujeto identifica más de un posible destinatario (es decir, es ambiguo);
- **congestión-STRM**: el sujeto no pudo progresar, debido a una congestión en el STRM;
- **bucle-detectado**: se detectó que el sujeto estaba haciendo un bucle dentro del STRM;
- **destinatario-indisponible**: el usuario-STRM destinatario estaba (o estaría) indisponible para recibir la entrega del mensaje-sujeto;
- **tiempo-máximo-expirado**: el tiempo máximo para entregar el mensaje-sujeto, o para realizar la sonda-sujeto, ha expirado;
- **tipos-información-codificada-no-admitidos**: el usuario-STRM destinatario no admite los **tipos-información-codificada** del mensaje-sujeto;
- **contenido-demasiado-largo**: la **longitud-contenido** del mensaje-sujeto es demasiado larga para que el usuario-STRM acepte la entrega (excede la **longitud-contenido-máxima-entregable**);
- **conversión-no-práctica**: la conversión requerida para entregar el mensaje-sujeto no resulta práctica;
- **conversión-implícita-prohibida**: la conversión requerida para entregar el mensaje-sujeto ha sido prohibida por el originador del sujeto (véase el § 8.2.1.1.1.9);
- **conversión-implícita-no-abonada**: el destinatario no se ha abonado a la conversión requerida para entregar el mensaje-sujeto;
- **argumentos-inválidos**: se ha detectado que uno o más argumentos del sujeto son inválidos;
- **error-sintaxis-contenido**: se ha detectado un error de sintaxis en el **contenido** del mensaje-sujeto (no aplicable a las sondas-sujeto);
- **violación-limitación-tamaño**: indica que el valor de uno o más parámetros del sujeto violaron las limitaciones de tamaño definidas en esta Recomendación, y que el STRM no estaba preparado para manejar el valor o valores especificados;
- **violación-protocolo**: indica que faltan uno o más argumentos obligatorios en el sujeto;
- **tipo-contenido-no-admitido**: indica que era (o sería) necesario el procesamiento de un **tipo-contenido** no admitido por el STRM para entregar el mensaje-sujeto;
- **demasiados-destinatarios**: indica que el STRM fue (o sería) incapaz de entregar el mensaje-sujeto debido al número de destinatarios especificados del mensaje-sujeto (véase el § 8.2.1.1.1.2);
- **no-acuerdo-bilateral**: indica que la entrega del mensaje-sujeto exigía (o exigiría) un acuerdo bilateral inexistente;

- **función-crítica-no-admitida**: indica que una función crítica requerida para la transferencia o entrega del mensaje-sujeto no estaba admitida por el ATM-que-origina del informe;
- **conversión-con-pérdida-prohibida**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información; la conversión con pérdida de información fue prohibida por el originador del sujeto (véase el § 8.2.1.1.1.10);
- **línea-demasiado-larga**: la conversión requerida para la entrega del mensaje-sujeto provocaría una pérdida de información porque la longitud de la línea era demasiado larga;
- **página-partida**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información porque se partiría una página original;
- **pérdida-símbolo-pictórico**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más símbolos pictóricos;
- **pérdida-símbolo-puntuación**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más símbolos de puntuación;
- **pérdida-carácter-alfabético**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida de información debido a la pérdida de uno o más caracteres alfabéticos;
- **pérdida-información-múltiple**: la conversión necesaria para la entrega del mensaje-sujeto provocaría una pérdida múltiple de información;
- **reasignación-destinatario-prohibida**: indica que el STRM no pudo (o no podría) entregar el mensaje-sujeto porque el originador del sujeto prohibió el redireccionamiento a un **destinatario-alternativo-asignado-destinatario** (véase el § 8.2.1.1.1.4);
- **bucle-redireccionamiento-detectado**: no pudo redirigirse el mensaje-sujeto a un destinatario-alternativo porque el destinatario había redirigido previamente el mensaje (bucle-redireccionamiento);
- **ampliación-LD-prohibida**: indica que el STRM no pudo (o no podría) entregar el mensaje-sujeto porque el originador del sujeto prohibió la ampliación de las LD (véase el § 8.2.1.1.1.6);
- **no-autorización-depósito-LD**: el originador del sujeto (o de la LD de la que esta LD es miembro, en el caso de LD anidadas) no tiene autorización para depositar mensajes en esta LD;
- **fallo-ampliación-LD**: indica que el STRM no pudo completar la ampliación de esta LD;
- **atributos-reproducción-física-no-admitidos**: el UAEF no admite los atributos-reproducción-física requeridos (véase el § 8.2.1.1.1.20);
- **entrega-física-correo-imposible-dirección-incorrecta**: fue imposible entregar el mensaje-sujeto porque la **dirección-O/D-postal** especificada del destinatario era incorrecta;
- **entrega-física-correo-imposible-oficina-incorrecta-o-inválida**: fue imposible entregar el mensaje-sujeto porque la oficina-entrega física identificada por la **dirección-O/D-postal** especificada del destinatario era incorrecta o inválida (no existe);
- **entrega-física-correo-imposible-dirección-incompleta**: fue imposible entregar el mensaje-sujeto porque la **dirección-O/D-postal** especificada del destinatario estaba incompletamente especificada;
- **correo-imposible-entregar-destinatario-desconocido**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** no era conocido en esa dirección;
- **correo-imposible-entregar-destinatario-fallecido**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** había fallecido;
- **correo-imposible-entregar-organización-desaparecida**: fue imposible entregar el mensaje-sujeto porque el destinarario especificado en la **dirección-O/D-postal** había desaparecido;
- **correo-imposible-entregar-destinatario-rehusó-aceptar**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** rehusó aceptarlo;
- **correo-imposible-entregar-destinatario-no-recogió**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** no recogió el correo;
- **correo-imposible-entregar-destinatario-cambió-dirección-permanente**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** ha cambiado la dirección permanente (se trasladó), y el reenvío no resultó procedente;
- **correo-imposible-entregar-destinatario-cambió-dirección-transitoriamente**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** ha cambiado la dirección transitoriamente (está de viaje), y el reenvío no resultó procedente;
- **correo-imposible-entregar-destinatario-cambió-dirección-transitoria**: fue imposible entregar el mensaje-sujeto porque el destinatario especificado en la **dirección-O/D-postal** había cambiado la dirección temporal («partido»), y el renvío no resultó procedente;
- **correo-imposible-entregar-nueva-dirección-desconocida**: fue imposible entregar el mensaje-sujeto porque el destinatario se había trasladado y la nueva dirección del destinatario era desconocida;
- **correo-imposible-entregar-destinatario-no-deseó-envío**: fue imposible entregar el mensaje-sujeto porque la entrega requeriría un envío-físico que el destinatario no deseó;

- **correo-imposible-entregar-originador-prohibió-envío**: el envío-físico necesario para la entrega del mensaje ha sido prohibido por el originador del mensaje-sujeto (véase el § 8.2.1.1.1.15);
- **error-mensajería-segura**: el sujeto no pudo progresar porque violaría la política-seguridad en vigor;
- **incapaz-de-subgradar**: el sujeto no puede ser transferido porque no puede ser degradado (véase el anexo B a la Recomendación X.419).

Pueden especificarse otros **códigos-diagnóstico-no-entrega** en futuras versiones de esta Recomendación.

8.3.1.2.1.12 *Certificado-ATM-informador*

Este argumento contiene el **certificado** del ATM que ha generado el informe. Debe ser generado por una fuente de confianza (por ejemplo, autoridad de certificación), y puede ser suministrado por el ATM-informador si se suministra una **comprobación-autenticación-origen-informe**.

Puede utilizarse un **certificado-ATM-informador** para transportar una copia verificada de la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) del ATM-informador.

El originador del mensaje y cualquier ATM a través del cual se transfiere el informe pueden utilizar la clave-cifrado-pública-asimétrica del ATM-informador, para validar la **verificación-autenticación-origen-informe**.

8.3.1.2.1.13 *Verificación-autenticación-origen-informe*

Este argumento proporciona al originador del mensaje-sujeto (o sonda-), y a cualquier otro ATM a través del cual se transfiere el informe, los medios para autenticar el origen del informe (para proporcionar el elemento-de-servicio autenticación del origen del informe definido en la Recomendación X.400). Puede ser generado por el ATM-informador si existe una **verificación-autenticación-origen-mensaje (o -sonda)**.

La **verificación-autenticación-origen-informe** proporciona la prueba del origen del informe (autenticación del origen del informe), y la prueba de la asociación entre la **etiqueta-seguridad-mensaje** y el informe.

La **verificación-autenticación-origen-informe** se calcula utilizando el algoritmo identificado por el **identificador-algoritmo-autenticación-origen-informe** (un **identificador-algoritmo**).

La **verificación-autenticación-origen-informe** contiene el **identificador-algoritmo-autenticación-origen-informe**, y una versión cifrada asimétricamente, desmenuzada del **identificador-algoritmo-autenticación-origen-informe**, el **identificador-contenido** y la **etiqueta-seguridad-mensaje** del sujeto, y todos los valores de los argumentos siguientes (por-destinatario): el **nombre-destinatario-real**, el **nombre-destinatario-deseado-originalmente**, y:

- para un informe-entrega: el **tiempo-entrega-mensaje**, el **tipo-de-usuario-STRM**, y si el originador del mensaje lo solicita para los destinatarios a los que se refiere el informe, el **certificado-destinatario**, y la **prueba-de-entrega** (no presente en un informe o sonda); o
- para un informe-no-entrega: el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega**.

Si están presentes en el informe, se incluyen componentes facultativos en la **verificación-autenticación-origen-informe**.

El ATM-informador puede calcular la **verificación-autenticación-origen-informe** utilizando la clave-cifrado-asimétrica del ATM-informador. El originador del sujeto y cualquier ATM a través del cual se transfiera el informe puede validar la **verificación-autenticación-origen-informe** utilizando la clave-cifrado-pública-asimétrica (**clave-pública-sujeto**) deducida a partir del **certificado-ATM-informador**.

Futuras versiones de esta Recomendación pueden definir otras formas de **verificación-autenticación-origen-informe** (por ejemplo, basadas en técnicas-cifrado-simétricas) que pueden utilizar los ATM a través de los cuales se transfieren informes para autenticar el origen del informe.

8.3.1.2.1.14 *Contenido-devuelto*

Este argumento contiene el **contenido** del mensaje-sujeto si el originador del mensaje-sujeto indicó que debe devolverse el **contenido** (véase el § 8.2.1.1.1.23). Debe ser generado por el originador del mensaje, y el STRM puede devolverlo (si el ATM-informador o el ATM-que-origina admite el elemento-de-servicio devolución de contenido).

Este argumento puede estar presente únicamente si existe al menos un informe de no-entrega en la entrega-informe, y si el destinatario del informe es el originador del mensaje-sujeto [y no, por ejemplo, el propietario de una LD (véase el § 8.3.1.2.1.4)].

Este argumento no estará presente si se ha realizado cualquier conversión de **tipo-información-codificada** sobre el **contenido** del mensaje-sujeto.

8.3.1.2.2 *Resultados*

La operación abstracta de entrega-informe devuelve un resultado vacío como indicación de éxito.

8.3.1.2.3 *Errores-abstractos*

El cuadro 19/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta entrega-informe, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 19/X.411

Errores-abstractos de entrega-informe

Error-abstracto	Punto
Control-entrega-violado	8.3.2.1
Error-seguridad	8.3.2.3
Función-crítica-no-admitida	8.3.2.4

8.3.1.3 *Control-entrega*

La operación-abstracta control-entrega permite al usuario-STRM limitar de forma transitoria las operaciones abstractas de puerto-entrega que puede invocar el STRM, y los mensajes que puede entregar el usuario-STRM a través de la operación-abstracta entrega-mensaje.

El STRM debe retener hasta un tiempo posterior, en vez de abandonar, las operaciones-abstractas y los mensajes prohibidos.

La ejecución satisfactoria de la operación-abstracta significa que los controles especificados están actualmente en vigor. Estos controles sobreseen cualquier otro previamente en vigor, y permanecen vigentes hasta que se libera la asociación, el usuario-STRM invoca la operación-abstracta de registro en el puerto-administración para imponer limitaciones más rigurosas que los controles especificados.

La operación-abstracta devuelve una indicación de cualquier operación-abstracta que invocara el STRM, o cualquier tipo de mensaje que entregaría o sobre el que informaría el STRM, a no ser por los controles que prevalecen.

8.3.1.3.1 *Argumentos*

El cuadro 20/X.411 enumera los argumentos de la operación-abstracta control-entrega y para cada argumento califica la presencia e identifica el punto donde se define el argumento.

8.3.1.3.1.1 *Limitación*

Este argumento indica si los controles sobre las operaciones de puerta-entrega deben actualizarse o suprimirse. Puede generarse por el usuario-STRM.

Este argumento puede tener uno de los siguientes valores:

- **actualización**: los demás argumentos actualizan los controles que prevalecen;
- **supresión**: todos los controles deben suprimirse (se aplicarán los controles por defecto registrados con el STRM mediante la operación-abstracta de registro del puerto-administración); los demás argumentos deben ignorarse.

En ausencia de este argumento, se supondrá por defecto el valor **actualización**.

CUADRO 20/X.411

Argumentos de control-entrega

Argumentos	Presencia	Punto
Argumentos de control de entrega		
Limitación	F	8.3.1.3.1.1
Operaciones-admisibles	F	8.3.1.3.1.2
Prioridad-inferior-admisible	F	8.3.1.3.1.3
Tipos-información-codificada-admisible	F	8.3.1.3.1.4
Tipos-contenido-admisibles	F	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	F	8.3.1.3.1.6
Contexto-seguridad-admisible	F	8.3.1.3.1.7

8.3.1.3.1.2 *Operaciones-admisibles*

Este argumento indica las operaciones-abstractas que el STRM puede invocar sobre el usuario-STRM. Puede generarse por el usuario-STRM.

Este argumento puede tener el valor **autorizado** o **prohibido** para cada uno de los siguientes:

- **entrega-mensaje**: el STRM puede/no puede invocar la operación-abstracta de entrega-mensaje; y
- **entrega-informe**: el STRM puede/no puede invocar la operación-abstracta de entrega-informe.

Otras operaciones-abstractas de puerta-entrega no están sujetas a controles, y pueden invocarse en cualquier momento.

En ausencia de este argumento, las operaciones-abstractas que puede invocar el STRM permanecen sin modificaciones. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará el control por defecto registrado con el STRM mediante la operación-abstracta de registro en el puerto-administración.

8.3.1.3.1.3 *Prioridad-inferior-admisible*

Este argumento contiene la **prioridad** del mensaje de prioridad más baja que el STRM debe remitir al usuario-STRM a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-STRM.

Este argumento puede tener uno de los siguientes valores del argumento de **prioridad** de la operación-abstracta de entrega-mensaje: **normal**, **no-urgente** o **urgente**.

En ausencia de este argumento, la **prioridad** del mensaje de inferior prioridad que debe entregar el STRM al usuario-STRM permanece sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se debe aplicar el control por defecto registrado con el STRM mediante la operación-abstracta registro del puerto-administración.

8.3.1.3.1.4 *Tipos-información-codificada-admisibles*

Este argumento indica los **tipos-información-codificada**, que deben aparecer en los mensajes que el STRM entregará al usuario-STRM a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-STRM.

Los **tipos-información-codificada-admisibles** especificados deben estar entre los autorizados a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**tipos-información-codificada-entregables**).

En ausencia de este argumento, los **tipos-información-codificada-admisibles** de un mensaje que el STRM puede entregar al usuario-STRM permanecen sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se debe aplicar el control por defecto registrado con el STRM mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.5 *Tipos-contenido-admisibles*

Este argumento contiene los **tipos-contenido**, que deben aparecer en el mensaje que el STRM debe entregar al usuario-STRM a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-STRM.

Los **tipos-contenido-admisibles** especificados deben estar entre los autorizados a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**tipos-contenido-entregables**).

En ausencia de este argumento, los **tipos-contenido-admisibles** de un mensaje que el STRM puede entregar al usuario-STRM permanecen sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará por defecto el control registrado con el STRM mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.6 *Longitud-contenido-máxima-admisible*

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el STRM debe remitir al usuario-STRM a través de la operación-abstracta entrega-mensaje. Puede generarse por el usuario-STRM.

La **longitud-contenido-máxima-admisible** no debe exceder la autorizada a largo plazo debido a la invocación previa de la operación-abstracta de registro en el puerto-administración (**longitud-contenido-máxima-entregable**).

En ausencia de este argumento, la **longitud-contenido-máxima-admisible** de un mensaje que el STRM puede entregar al usuario-STRM permanece sin modificar. Si no ha existido ninguna invocación previa de la operación-abstracta control-entrega en la asociación, se aplicará por defecto el control registrado con el STRM mediante la operación-abstracta de registro del puerto-administración.

8.3.1.3.1.7 *Contexto-seguridad-admisible*

Este argumento limita de forma transitoria la sensibilidad de las operaciones-abstractas de puerto-entrega (contexto-seguridad-entrega) que el STRM puede invocar en el usuario-STRM. Es una limitación temporal del **contexto-seguridad** establecido al iniciarse la asociación (véase el § 8.1.1.1.1.4). Puede generarse por el usuario-STRM.

El **contexto-seguridad-admisible** consta de una o más **etiquetas-seguridad** del conjunto de **etiquetas-seguridad** establecidas como **contexto-seguridad** al establecerse la asociación.

En ausencia de este argumento, el **contexto-seguridad** de las operaciones-abstractas de puerto-entrega permanece sin modificar.

8.3.1.3.2 *Resultados*

El cuadro 21/X.411 enumera los resultados de la operación-abstracta control-entrega, y para cada resultado califica su presencia e identifica el punto donde se define el resultado.

CUADRO 21/X.411

Resultados de control-entrega

Resultados	Presencia	Punto
Resultados «Esperando»		
Operaciones-esperando	F	8.3.1.3.2.1
Mensaje-esperando	F	8.3.1.3.2.2
Tipos-información-codificada-esperando	F	8.3.1.3.2.3
Tipos-contenido-esperando	F	8.3.1.3.2.4

8.3.1.3.2.1 *Operaciones-esperando*

Este resultado indica las operaciones-abstractas que retiene el STRM y que el STRM invocaría en el usuario-STRM si no fuera por los controles que prevalecen. Puede generarse por el STRM.

Este resultado puede tener el valor **reteniendo** o **no-reteniendo** para cada uno de los siguientes:

- **entrega-mensaje**: el STRM está/no está reteniendo mensajes, e invocaría la operación abstracta de entrega-mensaje en el usuario-STRM si no fuera por los controles que prevalecen; y
- **entrega-informe**: el STRM está/no está reteniendo informes, e invocaría la operación-abstracta de entrega-informe en el usuario-STRM si no fuera por los controles que prevalecen.

En ausencia de este resultado, puede suponerse que el STRM no está reteniendo ningún mensaje ni ninguna sonda para su entrega al usuario-STRM debido a los controles que prevalecen.

8.3.1.3.2.2 *Mensajes-esperando*

Este resultado indica la categoría de los mensajes que el STRM está reteniendo para su remisión al usuario-STRM, y que remitiría a través de la operación-abstracta entrega-mensaje, si no fuera por los controles que prevalecen.

Este resultado puede adoptar uno de los siguientes valores:

- **contenido-largo**: el STRM ha retenido mensajes para su entrega al usuario-STRM que exceden el control **longitud-contenido-máxima-admisible** actualmente en vigor;
- **baja-prioridad**: el STRM ha retenido mensajes para su entrega al usuario-STRM de una prioridad inferior al control de **prioridad-inferior-admisible** actualmente en vigor;
- **otras-etiquetas-seguridad**: el STRM ha retenido mensajes para su entrega al usuario-STRM que transportan **etiquetas-seguridad-mensaje** diferentes de las permitidas por el contexto-seguridad actual.

En ausencia de este resultado, puede suponerse que el STRM no está reteniendo ningún mensaje ni ninguna sonda para su entrega al usuario-STRM debido a los controles de **longitud-contenido-máxima-admisible**, **prioridad-inferior-admisible** o **contexto-seguridad-admisible** actualmente en vigor.

8.3.1.3.2.3 *Tipos-información-codificada-esperando*

Este resultado indica los **tipos-información-codificada** del **contenido** de cualquier mensaje retenido por el STRM para su entrega al usuario-STRM debido a los controles que prevalecen. Puede generarse por el STRM.

En ausencia de este resultado, los **tipos-información-codificada** de cualquier mensaje retenido por el STRM para su entrega al usuario-STRM estarán **sin-especificar**.

8.3.1.3.2.4 *Tipos-contenido-esperando*

Este resultado indica los **tipos-contenido** de cualquier mensaje retenido por el STRM para su entrega al usuario-STRM debido a los controles que prevalecen. Puede generarse por el STRM.

En ausencia de este resultado, los **tipos-contenido** de cualquier mensaje retenido por el STRM para su entrega al usuario-STRM estarán **sin-especificar**.

8.3.1.3.3 *Errores-abstractos*

El cuadro 22/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta control-entrega, y para cada error-abstracto identifica el punto donde se define el error-abstracto.

CUADRO 22/X.411

Errores-abstractos de control-entrega

Error-abstracto	Punto
Control-viola-registro	8.3.2.2
Error-seguridad	8.3.2.3

8.3.2 *Errores-abstractos*

En este punto se definen los siguientes errores-abstractos de puerto-entrega:

a) control-entrega-violado
b) control-viola-registro
c) error-seguridad
d) función-crítica-no-admitida.

8.3.2.1 *Control-entrega-violado*

El error-abstracto de control-entrega-violado informa de la violación por el STRM de un control sobre las operaciones-abstractas de puerto-entrega impuestas por el usuario-STRM a través de la operación-abstracta de control-entrega.

El error-abstracto de control-entrega-violado no tiene parámetros.

8.3.2.2 *Control-viola-registro*

El error-abstracto control-viola-registro informa que el STRM no puede aceptar el control que el usuario-STRM intenta imponer sobre las operaciones-abstractas porque violan los parámetros de registro existentes.

El error-abstracto control-viola-registro no tiene parámetros.

8.3.2.3 *Error-seguridad*

El error-abstracto error-seguridad informa que la operación-abstracta pedida no puede ser proporcionada por el usuario-STRM porque se violaría la política-seguridad en vigor.

El error-abstracto error-seguridad tiene los siguientes parámetros, generados por el usuario-STRM:

– **problema-seguridad**: identificador relativo a la causa de violación de la política-seguridad.

8.3.2.4 *Función-crítica-no-admitida*

El error-abstracto función-crítica-no-admitida informa que un argumento de la operación-abstracta ha sido marcado como **crítico-para-entrega** (véase el § 9.1) pero que no está admitido por el usuario-STRM.

El error-abstracto función-crítica-no-admitida no tiene parámetros.

8.4 *Puerto de administración*

En este punto se definen las operaciones-abstractas y los errores-abstractos que ocurren en un puerto-admiración.

8.4.1 *Operaciones-abstractas*

En este punto se definen las siguientes operaciones-abstractas de puerto-administración:

a) registro
b) cambio-credenciales.

8.4.1.1 *Registro*

La operación-abstracta registro permite a un usuario-STRM realizar cambios a largo-plazo en varios parámetros del usuario-STRM retenido por el STRM afectado por la entrega de mensajes al usuario-STRM.

Dichos cambios permanecen vigentes hasta ser superados por la nueva invocación de la operación-abstracta de registro. Sin embargo, algunos parámetros pueden ser transitoriamente reemplazados mediante la invocación de la operación-abstracta control-entrega.

Nota 1 – Esta operación-abstracta debe ser invocada antes de que pueda utilizarse cualquier otro puerto-remisión, puerto-entrega u operación-abstracta de puerto-administración o habrá tenido lugar un registro equivalente localmente.

Nota 2 – Esta operación-abstracta no incluye los parámetros existentes involucrados por el elemento-de-servicio destinatario alternativo autorizado y el elemento-de-servicio entrega-restringida definido en la Recomendación X.400. La forma en que se suministran y modifican dichos parámetros es asunto local.

8.4.1.1.1 *Argumentos*

El cuadro 23/X.411 enumera los argumentos de la operación-abstracta registro y para cada argumento califica la presencia e identifica el punto donde se define el argumento.

CUADRO 23/X.411

Argumentos de registro

Argumento	Presencia	Punto
Argumentos de registro		
Nombre-usuario	F	8.4.1.1.1.1
Dirección-usuario	F	8.4.1.1.1.2
Tipos-información-codificada-entregables	F	8.4.1.1.1.3
Tipos-contenido-entregables	F	8.4.1.1.1.4
Longitud-contenido-máxima-entregable	F	8.4.1.1.1.5
Destinatario-alternativo-asignado-destinatario	F	8.4.1.1.1.6
Etiquetas-seguridad-usuario	F	8.4.1.1.1.7
Argumentos de control de entrega por defecto		8.4.1.1.1.8
Limitaciones	F	8.3.1.3.1.1
Operaciones-admisibles	F	8.3.1.3.1.2
Prioridad-inferior-admisible	F	8.3.1.3.1.3
Tipos-información-codificada-admisibles	F	8.3.1.3.1.4
Tipos-contenido-admisibles	F	8.3.1.3.1.5
Longitud-contenido-máxima-admisible	F	8.3.1.3.1.6

8.4.1.1.1.1 *Nombre-usuario*

Este argumento contiene el **nombre-O/D** del usuario-STRM, si ha de cambiarse el **nombre-usuario**. Puede ser generado por el usuario-STRM.

En ausencia de este argumento, el **nombre-usuario** del usuario-STRM permanece sin modificar.

Un DG no está obligado a proporcionar a los usuarios-STRM la posibilidad de modificar sus **nombres-O/D**. Si así lo hace, el DG puede limitar esa posibilidad. Puede prohibir a ciertos usuarios-STRM cambiar sus **nombres-O/D**, o puede limitar el ámbito del cambio a un subconjunto definido localmente de los componentes de sus **nombres-O/D**. Un nuevo **nombre-O/D** propuesto será rechazado si ya está asignado a otro usuario-STRM.

8.4.1.1.1.2 *Dirección-usuario*

Este argumento contiene la **dirección-usuario** del usuario-STRM, si éste la solicita o si se ha de modificar. Puede ser generado por el usuario-STRM.

La **dirección-usuario** puede contener una de las siguientes formas de dirección del usuario-STRM:

- la **dirección-X.121** y/o el **ID-PAST** (identificador del punto de acceso del servicio de transporte); o
- la **dirección-DASP** (dirección del punto de acceso del servicio de presentación).

En las futuras versiones de esta Recomendación pueden definirse otras formas de **dirección-usuario**.

En ausencia de este argumento, la **dirección-usuario** del usuario-STRM (si existe) permanece sin modificar.

8.4.1.1.1.3 *Tipos-información-codificada-entregables*

Este argumento indica los **tipos-información-codificada** que el STRM permitirá que aparezcan en los mensajes entregados al usuario-STRM, si éstos deben modificarse. Pueden ser generados por el usuario-STRM.

El STRM debe rechazar como inentegrable cualquier mensaje para un usuario-STRM que no esté registrado para aceptar la entrega de todos los **tipos-información-codificada** del mensaje. Obsérvese que el usuario-STRM puede registrarse para recibir el **tipo-información-codificada indefinido**. Los tipos información-codificada-entregables indican también los posibles tipos-información-codificada hacia los que puede realizarse conversión implícita.

En ausencia de este argumento, los **tipos-información-codificada-entregable** permanecerán sin modificar.

8.4.1.1.1.4 *Tipos-contenido-entregables*

Este argumento indica los **tipos-contenido** que el STRM debe permitir que aparezcan en los mensajes entregados al usuario-STRM, si han de modificarse. Puede ser generado por el usuario-STRM.

El STRM debe rechazar como inentregable cualquier mensaje para un usuario-STRM que no esté registrado para aceptar la entrega de los **tipos-contenido** del mensaje. Obsérvese que el usuario-STRM puede registrarse para recibir el **tipo-contenido indefinido**.

En ausencia de este argumento, los **tipos-contenido-entregables** deben permanecer sin modificar.

8.4.1.1.1.5 *Longitud-máxima-contenido-entregable*

Este argumento contiene la **longitud-contenido**, en octetos, del mensaje de contenido más largo que el STRM debe permitir que aparezca en los mensajes entregados al usuario-STRM, si han de modificarse. Puede ser generado por el usuario-STRM.

El STRM deberá rechazar como imposible de entregar, cualquier mensaje para un usuario-STRM que no esté registrado para aceptar la entrega de mensajes de este tamaño.

En ausencia de este argumento, la longitud **máxima-contenido-entregable** del mensaje debe permanecer sin modificar.

8.4.1.1.1.6 *Destinatario-alternativo-asignado-destinatario*

Este argumento contiene el **nombre-O/D** de un destinatario-alternativo, especificado por el usuario-STRM al que deben redirigirse los mensajes, si debe modificarse el destinatario-alternativo. Puede ser generado por el usuario-STRM. Puede especificarse un valor diferente de este argumento para cada valor de las **etiquetas-seguridad-usuario**.

Si se registra un **destinatario-alternativo-asignado-destinatario** y se asocia con un valor de las **etiquetas-seguridad-usuario**, los mensajes que transporten una **etiqueta-seguridad-mensaje** acorde se deben redirigir al destinatario. Los mensajes que transportan una **etiqueta-seguridad-mensaje** para la cual no se ha registrado ningún **destinatario-alternativo-asignado-destinatario**, no se deben redirigir a un **destinatario-alternativo-asignado-destinatario**.

Si se registra un **destinatario-alternativo-asignado-destinatario** único, y no se le asocia un valor de **etiquetas-seguridad-usuario**, se deben redirigir todos los mensajes al destinatario-alternativo.

El **destinatario-alternativo-asignado-destinatario** deberá contener el **nombre-O/D** del destinatario-alternativo. Si el **destinatario-alternativo-asignado-destinatario** contiene el **nombre-O/D** del usuario-STRM (véase el § 8.4.1.1.1.1) no se registra ningún **destinatario-alternativo-asignado-destinatario**.

En ausencia de este argumento el **destinatario-alternativo-asignado-destinatario**, si lo hubiere, permanece sin modificar.

8.4.1.1.1.7 *Eiquetas-seguridad-usuario*

Este argumento contiene las **etiquetas-seguridad** del usuario-STRM, si han de modificarse. Puede ser generado por el usuario-STRM.

Puede registrarse un **destinatario-alternativo-asignado-destinatario** para cualquier valor de las **etiquetas-seguridad-usuario**.

En ausencia de este argumento, las **etiquetas-seguridad-usuario** permanecen sin modificar.

Obsérvese que algunas políticas-seguridad puede que permitan únicamente modificar las **etiquetas-seguridad-usuario** de esta forma sí se utiliza un enlace seguro. Pueden proporcionarse otros medios locales de modificar las **etiquetas-seguridad-usuario** de forma segura.

8.4.1.1.1.8 *Argumentos de control de entrega por defecto*

Los argumentos de control por defecto son los mismos que los argumentos de la operación-abstracta control-entrega, definidos en el § 8.3.1.3.1. Excepto para **contexto-seguridad-admisible**, pueden ser generados por el usuario-STRM.

Se registran los controles por defecto como argumentos de la operación-abstracta abstracta de registro. Estas actuaciones por defecto entran en vigor al comienzo de una asociación, y permanecen vigentes hasta que son suspendidas por una invocación de la operación-abstracta de control-entrega.

Los argumentos de control por defecto no deben admitir mensajes cuya entrega esté prohibida por los valores registrados prevalecientes del argumento **tipos-información-codificada-entregables**, del argumento **tipos-contenido-entregables** o del argumento **longitud-máxima-contenido-entregable**.

8.4.1.1.2 *Resultados*

La operación-abstracta registro devuelve un resultado vacío como indicación del éxito.

8.4.1.1.3 *Errores-abstractos*

El cuadro 24/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta de registro y para cada error-abstracto identifica el punto donde se define el error abstracto.

CUADRO 24/X.411

Errores-abstractos de registro

Error-abstracto	Punto
Registro-rechazado	8.4.2.1

8.4.1.2 *Cambio-credenciales*

La operación-abstracta cambio-credenciales permite al usuario-STRM modificar las **credenciales** del usuario-STRM en poder del STRM, o permite al STRM modificar las **credenciales** del STRM en poder del usuario-STRM.

Durante el establecimiento de una asociación se intercambian las **credenciales** para la autenticación mutua de la identidad del usuario-STRM y del STRM.

La finalización con éxito de la operación-abstracta significa que se han cambiado las **credenciales**.

La interrupción de la operación-abstracta por un error-abstracto indica que no se han cambiado las **credenciales**, bien porque las antiguas **credenciales** estaban incorrectamente especificadas o porque las nuevas **credenciales** resultan inaceptables.

8.4.1.2.1 *Argumentos*

El cuadro 25/X.411 enumera los argumentos de la operación-abstracta-credenciales y para cada argumento califica la presencia e identifica el punto donde se define el argumento.

CUADRO 25/X.411

Argumentos de cambio-credenciales

Argumento	Presencia	Punto
Argumentos de credenciales		
Credenciales-antiguas	O	8.4.1.2.1.1
Credenciales-nuevas	O	8.4.1.2.1.2

8.4.1.2.1.1 *Credenciales-antiguas*

Este argumento contiene las **credenciales** vigentes (antiguas) del invocador de la operación-abstracta en poder del ejecutor de la operación-abstracta. Debe ser generado por el invocador de la operación-abstracta.

Si se utiliza únicamente una autenticación-simple, las **credenciales** incluyen una **contraseña** simple asociada al **nombre-usuario**, o al **nombre-ATM** del invocador.

Si se utiliza una autenticación-fuerte, las **credenciales** incluyen el **certificado** del invocador, generado por una fuente de confianza (por ejemplo, autoridad-certificación), y proporcionado por el invocador.

8.4.1.2.1.2 *Credenciales-nuevas*

Este argumento contiene las **credenciales-nuevas** propuestas del invocador de la operación-abstracta que debe poseer el ejecutor de la operación-abstracta. Debe ser generado por el invocador de la operación-abstracta.

Las **credenciales-nuevas** deben ser del mismo tipo (simple o fuerte) que las **credenciales-antiguas**, definidas en el § 8.4.1.2.1.1.

8.4.1.2.2 *Resultados*

La operación-abstracta cambio-credenciales devuelve un resultado vacío como indicación del éxito.

8.4.1.2.3 *Errores-abstractos*

El cuadro 26/X.411 enumera los errores-abstractos que pueden interrumpir la operación-abstracta de cambio credenciales y para cada error-abstracto identifica el punto donde se define el error abstracto.

CUADRO 26/X.411

Errores-abstractos de cambio-credenciales

Error-abstracto	Punto
Credenciales-nuevas-inaceptables	8.4.2.2
Credenciales-antiguas-inaceptables	8.4.2.3

8.4.2 *Errores-abstractos*

En este punto, se definen los siguientes errores-abstractos del puerto-administración:

a) registro-rechazado
b) credenciales-nuevas-inaceptables
c) credenciales-antiguas-incorrectamente-especificadas.

8.4.2.1 *Registro-rechazado*

El error-abstracto registro-rechazado notifica que no pueden registrarse los parámetros pedidos porque uno o más están indebidamente especificados.

El error-abstracto registro-rechazado no tiene parámetros.

8.4.2.2 *Credenciales-nuevas-inaceptables*

El error-abstracto credenciales-nuevas-inaceptables notifica que no pueden cambiarse las **credenciales** porque las **credenciales-nuevas** son inaceptables.

El error-abstracto credenciales-nuevas-inaceptables no tiene parámetros.

8.4.2.3 *Credenciales-nuevas-incorrectamente-especificadas*

El error-abstracto credenciales-antiguas-incorrectamente-especificadas notifica que no pueden cambiarse las **credenciales** porque las **credenciales (antiguas)** vigentes están incorrentamente especificadas.

El error-abstracto-credenciales-antiguas-incorrectamente-especificadas no tiene parámetros.

8.5 *Tipos comunes de parámetros*

En este punto se define un cierto número de tipos comunes de parámetros del servicio abstracto STRM.

8.5.1 *Identificador-STRM*

El STRM asigna **identificadores-STRM** para distinguir entre los mensajes y sondas del servicio abstracto STRM y entre los mensajes, sondas e informes dentro del STRM.

El **identificador-STRM** asignado a un mensaje en un puerto-remisión (**identificador-remisión-mensaje**) es idéntico al **identificador-mensaje** correspondiente en un puerto-transferencia y al correspondiente **identificador-entrega-mensaje** en un puerto de entrega. De forma similar, el **identificador-STRM** asignado a una sonda en un puerto-remisión (**identificador-remisión-sonda**) es idéntico al **identificador-sonda** correspondiente en un puerto-transferencia. Se asignan igualmente **identificadores-STRM** a los informes en los puertos-transferencias (**identificador-informe**).

Un **identificador-STRM** consta de:

- un **identificador-local** asignado por el ATM, que identifica sin ambigüedad el suceso en cuestión dentro del DG:
- el **identificador-dominio-global** del DG, que garantiza que el **identificador-STRM** es inequívoco a lo largo del STRM.

8.5.2 *Identificador-dominio-global*

Un **identificador-dominio-global** identifica inequívocamente un DG en el interior del STM.

Se utiliza un **identificador-dominio-global** para garantizar que un **identificador-STRM** no resulta ambiguo a lo largo del STRM y para identificar la fuente de un **elemento-información-rastreo**.

En el caso de un DGAD, un **identificador-dominio-global** consta del **nombre-país** y del **nombre-dominio-administración** del DG. Para un DGPR, consta del **nombre-país** y del **nombre-dominio-administración** del DGAD asociado, más un **identificador-dominio-privado**. El **identificador-dominio-privado** es una identificación única del DGPR y puede ser idéntico al **nombre-dominio-privado** del DGPR. Como un asunto nacional, esta identificación puede ser relativa al país designado por el **nombre-país** o relativa al DGAD asociado.

Nota 1 – La distinción entre el **identificador-dominio-privado** y el **nombre-dominio-privado** se ha conservado para asegurar la compatibilidad con la Recomendación X.411 (1984). A menudo serán idénticos.

Nota 2 – En la publicación ISO/CEI 10021-4, en el **identificador-dominio-global** de un DGPR, el **nombre-dominio-administración** del DGAD asociado es optativo.

8.5.3 *Nombre-ATM*

Un **nombre-ATM** es un identificador para un ATM que identifica unívocamente al ATM dentro del DG al que pertenece.

8.5.4 *Tiempo*

Se especifica un parámetro **tiempo** en términos del TUC (tiempo universal coordinado) y puede contener igualmente de forma opcional una desviación respecto del TUC para incorporar el tiempo local. La precisión de la hora del día es de un segundo o de un minuto según determine el generador del parámetro.

8.5.5 *Nombre-O/D*

Un **nombre-O/D** identifica al originador o destinatario de un mensaje según los principios de denominación y direccionamiento descritos en la Recomendación X.402.

En un puerto-remisión, un **nombre-O/D** consta de una **dirección-O/D**, o un **nombre-guía** o ambos (**dirección-O/D-y-o-nombre-guía**). En todos los tipos de puerto restantes, un **nombre-O/D** consta de una **dirección-O/D** y, opcionalmente, un **nombre-guía** (**dirección-O/D-y-nombre-guía-facultativo**). Un **nombre-guía** y una **dirección-O/D** pueden denominar cada uno un originador o un destinatario individual o una LD.

En la Recomendación X.501 se define un **nombre-guía**. El STRM utiliza el **nombre-guía** únicamente cuando está ausente o es inválida la **dirección-O/D**.

Una **dirección-O/D** consta de un cierto número de **atributos-normales**, opcionalmente de un cierto número de **atributos-ampliación**, y opcionalmente de un cierto número de atributos definidos por el DG al cual está suscrito el originador/destinatario (**atributos-definidos-dominio**).

Los **atributos-normales** y **-ampliación** utilizados en una **dirección-O/D** se seleccionan a partir de los definidos en la Recomendación X.402. Unicamente pueden utilizarse estas combinaciones de atributos explícitamente definidos en la Recomendación X.402 para formar una **dirección-O/D** válida.

8.5.6 *Tipos-información-codificada*

Los **tipos-información-codificada** de un mensaje representan el tipo o tipos de información que aparecen en su **contenido**. Pueden especificarse tanto los **tipos-información-codificada** básicos como los **tipos-información-codificada** definidos externamente, en caso contrario los **tipos-información-codificada** de un mensaje están **sin-especificar**.

Los **tipos-información-codificada** definidos externamente son aquellos a los que una autoridad competente atribuye identificadores-objetos. Estos incluyen los **tipos-información-codificada** tanto normalizados como definidos-privadamente.

Los **tipos-información-codificada** básicos son aquellos especificados originalmente en la Recomendación X.411 (1984). El tipo **indefinido** es cualquier tipo distinto de los **tipos-información-codificada** definidos-externamente especificados y diferentes de los tipos siguientes. El tipo **télex** se define en la Recomendación F.1. El tipo **texto-ai5** (teleimpresor) se define en la Recomendación T.50. El tipo **facsímil-g3** se define en las Recomendaciones T.4 y T.30. El tipo **clase-1-g4** se define en las Recomendaciones T.5, T.6, T.400 y T.503. El tipo **teletex** se define en las Recomendaciones F.200, T.61 y T.60. El tipo **videotex** se define en las Recomendaciones T.100 y T.101. El tipo **documento-formatizable-simple (dfs)** se define en la Recomendación X.420 (1984) (obsérvese que los DFS ya no se definen en ninguna Recomendación de 1988). El tipo **modo mixto** se define en las Recomendaciones T.400 y T.501.

Se definen **parámetros-no-básicos** para el **facsímil-g3**, **teletex**, **g4-clase-1**, y **modo mixto**, los **tipos-información-codificada** para compatibilidad regresiva con la Recomendación X.411 únicamente. Se recomienda que para cada combinación requerida de un **tipo-información-codificada** básica y un conjunto específico de **parámetros-no-básicos**, se defina y utilice de preferencia un **tipo-información-codificada** definida-externamente.

Obsérvese que es probable que se supriman los **parámetros-no-básicos** en una futura versión de esta Recomendación.

Los **parámetros-no-básicos** para **facsímil-g3** corresponden a los campos de información facsímil (CIF) de tres -o cuatro- octetos transportados por la señal de instrucción digital (SID) definidos en T.30. Los parámetros son **bi-dimensional**, **resolución-fina**, **longitud-ilimitada**, **longitud-b4**, **anchura-a3**, **anchura-b4** y **sin-comprensión**.

Los **parámetros-no-básicos** para **teletex** corresponden a la capacidad terminal no-básica transportada por la instrucción de comienzo de documento (ICD) definida en la Recomendación T.62. Los parámetros son: **conjuntos-caracteres-gráficos**, **conjuntos-caracteres-control**, **formatos-páginas** opcionales, **capacidades-terminal-misceláneas** facultativas, y un parámetro de **uso-privado**.

Los **parámetros-no-básicos** para los tipos de **clase-1-g4** y **modo-mixto** especifican la resolución opcional, los conjuntos de caracteres gráficos opcionales, los conjuntos de caracteres de control opcionales, y así sucesivamente, que corresponden a los parámetros de las **capacidades-presentación** definidos en las Recomendaciones T.400, y T.503 y T.501.

Cuando se indican **parámetros-no-básicos**, estos parámetros representan el «O» lógico de los **parámetros-no-básicos** de cada ejemplo de **tipo-información-codificada** en un **contenido** de mensaje. Así, este parámetro sirve únicamente para indicar si existe compatibilidad de **tipo-información-codificada**, o si se requiere conversión. Si se requiere conversión, se inspeccionará el **contenido** del mensaje para determinar que **parámetros-no-básicos** se aplican a cualquier ejemplo de **tipo-información-codificada**.

8.5.7 *Certificado*

Puede utilizarse un **certificado** para transportar una copia verificada de la clave-cifrado-pública-asimétrica del sujeto del **certificado**.

Un **certificado** consta de los siguientes parámetros:

- **identificador-algoritmo-firma**: **algoritmo-identificador** para el algoritmo utilizado por la autoridad-certificación que expidió el **certificado** para calcular la firma;
- **expedidor**: **nombre-guía** de la autoridad-certificación que expidió el **certificado**;
- **validez**: fecha y hora del día antes de las cuales no debería utilizarse el **certificado**, y fecha y hora del día después de las cuales no debería confiarse en el **certificado**;
- **sujeto**: **nombre-guía** del sujeto del **certificado**;
- **claves-públicas-sujeto**: una o más claves-cifrado-públicas-asimétricas del sujeto (cada una utilizada junto con un **algoritmo** y una clave-cifrado-secreta-asimétrica del sujeto);
- **algoritmos**: uno o más **identificadores-algoritmo**, cada uno asociado con una **clave-pública-sujeto**;
- **firma**: versión asimétricamente cifrada, desmenuzada de los anteriores parámetros calculada por la autoridad-certificación que expidió el **certificado** utilizando el algoritmo identificado por el **identificador-algoritmo-firma** y la clave-cifrado-secreta-asimétrica de la autoridad-certificación.

Si el originador y un destinatario de un **certificado** se sirven de la misma autoridad-certificación, el destinatario puede utilizar la clave-cifrado-pública-asimétrica de la autoridad-certificación para validar el **certificado** y deducir la clave-cifrado-pública-asimétrica del originador (**clave-pública-sujeto**).

Si el originador y un destinatario de un **certificado** se sirven de autoridades-certificación diferentes, el destinatario puede necesitar un trayecto-retorno-certificación para autenticar el **certificado** del originador. Por lo tanto, el **certificado** puede incluir un **trayecto-certificación** asociado.

El **trayecto-certificación** puede incluir un **trayecto-certificación-hacia-adelante** que incorpora el certificado de la autoridad-certificación que expidió el **certificado** junto con los certificados de todas sus autoridades-certificación superiores. El **trayecto-certificación-hacia-adelante** puede incluir igualmente los certificados de otras autoridades-certificación, con certificación recíproca por la autoridad-certificación que expidió el **certificado** o por cualquier otra de sus autoridades-certificación superiores.

Un destinatario del **certificado** puede completar el trayecto-retorno-certificación requerido entre el destinatario y el originador del **certificado** añadiendo un trayecto-certificación-inverso propio del destinatario al **trayecto-certificación-hacia-adelante** suministrado por el originador en un punto-común-de-confianza. El trayecto-certificación-inverso incluye el certificado-inverso de la autoridad-certificación del destinatario del **certificado**, junto con los certificados-inversos de todas sus autoridades de certificación superiores. El trayecto-certificación-inverso puede incluir igualmente los certificados-inversos de otras autoridades-certificación con certificación recíproca por la autoridad-certificación del destinatario del **certificado**, o cualquiera de sus autoridades de certificación superiores.

El trayecto-retorno-certificación así formado permite al destinatario del certificado validar cada **certificado** en el trayecto-retorno-certificación, para deducir la clave-cifrado-pública-asimétrica de la autoridad-certificación que expidió el **certificado**. El destinatario puede entonces utilizar la clave-cifrado-pública-asimétrica de la autoridad de certificación que expidió el **certificado** para validar el **certificado** y deducir la clave-cifrado-pública-asimétrica del originador (**clave-pública-sujeto**).

La forma de un **certificado** y de un **trayecto-certificación** se definen posteriormente en la Recomendación X.509.

Futuras versiones de esta Recomendación pueden definir otras técnicas de distribución de claves (por ejemplo, basadas en técnicas-cifrado-simétricas).

8.5.8 *Testigo*

Puede utilizarse un **testigo** para transportar al destinatario del **testigo**, información relativa-seguridad protegida. El **testigo** proporciona la autenticación de la información relativa-seguridad pública, y la confidencialidad y autenticación de la información relativa-seguridad secreta.

El tipo de **testigo** se identifica mediante un **identificador-tipo-distintivo**. Esta Recomendación define un tipo de **testigo**: el **testigo-asimétrico**. Futuras versiones de esta Recomendación pueden definir otros tipos de **testigo**; por ejemplo, **testigo** basados en las técnicas de cifrado-simétrica.

Un **testigo-asimétrico** contiene los siguientes parámetros:

- **identificador-algoritmo-firma**: **algoritmo-identificador** para el algoritmo utilizado por el originador del **testigo** para calcular la **firma**;
- **nombre-destinatario**: el **nombre-dirección-O/D-y/o-nombre-guía** del destinatario-deseado del **testigo**;
- **tiempo**: fecha y hora del día en que se generó el **testigo**;
- **datos-firmados**: información relativa-seguridad pública;
- **identificador-algoritmo-cifrado**: **identificador-algoritmo** para el algoritmo utilizado por el originador del **testigo** para calcular los **datos-cifrados**;
- **datos-cifrados**: información relativa-seguridad secreta cifrada por el originador del **testigo** utilizando el algoritmo identificado por el **identificador-algoritmo-cifrada** y la clave-cifrada-pública-asimétrica del destinatario-pretendido del **testigo**;
- **firma**: versión **cifrada** asimétricamente desmenuzada de los parámetros anteriores calculada por el originador del **testigo** utilizando el algoritmo identificado por el **identificador-algoritmo-firma** y la clave-cifrada-asimétrica-secreta del originador.

La forma de un **testigo** se define posteriormente en la Recomendación X.509.

8.5.9 *Etiqueta-seguridad*

Pueden utilizarse las **etiquetas-seguridad** para asociar la información relativa-seguridad con los objetos dentro del STRM.

Pueden asignarse **etiquetas-seguridad** a un objeto en línea con la política-seguridad en vigor para dicho objeto. La política-seguridad puede definir igualmente como deben utilizarse las **etiquetas-seguridad** para reforzar la política-seguridad.

Dentro del campo de aplicación de esta Recomendación, pueden asociarse **etiquetas-seguridad** a los mensajes, las sondas, y los informes (véase el § 8.2.1.1.1.30), los usuarios-STRM (véase el § 8.4.1.1.1.7), los DG, los ATM y asociaciones entre un usuario-STRM y un DG (o ATM) (véase el § 8.1.1.1.1.4) o entre DG (o ATM) (véase el § 12.1.1.1.1.4). Más allá del campo de aplicación de esta Recomendación, una política-seguridad puede, como asunto local o mediante un acuerdo bilateral, asignar adicionalmente **etiquetas-seguridad** a otros objetos dentro del STRM (por ejemplo, rutas seguras).

Una **etiqueta-seguridad** comprende un conjunto de **atributos-seguridad**. Los **atributos-seguridad** pueden incluir un **identificador-política-seguridad**, una **clasificación-seguridad**, una **marca de privacidad**, y un conjunto de **categorías-seguridad**.

Puede utilizarse un **identificador-política-seguridad** para identificar la política-seguridad en vigor a que se refiere la **etiqueta-seguridad**.

Si está presente, una **clasificación-seguridad** puede tener una lista jerárquica de valores. La jerarquía básica de **clasificación-seguridad** se define en esta Recomendación pero la utilización de estos valores se define mediante la política-seguridad en vigor. Una política-seguridad puede definir igualmente valores adicionales de **clasificación-seguridad** y su posición en la jerarquía como asunto local o mediante un acuerdo bilateral. La jerarquía básica de **clasificación-seguridad** es, por orden ascendente: **sin-marcar**, **sin-clasificar**, **restringido**, **confidencial**, **secreto**, **alto secreto**.

Si existe, una **marca-privacidad** es una cadena imprimible. El contenido de la cadena imprimible puede definirse mediante una política-seguridad, que puede definir una lista de valores a utilizar o permitir la determinación por el originador de la **etiqueta-seguridad** de dicho valor. Ejemplos de marcas-privacidad son «**CONFIDENCIAL**» y «**MUY ESTRICTAMENTE CONFIDENCIAL**».

Si existe, el conjunto de **categorías-seguridad** proporciona otras restricciones dentro del contexto de una **clasificación-seguridad** y/o **marca-privacidad** típicamente sobre la base de un «necesita-saber». Las **categorías-seguridad** y sus valores pueden definirse por una política-seguridad como asunto local o mediante un acuerdo bilateral. Los ejemplos de posibles **categorías-seguridad** incluyen escritos sobre la **clasificación-seguridad** y/o la **marca-privacidad** (por ejemplo, «**PERSONAL-**», «**PLANTILLA-**», «**COMERCIAL-**», etc.), grupos-cerrados-usuarios, palabras de código, etc.

8.5.10 *Identificador-algoritmo*

Un **identificador-algoritmo** identifica un **algoritmo** y cualesquiera **parámetros-algoritmo** requeridos por el **algoritmo**.

Un **identificador-algoritmo** puede extraerse del registro internacional de algoritmos o definirse mediante un acuerdo bilateral.

9 Definición de la sintaxis abstracta del sistema de transferencia de mensajes

La sintaxis-abstracta del servicio abstracto del STRM se define en la figura 2/X.411.

La sintaxis-abstracta del servicio abstracto del STRM se define utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208, y los convenios de definiciones del servicio abstracto definidos en la Recomendación X.407.

La definición de la sintaxis-abstracta del servicio abstracto STRM tiene las siguientes partes principales:

- *Prólogo:* declaraciones de las exportaciones desde el módulo de servicio abstracto del STRM, y de las importaciones a éste (figura 2/X.411, parte 1).
- *Objetos y puertos:* definiciones de los objetos del STRM y del usuario-STRM, y de sus puertos-remisión, -entrega, -administración, (figura 2/X.411, parte 2).
- *Vinculación-STRM, y desvinculación-STRM:* definiciones de las operaciones vinculación-STRM y desvinculación-STRM utilizadas para establecer y liberar asociaciones entre un usuario-STRM y el STRM (figura 2/X.411, partes 3 y 4).
- *Puerto de remisión:* definiciones de las operaciones-abstractas de puerto-remisión: remisión-mensaje, remisión-sonda, cancelación-entrega-diferida y control-remisión; y sus errores-abstractos (figura 2/X.411 partes 5 a 7).
- *Puerto de entrega:* definiciones de las operaciones-abstractas de puerto-entrega: entrega-mensaje, entrega-informe y control-entrega; y sus errores-abstractos (figura 2/X.411, partes 8 a 9).
- *Puerto de administración:* definiciones de las operaciones-abstractas de puerto-administración: registro y cambio-credenciales; y sus errores abstractos (figura 2/X.411, partes 10 a 11).
- *Sobre de remisión de mensaje:* definición del sobre-remisión-mensaje (figura 2/X.411, parte 12).
- *Sobre de remisión de sonda:* definición del sobre-remisión-sonda (figura 2/X.411, parte 13).
- *Sobre de entrega de mensaje:* definición del sobre-entrega-mensaje (figura 2/X.411, parte 14).
- *Sobre de entrega de informe:* definición del sobre-entrega-informe (figura 2/X.411, parte 15).
- *Campos de sobre:* definiciones de los campos de sobre (figura 2/X.411, partes 16 a 19).
- *Campos de ampliación:* definiciones de los campos-ampliación (figura 2/X.411, partes 20 a 28).
- *Tipos de parámetros comunes:* definiciones de los tipos de parámetros comunes (figura 2/X.411, partes 29 a 41).

Nota 1 – El módulo implica ciertos cambios en el protocolo P3 definido en la Recomendación X.411 (1984). Estos cambios se señalan mediante subrayado.

Nota 2 – El módulo aplica limitaciones de tamaño a los tipos de datos de longitud-variable utilizando la ampliación de subtipificación SIZE de NSA.1. La violación de una restricción de tamaño constituye una violación de protocolo.

9.1 *Mecanismo de criticidad*

Cada **campo-ampliación** definido en la figura 2/X.411 (partes 20 a 27) transporta consigo una indicación de su **criticidad** para remisión, transferencia y entrega. Se concibe el mecanismo de criticidad para permitir la transparencia controlada de funciones ampliadas. Una función no-crítica puede ignorarse o descartarse en la entrega, pero no será descartada por un ATM retransmisor salvo cuando degrade a un mensaje (véase el anexo B a la Recomendación X.419), mientras que una función crítica debe conocerse y realizarse correctamente para que prosigan los procedimientos normales.

En general, un argumento de una operación-abstracta marcado como crítico para el tipo de puerto en cuestión debe tratarse correctamente por quién ejecuta la operación-abstracta o se debe informar del error en la forma adecuada. El invocador de la operación-abstracta debe tratar correctamente todas las funciones marcadas como críticas para este tipo de puerto.

Si la operación-abstracta es de las que informan de un resultado infructuoso, se notifica un fallo en la correcta ejecución de una función crítica mediante la devolución de un error-abstracto de función-crítica-no-admitida. Si la operación-abstracta no es de las que notifican un resultado infructuoso, debe invocarse una operación-abstracta (por ejemplo, un informe) para transportar el resultado infructuoso de la operación anterior (por ejemplo, utilizando el **código-diagnóstico-no-entrega de función-crítica-no-admitida** de un informe).

La ampliación que aparece en el resultado de una operación-abstracta no debe marcarse como crítica para el tipo de puerto en cuestión.

En el caso de **crítica-para-remisión**, el STRM deberá ejecutar correctamente los procedimientos definidos para una función marcada como **crítica-para-remisión** en una operación-abstracta de remisión-mensaje o remisión-sonda o devolverá un error-abstracto de función-crítica-no-admitida.

En el caso de **crítica-para-transferencia**, un ATM receptor deberá ejecutar correctamente los procedimientos definidos para una función en un mensaje o sonda marcado como **crítica-para-transferencia**, o deberá devolver un informe-no-entrega con el **código-diagnóstico-no-entrega** puesto en **función-crítica-no-admitida**. Un ATM incapaz de proporcionar una función marcada como **crítica-para-transferencia** en un informe debe descartar el informe (obsérvese que una política o acuerdo local puede exigir que esta acción sea auditada). Una ampliación marcada como **crítica-para-transferencia** que aparece como un argumento de una operación de remisión-mensaje o remisión-sonda deberá aparecer sin modificación en una operación resultante de transferencia-mensaje o transferencia-sonda en un puerto-transferencia.

En el caso de **crítica-para-entrega**, un ATM-que-entrega ejecutará correctamente los procedimientos definidos para una función marcada como **crítica-para-entrega**, o no entregará el mensaje o sonda y devolverá un informe-no-entrega con el **código-diagnóstico-no-entrega** puesto en **función-crítica-no-admitida**. Un usuario-STRM receptor ejecutará correctamente los procedimientos definidos para una función marcada como **crítica-para-entrega** o devolverá un error-abstracto de función-crítica-no-admitida. Una ampliación marcada como **crítica-para-entrega** que aparece como argumento de una operación de remisión-mensaje o remisión-sonda debe aparecer sin modificación en una operación de transferencia-mensaje o transferencia-sonda en un puerto-transferencia. Una ampliación marcada como **crítica-para-entrega** que aparece como argumento de una operación de transferencia-mensaje o transferencia-sonda debe aparecer sin modificación en cualquier operación de transferencia-mensaje o transferencia-sonda en un puerto-transferencia.

Un ATM que genera un informe no deberá copiar las funciones críticas no admitidas procedentes del sujeto en el informe. Al generar el informe un ATM deberá indicar la **criticidad** (para transferencia y/o entrega) de cualquier función admitida copiada del sujeto en el informe; la **criticidad** de una función en un informe puede ser diferente de su **criticidad** en el sujeto.

Si el ATM o usuario-STRM no puede realizar correctamente los procedimientos definidos para una función marcada como «crítica-para-entrega», el informe es descartado.

Los procedimientos relativos a los **campos-ampliación** y a sus indicaciones sobre la **criticidad** se definen posteriormente en el § 14.

Esta Recomendación define mediante la macronotación de NSA.1 el establecimiento por defecto de la indicación de **criticidad** de los **campos-ampliación** que debe suministrar el originador de un mensaje. El originador de un mensaje o sonda puede escoger, mensaje por mensaje, o de acuerdo con una política local (por ejemplo, una política-seguridad) fijar una indicación de **criticidad** de un campo-ampliación diferente de la definida en esta Recomendación, relajar o restringir aún más dicha **criticidad**.

```
MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- Prólogo
-- Exporta todo


IMPORTS
        -- Macros del servicio abstracto
        OBJECT, PORT, ABSTRACT-BIND, ABSTRACT-UNBIND, ABSTRACT-OPERATION, ABSTRACT-ERROR
                FROM AbstractServiceNotation { joint-iso-ccitt mhs-motis(6) asdc(2) modules(0)
                    notation(1) }


        -- Ampliación del servicio abstracto de MM
        forwarding-request
                FROM MSAbstractService { joint-iso-ccitt mhs-motis(6) ms(4) modules(0)
                    abstract-service(1) }


        -- Identificadores de objetos
        id-ot-mts, id-ot-mts-user,
        id-pt-submission, id-pt-delivery, id-pt-administration,
        id-att-physicalRendition-basic,
        id-tok-asymmetricToken
                FROM MTSObjectifiers { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    object-identifiers(0) }


        -- Definiciones de guía
        Name
                FROM InformationFramework { joint-iso-ccitt ds(5) modules(1)
                    information-framework(1) }
        PresentationAddress
                FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) modules(1)
                    selectedAttributeTypes(5) }
        Certificates, AlgorithmIdentifier, ALGORITHM, SIGNED, SIGNATURE, ENCRYPTED
                FROM AuthenticationFramework { joint-iso-ccitt ds(5) modules(1)
                    authentication-framework(7) }
```

FIGURA 2/X.411 (parte 1 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Cotas superiores

ub-bit-options, ub-built-in-content-type, ub-built-in-encoded-information-types,
ub-common-name-length, ub-content-id-length, ub-content-length,
ub-content-types, ub-country-name-alpha-length, ub-country-name-numeric-length,
ub-dl-expansions, ub-domain-defined-attribute-value-length,
ub-domain-defined-attributes, ub-domain-defined-attribute-type-length,
ub-domain-name-length, ub-e163-4-number-length, ub-e163-4-subaddress-length,
ub-encoded-information-types, ub-extension-attributes, ub-extension-types,
ub-generation-qualifier-length, ub-given-name-length, ub-initials-length,
ub-integer-options, ub-labels-and-redirections, ub-local-id-length,
ub-mta-name-length, ub-mts-user-types, ub-numeric-user-id-length,
ub-organization-name-length, ub-organizational-unit-name-length,
ub-organizational-units, ub-password-length, ub-pds-name-length,
ub-pds-parameter-length, ub-pds-physical-address-lines, ub-postal-code-length, ub-privacy-mark-length,
ub-queue-size, ub-reason-codes, ub-recipients,
ub-recipient-number-for-advice-length, ub-redirections, ub-security-categories
ub-security-labels, ub-security-problems, ub-supplementary-info-length,
ub-surname-length, ub-terminal-id-length, ub-tsap-id-length,
ub-informated-address-length, ub-x121-address-length

        FROM MTSUpperBounds { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                upper-bounds(3) };
```

FIGURA 2/X.411 (parte 1 *bis* de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Objetos

mTS OBJECT
        PORTS { submission [S], delivery [S], administration [S] }
        ::= id-ot-mts

mTSUser OBJECT
        PORTS { submission [C], delivery [C], administration [C] }
        ::= id-ot-mts-user


-- Puertos

submission PORT
        CONSUMER INVOKES { MessageSubmission, ProbeSubmission, CancelDeferredDelivery }
        SUPPLIER INVOKES { SubmissionControl }
        ::= id-pt-submission

delivery PORT
        CONSUMER INVOKES { DeliveryControl }
        SUPPLIER INVOKES { MessageDelivery, ReportDelivery }
        ::= id-pt-delivery

administration PORT
        CONSUMER INVOKES { ChangeCredentials, Register }
        SUPPLIER INVOKES { ChangeCredentials }
        ::= id-pt-administration
```

FIGURA 2/X.411 (parte 2 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Vinculación – STRM y Desvinculación – STRM

MTSBind ::= ABSTRACT-BIND
        TO {submission, delivery, administration}
        BIND
        ARGUMENT SET{
                initiator-name ObjectName,
                messages-waiting [1] EXPLICIT MessagesWaiting OPTIONAL,
                initiator-credentials [2] InitiatorCredentials,
                security-context [3] SecurityContext OPTIONAL}
        RESULT SET{
                responder-name ObjectName,
                messages-waiting [1] EXPLICIT MessagesWaiting OPTIONAL,
                responder-credentials [2] ResponderCredentials}
        BIND-ERROR INTEGER{
                busy (0)
                authentication-error (2),
                unacceptable-dialogue-mode (3),
                unacceptable-security-context (4)} (0. .ub-integer-options)

MTSUnbind ::=ABSTRACT-UNBIND
        FROM {submission, delivery, administration}


-- Parámetros de control de asociación

ObjectName ::= CHOICE{
        mTS-userORAddressAndOptionalDirectoryName,
        mTA [0] MTAName,
        message-store [4] ORAddressAndOptionalDirectoryName}

MessagesWaiting ::= SET{
        urgent [0] DeliveryQueue,
        normal [1] DeliveryQueue,
        non-urgent [2] DeliveryQueue}

DeliveryQueue ::= SET{
        messages [0] INTEGER (0. .ub-queue-size),
        octets [1] INTEGER (0. .ub-content-length) OPTIONAL}

InitiatorCredentials ::= CHOICE{
        simple Password,
        strong [0] StrongCredentials (WITH COMPONENTS{
                ...,
                bind-token PRESENT})}
```

FIGURA 2/X.411 (parte 3 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
ResponderCredentials ::= CHOICE{
        simple Password,
        strong [0] StrongCredentials (WITH COMPONENTS{
                bind-token})}

Password ::= CHOICE{
        IA5String (SIZE (0. .ub-password-length))
        OCTET STRING (SIZE (0. .ub-password-length))}

StrongCredentials ::= SET{
        bind-token [0] Token OPTIONAL,
        certificate [1] Certificates OPTIONAL}

Security Context ::= SET SIZE (1. .ub-security-labels) OF SecurityLabel
```

FIGURA 2/X.411 (parte 4 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Puerto de remisión

MessageSubmission ::= ABSTRACT-OPERATION
        ARGUMENT SEQUENCE {
                envelope MessageSubmissionEnvelope,
                content Content }
        RESULT SET {
                message-submission-identifier MessageSubmissionIdentifier,
                message-submission-time [0] MessageSubmissionTime,
                content-identifier ContentIdentifier OPTIONAL,
                extensions [1] EXTENSIONS CHOSEN FROM {
                    originating-MTA-certificate,
                    proof-of-submission } DEFAULT {} }

        ERRORS {
                SubmissionControlViolated,
                ElementOfServiceNotSubscribed,
                OriginatorInvalid,
                RecipientImproperlySpecified,
                InconsistentRequest,
                SecurityError,
                UnsupportedCriticalFunction,
                RemoteBindError }

ProbeSubmission ::= ABSTRACT-OPERATION
        ARGUMENT
                envelope ProbeSubmissionEnvelope
        RESULT SET {
                probe-submission-identifier ProbeSubmissionIdentifier,
                probe-submission-time [0] ProbeSubmissionTime,
                content-identifier ContentIdentifier OPTIONAL }
        ERRORS {
                SubmissionControlViolated,
                ElementOfServiceNotSubscribed,
                OriginatorInvalid,
                RecipientImproperlySpecified,
                InconsistentRequest,
                SecurityError,
                UnsupportedCriticalFunction,
                RemoteBindError }

CancelDeferredDelivery :: ABSTRACT-OPERATION
        ARGUMENT
                message-submission-identifier MessageSubmissionIdentifier
        RESULT
        ERRORS {
                DeferredDeliveryCancellationRejected,
                MessageSubmissionIdentifierInvalid,
                RemoteBindError }
```

FIGURA 2/X.411 (parte 5 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
SubmissionControl ::= ABSTRACT-OPERATION
        ARGUMENT
                controls SubmissionControls
        RESULT
                waiting Waiting
        ERRORS {
                SecurityError,
                RemoteBindError }

SubmissionControlViolated ::= ABSTRACT-ERROR
        PARAMETER  NULL

ElementOfServiceNotSubscribed ::= ABSTRACT-ERROR
        PARAMETER  NULL

DeferredDeliveryCancellationRejected ::= ABSTRACT-ERROR
        PARAMETER  NULL

OriginatorInvalid ::= ABSTRACT-ERROR
        PARAMETER  NULL

RecipientImproperlySpecified ::= ABSTRACT-ERROR
        PARAMETER
                improperly-specified-recipients SEQUENCE SIZE (1. .ub-recipients OF
                    ORAddressAndOptionalDirectoryName

MessageSubmissionIdentifierInvalid ::= ABSTRACT-ERROR
        PARAMETER  NULL

InconsistentRequest ::= ABSTRACT-ERROR
        PARAMETER  NULL

SecurityError ::= ABSTRACT-ERROR
        PARAMETER
                security-problem SecurityProblem

SecurityProblem ::= INTEGER (0. .ub-security-problems)

UnsupportedCriticalFunction ::= ABSTRACT-ERROR
        PARAMETER  NULL

RemoteBindError ::= ABSTRACT-ERROR
        PARAMETER  NULL
```

FIGURA 2/X.411 (parte 6 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
--Parámetros del puerto de remisión

MessageSubmissionIdentifier ::= MTSIdentifier

MessageSubmissionTime ::= Time

ProbeSubmissionIdentifier ::= MTSIdentifier

ProbeSubmissionTime ::= Time

SubmissionControls ::= Controls (WITH COMPONENTS {
        permissible-content-types ABSENT,
        permissible-encoded-information-types ABSENT })

Waiting ::= SET {
        waiting-operations [0] Operations DEFAULT { },
        waiting-messages [1] WaitingMessages DEFAULT { },
        waiting-content-types [2] SET SIZE (0. .ub-content-types) OF ContentType DEFAULT { },
        waiting-encoded-information-types EncodedInformationTypes OPTIONAL }

Operations ::= BIT STRING {
        probe-submission-or-report-delivery (0),
        message-submission-or-message-delivery (1) } (SIZE (0. .ub-bit-options))
        --con retención 'UNO', sin retención 'CERO'

WaitingMessages ::= BIT STRING {
        long-content (0),
        low-priority (1),
        other-security-labels (2) } (SIZE (0. .ub-bit-options))
```

FIGURA 2/X.411 (parte 7 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Puerto de entrega

MessageDelivery ::= ABSTRACT-OPERATION
        ARGUMENT SEQUENCE {
                COMPONENTS OF MessageDeliveryEnvelope,
                content Content }
        RESULT SET {
                recipient-certificate [0] RecipientCertificate OPTIONAL,
                proof-of-delivery [1] ProofOfDelivery OPTIONAL } DEFAULT { }
        ERRORS {
                DeliveryControlViolated,
                SecurityError,
                UnsupportedCriticalFunction }

ReportDelivery ::= ABSTRACT-OPERATION
        ARGUMENT SET {
                COMPONENTS OF ReportDeliveryEnvelope,
                returned-content [0] Content OPTIONAL }
        RESULT
        ERRORS {
                DeliveryControlViolated,
                SecurityError,
                UnsupportedCriticalFunction }

DeliveryControl ::= ABSTRACT-OPERATION
        ARGUMENT
                controls DeliveryControls
        RESULT
                waiting Waiting
        ERRORS {
                ControlViolatesRegistration,
                SecurityError }

DeliveryControlViolated ::= ABSTRACT-ERROR
        PARAMETER  NULL

ControlViolatesRegistration ::= ABSTRACT-ERROR
        PARAMETER  NULL


-- Error de seguridad – definido en la figura 2/X.411, parte 6 de 41

-- Función crítica no soportada – definida en la figura 2/X.411, parte 6 de 41
```

FIGURA 2/X.411 (parte 8 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Parámetros del puerto de entrega

RecipientCertificate ::= Certificates

ProofOfDelivery ::= SIGNATURE SEQUENCE {
        algorithm-identifier ProofOfDeliveryAlgorithmIdentifier,
        delivery-time MessageDeliveryTime,
        this-recipient-name ThisRecipientName,
        originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
        content Content,
        content-identifier ContentIdentifier OPTIONAL,
        message-security-label MessageSecurityLabel OPTIONAL }

ProofOfDeliveryAlgorithmIdentifier ::= AlgorithmIdentifier

DeliveryControls ::= Controls

Controls ::= SET {
        restrict [0] BOOLEAN DEFAULT TRUE,
        -- update 'TRUE', remove 'FALSE'
        permissible-operations [1] Operations OPTIONAL,
        permissible-maximum-content-length [2] ContentLength OPTIONAL,
        permissible-lowest-priority Priority OPTIONAL,
        permissible-content-types [4] SET SIZE (1. .ub-content-types) OF ContentType OPTIONAL,
        permissible-encoded-information-types EncodedInformationTypes OPTIONAL,
        permissible-security-context [5] SecurityContext OPTIONAL }

-- Nota – Los rótulos [0], [1] y [2] sólo se alteran para la operación de registro.
```

FIGURA 2/X.411 (parte 9 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Puerto de administración

Register ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                user-name UserName OPTIONAL,
                user-address [0] UserAddress OPTIONAL,
                deliverable-encoded-information-types EncodedInformationTypes OPTIONAL,
                deliverable-maximum-content-length [1] EXPLICIT ContentLength OPTIONAL,
                default-delivery-controls [2] EXPLICIT DefaultDeliveryControls OPTIONAL,
                deliverable-content-types [3] SET SIZE (1 . .ub-content-types) OF ContentType OPTIONAL,
                labels-and-redirections [4] SET SIZE (1. .ub-labels-and-redirections) OF
                    LabelAndRedirection OPTIONAL }
        RESULT
        ERRORS{
                RegisterRejected }

ChangeCredentials ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                old-credentials [0] Credentials,
                new-credentials [1] Credentials -- same CHOICE as for old-credentials -- }
        RESULT
        ERRORS{
                NewCredentialsUnacceptable,
                OldCredentialsIncorrectlySpecified }

RegisterRejected ::= ABSTRACT-ERROR
        PARAMETER  NULL

NewCredentialsUnacceptable ::= ABSTRACT-ERROR
        PARAMETER  NULL

OldCredentialsIncorrectlySpecified ::= ABSTRACT-ERROR
        PARAMETER  NULL
```

FIGURA 2/X.411 (parte 10 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Parámetros del puerto de administración

UserName ::= ORAddressAndOptionalDirectoryName

UserAddress ::= CHOICE {
        x121 [0] SEQUENCE {
                x121-address NumericString (Size (1. .ub-x121-address-length)) OPTIONAL,
                tsap-id PrintableString (SIZE (1. .ub-tsap-id-length)) OPTIONAL },
        presentation [1] PSAPAddress }

PSAPAddress ::= PresentationAddress

DefaultDeliveryControls ::= Controls (WITH COMPONENTS {
        ...,
        permissible-security-context ABSENT })

Credentials ::= CHOICE {
        simple Password,
        strong [0] StrongCredentials (WITH COMPONENTS {
                certificate }) }

LabelAndRedirection ::= SET {
        user-security-label [0] UserSecurityLabel OPTIONAL,
        recipient-assigned-alternate-recipient [1] RecipientAssignedAlternateRecipient OPTIONAL }

UserSecurityLabel ::= SecurityLabel

RecipientAssignedAlternateRecipient ::= ORAddressAndOptionalDirectoryName
```

FIGURA 2/X.411 (parte 11 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Sobre de remisión del mensaje

MessageSubmissionEnvelope ::= SET{
        COMPONENTS OF PerMessageSubmissionFields,
        per-recipient-fields [1] SEQUENCE SIZE (1..ub-recipients) OF
                PerRecipientMessageSubmissionFields }

PerMessageSubmissionFields ::= SET{
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        priority Priority DEFAULT normal,
        per-message-indicators PerMessageIndicators DEFAULT {},
        deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
        extensions [2] PerMessageSubmissionExtensions DEFAULT {}}

PerMessageSubmissionExtensions ::= EXTENSIONS CHOSEN FROM{
        recipient-reassignment-prohibited,
        dl-expansion-prohibited,
        conversion-with-loss-prohibited,
        latest-delivery-time
        originator-return-address,
        originator-certificate,
        content-confidentiality-algorithm-identifier,
        message-origin-authentication-check,
        message-security-label,
        proof-of-submission-request,
        content-correlator,
        forwarding-request -- for MS Abstract Service only --}

PerRecipientMessageSubmissionFields ::= SET{
        recipient-name RecipientName,
        originator-report-request [0] OriginatorReportRequest,
        explicit-conversion [1] ExplicitConversion OPTIONAL,
        extensions [2] PerRecipientMessageSubmissionExtensions DEFAULT {}}

PerRecipientMessageSubmissionExtensions ::= EXTENSIONS CHOSEN FROM{
        originator-requested-alternate-recipient,
        requested-delivery-method,
        physical-forwarding-prohibited,
        physical-forwarding-address-request,
        physical-delivery-modes,
        registered-mail-type,
        recipient-number-for-advice,
        physical-rendition-attributes,
        physical-delivery-report-request,
        message-token,
        content-integrity-check,
        proof-of-delivery-request }
```

FIGURA 2/X.411 (parte 12 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Sobre de remisión de sonda

ProbeSubmissionEnvelope ::= SET{
        COMPONENTS OF PerProbeSubmissionFields,
        per-recipient-fields [3] SEQUENCE SIZE (1. .ub-recipients) OF
                PerRecipientProbeSubmissionFields }

PerProbeSubmissionFields ::= SET{
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT {},
        extensions [2] EXTENSIONS CHOSEN FROM{
                recipient-reassignment-prohibited,
                dl-expansion-prohibited,
                conversion-with-loss-prohibited,
                originator-certificate,
                message-security-label,
                content-correlator,
                probe-origin-authentication-check } DEFAULT {}}

PerRecipientProbeSubmissionFields ::= SET{
        recipient-name RecipientName,
        originator-report-request [0] OriginatorReportRequest,
        explicit-conversion [1] ExplicitConversion OPTIONAL,
        extensions [2] EXTENSIONS CHOSEN FROM{
                originator-requested-alternate-recipient,
                requested-delivery-method
                physical-rendition-attributes } DEFAULT {}}
```

FIGURA 2/X.411 (parte 13 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Sobre de entrega de mensajes

MessageDeliveryEnvelope ::= SEQUENCE {
        message-delivery-identifier MessageDeliveryIdentifier,
        message-delivery-time MessageDeliveryTime,
        other-fields OtherMessageDeliveryFields }

OtherMessageDeliveryFields ::= SET {
        content-type DeliveredContentType,
        originator-name OriginatorName,
        original-encoded-information-types [1] OriginalEncodedInformationTypes OPTIONAL,
        priority Priority DEFAULT normal,
        delivery-flags [2] DeliveryFlags OPTIONAL,
        other-recipient-names [3] OtherRecipientNames OPTIONAL,
        this-recipient-name [4] ThisRecipientName,
        originally-intended-recipient-name [5] OriginallyIntendedRecipientName OPTIONAL,
        converted-encoded-information-types [6] ConvertedEncodedInformationTypes OPTIONAL,
        message-submission-time [7] MessageSubmissionTime,
        content-identifier [8] ContentIdentifier OPTIONAL,
        extensions [9] EXTENSIONS CHOSEN FROM {
                conversion-with-loss-prohibited,
                requested-delivery-method,
                physical-forwarding-prohibited,
                physical-forwarding-address-request,
                physical-delivery-modes,
                registered-mail-type,
                recipient-number-for-advice,
                physical-rendition-attributes,
                originator-return-address,
                physical-delivery-report-request,
                originator-certificate,
                message-token,
                content-confidentiality-algorithm-identifier,
                content-integrity-check,
                message-origin-authentication-check,
                message-security-label,
                proof-of-delivery-request,
                redirection-history,
                dl-expansion-history } DEFAULT {}}
```

FIGURA 2/X.411 (parte 14 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Sobre de entrega de informe

ReportDeliveryEnvelope ::= SET {
        COMPONENTS OF PerReportDeliveryFields,
        per-recipient-fields SEQUENCE SIZE (1. .ub-recipients) OF PerRecipientReportDeliveryFields }

PerReportDeliveryFields ::= SET {
        subject-submission-identifier SubjectSubmissionIdentifier,
        content-identifier ContentIdentifer OPTIONAL,
        content-type ContentType OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        extension [1] EXTENSIONS CHOSEN FROM {
                message-security-label,
                content-correlator,
                originator-and-DL-expansion-history,
                reporting-DL-name,
                reporting-MTA-certificate,
                report-origin-authentication-check } DEFAULT {} }

PerRecipientReportDeliveryFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        report-type [1] ReportType,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        originally-intended-recipient-name [2] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [3] SupplementaryInformation OPTIONAL,
        extensions [4] EXTENSIONS CHOSEN FROM {
                redirection-history,
                physical-forwarding-address,
                recipient-certificate,
                proof-of-delivery } DEFAULT {} }

ReportType ::= CHOICE {
        delivery [0] DeliveryReport,
        non-delivery [1] NonDeliveryReport }

DeliveryReport ::= SET {
        message-delivery-time [0] MessageDeliveryTime,
        type-of-MTS-user [1] TypeOfMTSUser DEFAULT public }

NonDeliveryReport ::= SET {
        non-delivery-reason-code [0] NonDeliveryReasonCode,
        non-delivery-diagnostic-code [1] NonDeliveryDiagnosticCode OPTIONAL }
```

FIGURA 2/X.411 (parte 15 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Campos de sobre

OriginatorName :: = ORAddressAndOrDirectoryName

OriginalEncodedInformationTypes ::= EncodedInformationTypes

ContentType ::= CHOICE{
        built-in BuiltInContentType,
        external ExternalContentType}

BuiltInContentType ::= [APPLICATION 6] INTEGER{
        unidentified (0),
        external (1),                          -- identified by the object-identifier of the EXTERNAL content
        interpersonal-messaging-1984 (2),
        interpersonal-messaging-1988 (22)} (0. .ub-built-in-content-type)

ExternalContentType ::= OBJECT IDENTIFIER

DeliveredContentType ::= CHOICE{
        built-in [0] BuiltInContentType,
        external ExternalContentType}

ContentIdentifier ::= [APPLICATION 10] PrintableString (SIZE (1. .ub-content-id-length))

PerMessageIndicators ::= [APPLICATION 8] BIT STRING{
        disclosure-of-recipients (0),          -- disclosure-of-recipients-allowed 'one',
                                               -- disclosure-of-recipient-prohibited 'zero',
                                               -- ignored for Probe-submission
        implicit-conversion-prohibited (1),    -- implicit-conversion-prohibited 'one';
                                               -- implicit-conversion-allowed 'zero'
        alternate-recipient-allowed (2),       -- alternate-recipient-allowed 'one',
                                               -- alternate-recipient-prohibited 'zero'
        content-return-request (3)             -- content-return-requested 'one',
                                               -- content-return-not-requested 'zero';
                                               -- ignored for Probe-submission --}
        (SIZE (0. .ub-bit-options))

RecipientName ::= ORAddressAndOrDirectoryName

OriginatorReportRequest ::= BIT STRING{
        report (3),
        non-delivery-report (4)
        -- at most one bit shall be 'one':
        -- report bit 'one' requests a 'report';
        -- non-delivery-report bit 'one' requests a 'non-delivery-report';
        -- both bits 'zero' requests 'no-report' --} (SIZE (0. .ub-bit-options))
```

FIGURA 2/X.411 (parte 16 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
ExplicitConversion ::= INTEGER {
        ia5-text-to-teletex (0),
        teletex-to-telex (1),
        telex-to-ia5-text (2),
        telex-to-teletex (3),
        telex-to-g4-class-1 (4),
        telex-to-videotex (5),
        ia5-text-to-telex (6),
        telex-to-g3-facsimile (7),
        ia5-text-to-g3-facsimile (8),
        ia5-text-to-g4-class-1 (9),
        ia5-text-to-videotex (10),
        teletex-to-ia5-text (11),
        teletex-to-g3-facsimile (12),
        teletex-to-g4-class-1 (13),
        teletex-to-videotex (14),
        videotex-to-telex (15),
        videotex-to-ia5-text (16),
        videotex-to-teletex (17) } (0. .ub-integer-options)

DeferredDeliveryTime ::= Time

Priority ::= [APPLICATION 7] ENUMERATED {
        normal (0),
        non-urgent (1),
        urgent (2) }

ContentLength ::= INTEGER (0. .ub-content-length)

MessageDeliveryIdentifier ::= MTSIdentifier

MessageDeliveryTime ::= Time

DeliveryFlags ::= BIT STRING {
        implicit-conversion-prohibited (1)          -- implicit-conversion-prohibited 'one',
                                                    -- implicit-conversion-allowed 'zero' -- }
        (SIZE (0. .ub-bit-options))

OtherRecipientNames ::= SEQUENCE SIZE (1. .ub-recipients) OF OtherRecipientName

OtherRecipientName ::= OrAddressAndOrDirectoryName

ThisRecipientName ::= OrAddressAndOrDirectoryName

OriginallyIntendedRecipientName ::= OrAddressAndOrDirectoryName
```

FIGURA 2/X.411 (parte 17 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
ConvertedEncodedInformationTypes ::= EncodedInformationTypes

SubjectSubmissionIdentifier ::= MTSIdentifier

ActualRecipientName ::= ORAddressAndOrDirectoryName

TypeOfMTSUser ::= INTEGER {
        public (0),
        private (1),
        ms (2),
        dl (3),
        pdau (4),
        physical-recipient (5),
        other (6) } (0. .ub-mts-user-types)

NonDeliveryReasonCode ::= INTEGER {
        transfer-failure (0),
        unable-to-transfer (1),
        conversion-not-performed (2),
        physical-rendition-not-performed (3),
        physical-delivery-not-performed (4),
        restricted-delivery (5),
        directory-operation-unsuccessful (6) } (0. .ub-reason-codes)

NonDeliveryDiagnosticCode ::= INTEGER {
        unrecognised-OR-name (0),
        ambiguous-OR-name (1),
        mts-congestion (2),
        loop-detected (3),
        recipient-unavailable (4),
        maximum-time-expired (5),
        encoded-information-types-unsupported (6),
        content-too-long (7),
        conversion-impractical (8),
        implicit-conversion-prohibited (9),
        implicit-conversion-not-subscribed (10),
        invalid-arguments (11),
        content-syntax-error (12),
        size-constraint-violation (13),
        protocol-violation (14),
        content-type-not-supported (15),
        too-many-recipients (16),
        no-bilateral-agreement (17),
        unsupported-critical-function (18),

        -- continuación
```

FIGURA 2/X.411 (parte 18 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

-- continuación

```
conversion-with-loss-prohibited (19),
line-too-long (20),
page-split (21),
pictorial-symbol-loss (22),
punctuation-symbol-loss (23),
alphabetic-character-loss (24),
multiple-information-loss (25),
recipient-reassignment-prohibited (26),
redirection-loop-detected (27),
dL-expansion-prohibited (28),
no-DL-submit-permission (29),
dl-expansion-failure (30),
physical-rendition-attributes-not-supported (31),
undeliverable-mail-physical-delivery-address-incorrect (32),
undeliverable-mail-physical-delivery-office-incorrect-or-invalid (33),
undeliverable-mail-physical-delivery-address-incomplete (34),
undeliverable-mail-recipient-unknown (35),
undeliverable-mail-recipient-deceased (36),
undeliverable-mail-organization-expired (37),
undeliverable-mail-recipient-refused-to-accept (38),
undeliverable-mail-recipient-did-not-claim (39),
undeliverable-mail-recipient-changed-address-permanently (40),
undeliverable-mail-recipient-changed-address-temporarily (41),
undeliverable-mail-recipient-changed-temporary-address (42),
undeliverable-mail-new-address-unknown (43),
undeliverable-mail-recipient-did-not-want-forwarding (44),
undeliverable-mail-originator-prohibited-forwarding (45),
secure-messaging-error (46),
unable-to-downgrade (47) } (0. .ub-diagnostic-codes)
SupplementaryInformation ::= PrintableString (SIZE (1. .ub-supplementary-info-length))
```

FIGURA 2/X.411 (parte 19 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Campos de ampliación

ExtensionField ::= SEQUENCE {
        type [0] EXTENSION,
        criticality [1] Criticality DEFAULT { },
        value [2] AND DEFINED BY type DEFAULT NULL NULL }

Criticality ::= BIT STRING {
        for-submission (0),
        for-transfer (1),
        for-delivery (2) } (SIZE (0. .ub-bit-options))      -- critical 'one', non-critical 'zero'

EXTENSIONS MACRO ::=
BEGIN

TYPE NOTATION ::= "CHOSEN FROM" "{ "ExtensionList" }"
VALUE NOTATION ::= Value (VALUE SET OF ExtensionField      -- each of a different type --)

ExtensionList ::= Extension"," ExtensionList | Extension | empty
Extension ::= value (EXTENSION)

END     -- of EXTENSIONS

EXTENSION MACRO ::=
BEGIN

TYPE NOTATION ::= DataType Critical | empty
VALUE NOTATION ::= value (VALUE ExtensionType)

DataType ::= type (X) Default | empty
Default ::= "DEFAULT" value (X) | empty
Critical ::= "CRITICAL FOR" CriticalityList | empty
CriticalityList ::= Criticality | CriticalityList "," Criticality
Criticality ::= "SUBMISSION" | "TRANSFER" | "DELIVERY"

END   -- of EXTENSION

ExtensionType ::= INTEGER (0. .ub-extension-types)

recipient-reassignment-prohibited EXTENSION
        RecipientReassignmentProhibited DEFAULT recipient-reassignment-allowed
        CRITICAL FOR DELIVERY
        ::= 1
```

FIGURA 2/X.411 (parte 20 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
RecipientReassignmentProhibited ::= ENUMERATED {
        recipient-reassignment-allowed (0),
        recipient-reassignment-prohibited (1) }

originator-requested-alternate-recipient EXTENSION
        OriginatorRequestedAlternateRecipient
        CRITICAL FOR SUBMISSION
        ::= 2

OriginatorRequestedAlternateRecipient ::= ORAddressAndOrDirectoryName

-- OriginatorRequestedAlternateRecipient, tal como aquí se define, difiere
-- del campo del mismo nombre de la figura 4/X.411, ya que no es necesario
-- que esté presente al remitir la dirección-OD, pero sí debe estar
-- presente al transferir la dirección-OD

dl-expansion-prohibited EXTENSION
        DLExpansionProhibited DEFAULT dl-expansion-allowed
        CRITICAL FOR DELIVERY
        ::= 3

DLExpansionProhibited ::= ENUMERATED {
        dl-expansion-allowed (0),
        dl-expansion-prohibited (1) }

conversion-with-loss-prohibited EXTENSION
        ConversionWithLossProhibited DEFAULT conversion-with-loss-allowed
        CRITICAL FOR DELIVERY
        ::= 4

ConversionWithLossProhibited ::= ENUMERATED {
        conversion-with-loss-allowed (0),
        conversion-with-loss-prohibited (1) }

latest-delivery-time EXTENSION
        LatestDeliveryTime
        CRITICAL FOR DELIVERY
        ::= 5

LatestDeliveryTime ::= Time

requested-delivery-method EXTENSION
        RequestedDeliveryMethod DEFAULT any-delivery-method
        CRITICAL FOR DELIVERY
        ::= 6
```

FIGURA 2/X.411 (parte 21 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
RequestedDeliveryMethod ::= SEQUENCE OF INTEGER { -- cada uno distinto en orden de preferencia siendo
                                                    el primero el más preferido

        any-delivery-method (0),
        mhs-delivery (1),
        physical-delivery (2),
        telex-delivery (3),
        teletex-delivery (4),
        g3-facsimile-delivery (5),
        g4-facsimile-delivery (6),
        ia5-terminal-delivery (7),
        videotex-delivery (8),
        telephone-delivery (9) }  (0. .ub-integer-options)

physical-forwarding-prohibited EXTENSION
        PhysicalForwardingProhibited DEFAULT physical-forwarding-allowed
        CRITICAL FOR DELIVERY
        ::= 7

PhysicalForwardingProhibited ::= ENUMERATED {
        physical-forwarding-allowed (0),
        physical-forwarding-prohibited (1) }

physical-forwarding-address-request EXTENSION
        PhysicalForwardingAddressRequest DEFAULT physical-forwarding-address-not-requested
        CRITICAL FOR DELIVERY
        ::= 8

PhysicalForwardingAddressRequest ::= ENUMERATED {
        physical-forwarding-address-not-requested (0),
        physical-forwarding-address-requested (1) }

physical-delivery-modes EXTENSION
        PhysicalDeliveryModes DEFAULT ordinary-mail
        CRITICAL FOR DELIVERY
        ::= 9

PhysicalDeliveryModes ::= BIT STRING {
        ordinary-mail (0),
        special-delivery (1),
        express-mail (2),
        counter-collection (3),
        counter-collection-with-telephone-advice (4),
        counter-collection-with-telex-advice (5),
        counter-collection-with-teletex-advice (6),
        bureau-fax-delivery (7)
        -- los bits 0 a 6 se excluyen mutuamente
        -- el bit 7 puede ser fijado con cualquiera de los bits 0 a 6 -- } (SIZE (0. .ub-bit-options))
```

FIGURA 2/X.411 (parte 22 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
registered-mail-type EXTENSION
        RegisteredMailType DEFAULT non-registered-mail
        CRITICAL FOR DELIVERY
        ::= 10

RegisteredMailType ::= INTEGER
        non-registered-mail (0),
        registered-mail (1),
        registered-mail-to-addresse-in-person (2) } (0. .ub-integer-options)

recipient-number-for-advice EXTENSION
        RecipientNumberForAdvice
        CRITICAL FOR DELIVERY
        ::= 11

RecipientNumberForAdvice ::= TeletexString (SIZE (1. .ub-recipient-number-for-advice-length))

physical-rendition-attributes EXTENSION
        PhysicalRenditionAttributes DEFAULT id-att-physicalRendition-basic
        CRITICAL FOR DELIVERY
        :: = 12

PhysicalRenditionAttributes ::= OBJECT IDENTIFIER

originator-return-address EXTENSION
        OriginatorReturnAddress
        CRITICAL FOR DELIVERY
        ::= 12

OriginatorReturnAddress ::= ORAddress

physical-delivery-report-request EXTENSION
        PhysicalDeliveryReportRequest DEFAULT return-of-undeliverable-mail-by-PDS
        CRITICAL FOR DELIVERY
        ::= 14

PhysicalDeliveryReportRequest::= INTEGER {
        return-of-undeliverable-mail-by-PDS (0),
        return-of-notification-by-PDS (1),
        return-of-notification-by-MHS (2),
        return-of-notification-by-MHS-and-PDS (3) } (0. .ub-integer-options)
```

FIGURA 2/X.411 (parte 23 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
originator-certificate EXTENSION
        OriginatorCertificate
        CRITICAL FOR DELIVERY
        ::= 15

OriginatorCertificate ::= Certificates

message-token EXTENSION
        MessageToken
        ::= 16

MessageToken ::= Token

content-confidentiality-algorithm-identifier EXTENSION
        ContentConfidentialityAlgorithmIdentifier
        ::= 17

ContentConfidentialityAlgorithmIdentifier ::= AlgorithmIdentifier

content-integrity-check EXTENSION
        ContentIntegrityCheck
        ::= 18

ContentIntegrityCheck ::= SIGNATURE SEQUENCE {
        algorithm-identifier ContentIntegrityAlgorithmIdentifier,
        content Content }

ContentIntegrityAlgorithmIdentifier ::= AlgorithmIdentifier

message-origin-authentication-check EXTENSION
        MessageOriginAuthenticationCheck
        CRITICAL FOR DELIVERY
        ::= 19

MessageOriginAuthenticationCheck ::= SIGNATURE SEQUENCE {
        algorithm-identifier MessageOriginAuthenticationAlgorithmIdentifier,
        content Content
        content-identifier ContentIdentifier OPTIONAL,
        message-security-label MessageSecurityLabel OPTIONAL }

MessageOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier
```

FIGURA 2/X.411 (parte 24 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
message-security-label EXTENSION
        MessageSecurityLabel
        CRITICAL FOR DELIVERY
        ::= 20

MessageSecurityLabel ::= SecurityLabel

proof-of-submission-request EXTENSION
        ProofOfSubmissionRequest DEFAULT proof-of-submission-not-requested
        CRITICAL FOR SUBMISSION
        ::= 21

ProofOfSubmissionRequest ::= ENUMERATED {
        proof-of-submission-not-requested (0),
        proof-of-submission-requested (1) }

proof-of-delivery-request EXTENSION
        ProofOfDeliveryRequest DEFAULT proof-of-delivery-not-requested
        CRITICAL FOR DELIVERY
        ::= 22

ProofOfDeliveryRequest ::= ENUMERATED {
        proof-of-delivery-not-requested (0),
        proof-of-delivery-requested (1) }

content-correlator EXTENSION
        ContentCorrelator
        ::= 23

ContentCorrelator ::= ANY       -- maximum ub-content-correlator-length octets including all encoding

probe-origin-authentication-check EXTENSION
        ProbeOriginAuthenticationCheck
        CRITICAL FOR DELIVERY
        ::= 24

ProbeOriginAuthenticationCheck ::= SIGNATURE SEQUENCE {
        algorithm-identifier ProbeOriginAuthenticationAlgorithmIdentifier,
        content-identifier ContentIdentifier OPTIONAL,
        message-security-label MessageSecurityLabel OPTIONAL }

ProbeOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier
```

FIGURA 2/X.411 (parte 25 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
redirection-history EXTENSION
        RedirectionHistory
        ::= 25

RedirectionHistory ::= SEQUENCE SIZE (1. .ub-redirections) OF Redirection

Redirection ::= SEQUENCE {
        intended-recipient-name IntendedRecipientName,
        redirection-reason RedirectionReason }

IntendedRecipientName ::= SEQUENCE {
        OrAddressAndOptionalDirectoryName,
        redirection-time Time }

RedirectionReason ::= ENUMERATED {
        recipient-assigned-alternate-recipient (0),
        originator-requested-alternate-recipient (1),
        recipient-MD-assigned-alternate-recipient (2) }

dl-expansion-history EXTENSION
        DLExpansionHistory
        ::= 26

DLExpansionHistory ::= SEQUENCE SIZE (1. .ub-dl-expansions) OF DLExpansion

DLExpansion ::= SEQUENCE {
        ORAddressAndOptionalDirectoryName,
        dl-expansion-time Time }

physical-forwarding-address EXTENSION
        PhysicalForwardAddress
        ::= 27

PhysicalForwardingAddress ::= ORAddressAndOptionalDirectoryName

recipient-certificate EXTENSION
        RecipientCertificate
        ::= 28

proof-of-delivery EXTENSION
        ProofOfDelivery
        ::= 29

originator-and-DL-expansion-history EXTENSION
        OriginatorAndDLExpansionHistory
        ::= 30

OriginatorAndDLExpansionHistory ::= SEQUENCE SIZE (0. .ub-dl-expansions) OF OriginatorAndDLExpansion

OriginatorAndDLExpansion ::= SEQUENCE {
        originator-or-dl-name ORAddressOptionalDirectoryName,
        origination-or-expansion-time TIME }
```

FIGURA 2/X.411 (parte 26 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
reporting-DL-name EXTENSION
        ReportingDLName
        ::= 31

ReportingDLName ::= ORAddressAndOptionalDirectoryName

reporting-MTA-certificate EXTENSION
        ReportingMTACertificate
        CRITICAL FOR DELIVERY
        ::= 32

ReportingMTACertificate ::= Certificates

report-origin-authentication-check EXTENSION
        ReportOriginAuthenticationCheck
        CRITICAL FOR DELIVERY
        ::= 33

ReportOriginAuthenticationCheck ::= SIGNATURE SEQUENCE {
        algorithm-identifier ReportOriginAuthenticationAlgorithmIdentifier,
        content-identifier ContentIdentifier OPTIONAL,
        message-security-label MessageSecurityLabel OPTIONAL,
        per-recipient SEQUENCE SIZE (1. .ub-recipients) OF PerRecipientReportFields }

ReportOriginAuthenticationAlgorithmIdentifier ::= AlgorithmIdentifier

PerRecipientReportFields ::= SEQUENCE {
        actual-recipient-name ActualRecipientName,
        originally-intended-recipient-name OriginallyIntendedRecipientName OPTIONAL,
        CHOICE {
                delivery [0] PerRecipientDeliveryReportFields,
                non-delivery [1] PerRecipientNonDeliveryReportFields } }

PerRecipientDeliveryReportFields ::= SEQUENCE {
        message-delivery-time MessageDeliveryTime,
        type-of-MTS-user TypeOfMTSUser,
        recipient-certificate [0] RecipientCertificate OPTIONAL,
        proof-of-delivery [1] ProofOfDelivery OPTIONAL }

PerRecipientNonDeliveryReportFields ::= SEQUENCE {
        non-delivery-reason-code NonDeliveryReasonCode,
        non-delivery-diagnostic-code NonDeliveryDiagnosticCode OPTIONAL }
```

FIGURA 2/X.411 (parte 27 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

ARCHIVES U.I.T. GENÈVE

```
originating-MTA-certificate EXTENSION
        OriginatingMTACertificate
        ::= 34

OriginatingMTACertificate ::= Certificates

proof-of-submission EXTENSION
        ProofOfSubmission
        ::= 35

ProofOfSubmission ::= SIGNATURE SEQUENCE {
        algorithm-identifier ProofOfSubmissionAlgorithmIdentifier,
        message-submission-envelope MessageSubmissionEnvelope,
        content Content,
        message-submission-identifier MessageSubmissionIdentifier,
        message-submission-time MessageSubmissionTime }

ProofOfSubmissionAlgorithmIdentifier ::= AlgorithmIdentifier
```

FIGURA 2/X.411 (parte 28 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Tipos de parámetros comunes

Content ::= OCTET STRING        -- cuando el tipo-contenido tiene el valor entero
                                -- externo, el valor de la cadena de octetos de
                                -- contenido es la codificación NSA.1 del contenido-externo
                                -- un contenido-externo es un tipo de datos EXTERNO

MTSIdentifier ::= [APPLICATION 4] SEQUENCE {
        global-domain-identifier GlobalDomainIdentifier,
        local-identifier LocalIdentifier }

LocalIdentifier ::= IA5String (SIZE (1..ub-local-id-length))

GlobalDomainIdentifier ::= [APPLICATION 3] SEQUENCE {
        country-name CountryName,
        administration-domain-name AdministrationDomainName,
        private-domain-identifier PrivateDomainIdentifier OPTIONAL }

PrivateDomainIdentifier ::= CHOICE {
        numeric NumericString (SIZE (1..ub-domain-name-length)),
        printable PrintableString (SIZE (1..ub-domain-name-length)) }

MTAName ::= IA5String (SIZE (1..ub-mta-name-length))

Time ::= UTCTime
```

FIGURA 2/X.411 (parte 29 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Nombres O/D

ORAddressAndOrDirectoryName ::= ORName

ORAddressAndOptionalDirectoryName ::= ORName

ORName ::= [APPLICATION 0] SEQUENCE {
        address COMPONENTS OF ORAddress,
        directory-name [0] Name OPTIONAL }

ORAddress ::= SEQUENCE {
        standard-attributes StandardAttributes,
        domain-defined-attributes DomainDefinedAttributes OPTIONAL,
                -- véase también atributos-definidos-dominio-téletex
        extension-attributes ExtensionAttributes OPTIONAL }

-- Nota – La dirección-OD está semánticamente ausente del nombre-OD si la secuencia de atributo-normal está vacía
-- y se omiten los atributos-definidos-dominio y los atributos-ampliación.


-- Atributos normales

StandardAttributes ::= SEQUENCE
        country-name CountryName OPTIONAL,
        administration-domain-name AdministrationDomainName OPTIONAL,
        network-address [0] NetworkAddress OPTIONAL, -- véase también la dirección-red-ampliada
        terminal-identifier [1] TerminalIdentifier OPTIONAL,
        private-domain-name [2] PrivateDomainName OPTIONAL,
        organization-name [3] OrganizationName OPTIONAL, -- véase también el nombre-organización-teletex
        numeric-user-identifier [4] NumericUserIdentifier OPTIONAL,
        personal-name [5] PersonalName OPTIONAL, -- véase también el nombre personal teletex
        organizational-unit-names [6] OrganizationalUnitNames OPTIONAL
                -- véase también los nombres-unidad-organización-teletex -- }

CountryName ::= [APPLICATION 1] CHOICE {
        x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
        iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length)) }

AdministrationDomainName ::= [APPLICATION 2] CHOICE {
        numeric NumericString (SIZE (0. .ub-domain-name-length)),
        printable PrintableString (SIZE (0. .ub-domain-name-length)) }

NetworkAddress ::= x121Address

X121Address ::= NumericString (SIZE (1. .ub-x121-address-length))

TerminalIdentifier ::= PrintableString (SIZE (1. .ub-terminal-id-length))
```

FIGURA 2/X.411 (parte 30 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
PrivateDomainName ::= CHOICE {
        numeric NumericString (SIZE (1. .ub-domain-name-length)),
        printable PrintableString (SIZE (1. .ub-domain-name-length)), }

OrganizationName ::= Printable String (SIZE (1. .ub-organization-name-length))

NumericUserIdentifier ::= NumericString (SIZE (1. .ub-numeric-user-id-length))

Personal Name ::= SET {
        surname [0] PrintableString (SIZE (1. .ub-surname-length)),
        given-name [1] PrintableString (SIZE (1. .ub-given-name-length)), OPTIONAL,
        initials [2] PrintableString (SIZE (1. .ub-initials-length)) OPTIONAL }
        generation-qualifier [3] PrintableString (SIZE (1. .ub-generation-qualifier-length)) OPTIONAL }

OrganizationUnitNames ::= SEQUENCE SIZE (1. .ub-organizational-units) OF OrganizationUnitName

OrganizationUnitName ::= PrintableString (SIZE (1. .ub-organizational-unit-name-length))


-- Atributos definidos-dominio

DomainDefinedAttributes ::= SEQUENCE SIZE (1. .ub-domain-defined-attributes) OF DomainDefinedAttribute

DomainDefinedAttribute ::= SEQUENCE {
        type PrintableString (SIZE (1. .ub-domain-attribute-type-length)),
        value PrintableString (SIZE (1. .ub-domain-defined-attribute-value-length)) }


-- Atributos de prolongación

ExtensionAttributes ::= SET SIZE (1. .ub-extension-attributes) OF ExtensionAttribute

ExtensionAttribute ::= SEQUENCE {
        extension-attribute-type [0] EXTENSION-ATTRIBUTE,
        extension-attribute-value [1] ANY DEFINED BY extension-attribute-type }

EXTENSION-ATTRIBUTE MACRO ::=
BEGIN

TYPE NOTATION::= TYPE | empty
VALUE NOTATION ::= value (VALUE INTEGER (0. .ub-extension-attributes))

END  -- de ATRIBUTO-PROLONGACIÓN
```

FIGURA 2/X.411 (parte 31 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
common-name EXTENSION-ATTRIBUTE
        CommonName
        ::= 1

CommonName ::= PrintableString (SIZE (1. . .ub-common-name-length))

teletex-common-name EXTENSION-ATTRIBUTE
        TeletexCommonName
        ::= 2

TeletexCommonName ::= TeletexString (SIZE (1. . .ub-common-name-length))

teletex-organization-name EXTENSION-ATTRIBUTE
        TeletexOrganizationName
        ::= 3

TeletexOrganizationName ::= TeletexString (SIZE (1. . .ub-organization-name-length))

teletex-personal-name EXTENSION-ATTRIBUTE
        TeletexPersonalName
        ::= 4

TeletexPersonalName ::= SET{
        surname [0] TeletexString (SIZE (1. . .ub-surname-length)),
        given-name [1] TeletexString (SIZE (1. . .ub-given-name-length)) OPTIONAL,
        initials [2] TeletexString (SIZE (1. . .ub-initials-length)) OPTIONAL,
        generation-qualifier [3] TeletexString (SIZE (1. . .ub-generation-qualifier-length)) OPTIONAL}

teletex-organizational-unit-names EXTENSION-ATTRIBUTE
        TeletexOrganizationalUnitNames
        ::= 5

TeletexOrganizationUnitNames ::= SEQUENCE (SIZE (1. . .ub-organizational-units) OF
        TeletexOrganizationalUnitName

TeletexOrganizationalUnitName ::= TeletexString (SIZE (1. . .ub-organizational-unit-name-length))

teletex-domain-defined-attributes EXTENSION-ATTRIBUTE
        TeletexDomainDefinedAttributes
        ::= 6

TeletexDomainDefinedAttributes ::= SEQUENCE SIZE (1. . .ub-domain-defined-attributes) OF
        TeletexDomainDefinedAttribute
```

FIGURA 2/X.411 (parte 32 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
TeletexDomainDefinedAttribute ::= SEQUENCE {
        typeTeletexString (SIZE (1...ub-domain-defined-attribute-type-length)),
        value TeletexString (SIZE (1...ub-domain-defined-attribute-value-length))}

pds-name EXTENSION-ATTRIBUTE
        PDSName
        ::= 7

PDSName ::= PrintableString (SIZE (1...ub-pds-name-length))

physical-delivery-country-name EXTENSION-ATTRIBUTE
        PhysicalDeliveryCountryName
        ::= 8

PhysicalDeliveryCountryName ::= CHOICE {
        x121-dcc-code NumericString (SIZE (ub-country-name-numeric-length)),
        iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length))}

postal-code EXTENSION-ATTRIBUTE
        PostalCode
        ::= 9

PostalCode ::= CHOICE {
        numeric-code NumericString (SIZE (1...ub-postal-code-length)),
        printable-code PrintableString (SIZE (1...ub-postal-code-length))}

physical-delivery-office-name EXTENSION-ATTRIBUTE
        PhysicalDeliveryOfficeName
        ::= 10

PhysicalDeliveryOfficeName ::= PDS Parameter

physical-delivery-office-number EXTENSION-ATTRIBUTE
        PhysicalDeliveryOfficeNumber
        ::= 11

PhysicalDeliveryOfficeNumber ::= PDS Parameter

extension-OR-address-components EXTENSION-ATTRIBUTE
        ExtensionORAddressComponents
        ::= 12
```

FIGURA 2/X.411 (parte 33 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
ExtensionORAddressComponents ::= PDS Parameter

physical-delivery-personal-name EXTENSION-ATTRIBUTE
        PhysicalDeliveryPersonalName
        ::= 13

PhysicalDeliveryPersonalName ::= PDS Parameter

physical-delivery-organization-name EXTENSION-ATTRIBUTE
        PhysicalDeliveryOrganizationName
        ::= 14

PhysicalDeliveryOrganizationName ::= PDS Parameter

extension-physical-delivery-address-components EXTENSION-ATTRIBUTE
        ExtensionPhysicalDeliveryAddressComponents
        ::= 15

ExtensionPhysicalDeliveryAddressComponents ::= PDS Parameter

unformatted-postal-address EXTENSION-ATTRIBUTE
        UnformattedPostalAddress
        ::= 16

UnformattedPostalAddress ::= SET{
        printable-address SEQUENCE SIZE (1. . .ub-pds-physical-address-lines) OF
                PrintableString (SIZE (1. . .ub-pds-parameter-length)) OPTIONAL,
        teletex-string TeletexString (SIZE (1. . .ub-unformatted-address-length)) OPTIONAL}

street-address EXTENSION-ATTRIBUTE
        StreetAddress
        ::= 17

StreetAddress ::= PDS Parameter
```

FIGURA 2/X.411 (parte 34 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
post-office-box-address EXTENSION-ATTRIBUTE
        PostOfficeBoxAddress
        ::= 18

PostOfficeBoxAddress ::= PDS Parameter

poste-restante-address EXTENSION-ATTRIBUTE
        PosteRestanteAddress
        ::= 19

PosteRestanteAddress ::= PDS Parameter

unique-postal-name EXTENSION-ATTRIBUTE
        UniquePostalName
        ::= 20

UniquePostalName ::= PDS Parameter

local-postal-attributes EXTENSION-ATTRIBUTE
        LocalPostalAttributes
        ::= 21

LocalPostalAttributes ::= PDS Parameter

PDS Parameter ::= SET
        printable-string PrintableString (SIZE (1. . .ub-pds-parameter-length)) OPTIONAL,
        teletex-string TeletexString (SIZE (1. . .ub-pds-parameter-length)) OPTIONAL }

extended-network-address EXTENSION-ATTRIBUTE
        ExtendedNetworkAddress
        ::= 22

ExtendedNetworkAddress ::= CHOICE {
        e163-4-address SEQUENCE {
                number [0] NumericString (SIZE (1. . .ub-e163-4-number-length)),
                sub-address [1] NumericString (SIZE (1. . .ub-e163-4-sub-address-length)) OPTIONAL }
        psap-address [0] PresentationAddress }

terminal-type EXTENSION-ATTRIBUTE
        TerminalType
        ::= 23
```

FIGURA 2/X.411 (parte 35 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
TerminalType ::= INTEGER {
        telex (3),
        teletex (4),
        g3-facsimile (5),
        g4-facsimile (6),
        ia5-terminal (7),
        videotex (8) } (0. . .ub-integer-options)
```

FIGURA 2/X.411 (parte 36 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Tipos de información codificada

EncodedInformationTypes ::= [APPLICATION 5] SET {
        built-in-encoded-information-types [0] BuiltInEncodedInformationTypes,
        non-basic-parameters COMPONENTS OF NonBasicParameters,
        external-encoded-information-types [4] ExternalEncodedInformationTypes OPTIONAL }


-- Tipos de información codificada incorporados

Built-inEncodedInformationTypes ::= BIT STRING {
        undefined (0),
        telex (1),
        ia5-text (2),
        g3-facsimile (3),
        g4-class-1 (4),
        teletex (5),
        videotex (6),
        voice (7),
        sfd (8),
        mixed-mode (9) } (SIZE (0. . .ub-built-in-encoded-information-types))


-- Parámetros no-básicos

NonBasicParameters ::= SET {
        g3-facsimile [1]G3FacsimileNonBasicParameters DEFAULT {},
        teletex [2] TeletexNonBasicParameters DEFAULT {},
        g4-class-1-and-mixed-mode [3] G4Class1AndMixedModeNonBasicParameters OPTIONAL }

G3FacsimileNonBasicParameters ::= BIT STRING {
        two-dimensional (8),
        fine-resolution (9),
        unlimited-length (20),
        b4-length (21),
        a3-width (22),
        b4-width (23),
        uncompressed (30) }                    -- según se define en la Recomendación T.30

TeletexNonBasicParameters ::= SET {
        graphic-character-sets [0] TeletexString OPTIONAL,
        control-character-sets [1] TeletexString OPTIONAL,
        page-formats [2] OCTET STRING OPTIONAL,
        miscellaneous-terminal-capabilities [3] TeletexString OPTIONAL,
        private-use [4] OCTET STRING OPTIONAL      -- maximum ub-teletex-private-use-length octets -- }
        -- según se define en la Recomendación T.62
```

FIGURA 2/X.411 (parte 37 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
G4Class1AndMixedModeNonBasicParameters ::= PresentationCapabilities

PresentationCapabilities ::= ANY        -- según se define en las Recomendaciones T.400 T.503 y T.501


-- Tipos de información codificada externos

ExternalEncodedInformationTypes ::= SET SIZE (1. . .ub-encoded-information-types) OF
        ExternalEncodedInformationType

ExternalEncodedInformationTypes ::= OBJECT IDENTIFIER
```

FIGURA 2/X.411 (parte 38 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
-- Testigo

Token ::= SEQUENCE {
        token-type-identifier [0] TOKEN,
        token [1] ANY DEFINED BY token-type-identifier }

TOKEN MACRO ::=
BEGIN

TYPE NOTATION ::= type | empty
VALUE NOTATION ::= value (VALUE OBJECT IDENTIFIER)

END  -- of TOKEN

asymmetric-token TOKEN
                AsymmetricToken
        ::= id-tok-asymmetricToken

AsymmetricToken ::= SIGNED SEQUENCE {
        signature-algorithm-identifier AlgorithmIdentifier,
        recipient-name RecipientName,
        time Time,
        signed-data [0] TokenData OPTIONAL,
        encryption-algorithm-identifier [1] AlgorithmIdentifier OPTIONAL,
        encrypted-data [2] ENCRYPTED TokenData OPTIONAL }

TokenData ::= SEQUENCE {
        type [0] TOKEN-DATA,
        value [1] ANY DEFINED BY type }

TOKEN-DATA MACRO ::=
BEGIN

TYPE NOTATION ::= type | empty
VALUE NOTATION ::= value (VALUE INTEGER)

END  -- TOKEN-DATA

bind-token-signed-data TOKEN-DATA
                BindTokenSignedData
        ::=

BindTokenSignedData ::= RandomNumber
```

FIGURA 2/X.411 (parte 39 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
RandomNumber ::= BIT STRING

message-token-signed-data TOKEN-DATA
                MessageTokenSignedData
        ::= 2

MessageTokenSignedData ::= SEQUENCE {
        content-confidentiality-alogorithm-identifier [0] ContentConfidentialityAlgorithmIdentifier
                OPTIONAL,
        content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
        message-security-label [2] MessageSecurityLabel OPTIONAL,
        proof-of-delivery-request [3] ProofOfDeliveryRequest OPTIONAL,
        message-sequence-number [4] INTEGER OPTIONAL }

message-token-encrypted-data TOKEN-DATA
                MessageTokenEncryptedData
        ::= 3

MessageTokenEncryptedData ::= SEQUENCE {
        content-confidentiality-key [0] EncryptionKey OPTIONAL,
        content-integrity-check [1] ContentIntegrityCheck OPTIONAL,
        message-security-label [2] MessageSecurityLabel OPTIONAL,
        content-integrity-key [3] EncryptionKey OPTIONAL,
        message-sequence-number [4] INTEGER OPTIONAL }

EncryptionKey ::= BIT STRING


-- Etiqueta de seguridad

Security label ::= SET {
        security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
        security-classification SecurityClassification OPTIONAL,
        privacy-mark PrivacyMark OPTIONAL,
        security-categories SecurityCategories OPTIONAL }

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

SecurityClassification ::= INTEGER {
        unmarked (0),
        unclassified (1),
        restricted (2),
        confidential (3),
        secret (4),
        top-secret (5) } (0. . .ub-integer-options)
```

FIGURA 2/X.411 (parte 40 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

```
PrivacyMark ::= PrintableString (SIZE (1. . .ub-privacy-mark-length))

SecurityCategories ::= SET (SIZE (1. . .ub-security-categories) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
        type [0] SECURITY-CATEGORY,
        value [1] ANY DEFINED BY type }

SECURITY-CATEGORY MACRO ::=
BEGIN

TYPE NOTATION ::= type | empty
VALUE NOTATION ::= value (VALUE OBJECT IDENTIFIER)

END  -- de CATEGORÍA-SEGURIDAD

END  -- del servicio abstracto STRM
```

FIGURA 2/X.411 (parte 41 de 41)

Definición de sintaxis abstracta del servicio abstracto del STRM

10 Modelo perfeccionado del sistema de transferencia de mensajes

En el § 6 se describe el STRM como un objeto, sin referencia a su estructura interna. El presente punto perfecciona el modelo del STRM, y expone sus objetos constituyentes y los puertos compartidos entre ellos.

La figura 3/X.411 proporciona un modelo del STRM y revela su estructura interna.

El STRM consta de una colección de objetos agente-transferencia-mensaje (ATM), que cooperan entre si para formar el STRM y ofrecer a sus usuarios el servicio abstracto de STRM. Los ATM realizan las funciones activas del STRM, es decir la transferencia de mensajes, sondas e informes, generación de informes, y conversión de contenidos.

Los objetos del ATM tienen igualmente puertos, algunos de los cuales son concretamente los que resultan igualmente visibles en la frontera del objeto del STRM, es decir, puertos-remisión, puertos-entrega y puertos-administración. Sin embargo, los ATM tienen igualmente otro tipo de puerto, el puerto-transferencia, que se ocupa de la distribución del servicio abstracto del STRM entre los ATM y que no resulta visible en la frontera del objeto STRM.

El puerto-transferencia permite a un ATM transferir mensajes, sondas e informes a otro ATM. En general, puede que haya que transferir un mensaje, una sonda o un informe, un cierto número de veces entre diferentes ATM hasta alcanzar el destino deseado.

Si se dirige un mensaje a múltiples destinatarios servidos por varios ATM diferentes, debe transferirse el mensaje a través del STRM a lo largo de varios trayectos diferentes. Desde la perspectiva del ATM que transfiere dicho mensaje, se pueden alcanzar algunos destinatarios a través de un trayecto mientras que a otros se llega a través de otro distinto. En dicho ATM, se crean dos copias del mensaje, transfiriéndose cada una de ellas al próximo ATM a lo largo de su trayecto respectivo. La copia y ramificación del mensaje se repiten hasta que cada copia haya alcanzado un ATM de destino final, donde pueda entregarse el mensaje a uno o más usuarios-STRM destinatarios.

Cada ATM a lo largo de un trayecto tomado por un mensaje, es responsable de la entrega o transferencia del mensaje a un subconjunto determinado de destinatarios-especificados-originalmente. Otros ATM se encargan de la entrega o transferencia a los restantes destinatarios, utilizando copias de los mensajes creados a lo largo del camino.

Los ATM generan informes sobre la entrega o no-entrega de un mensaje dirigido a uno o más usuarios STRM destinatarios, de conformidad con la petición del originador del mensaje y del ATM-que-origina. Un ATM puede generar un informe-entrega al entregar con éxito una copia de un mensaje a un usuario-STRM destinatario. Puede generar un informe-no-entrega al determinar que una copia de un mensaje resulta imposible de entregar a uno o más destinatarios, es decir, el ATM no ha podido entregar el mensaje a los usuarios-STRM destinatarios, o no puede transferir el mensaje a un ATM adyacente que tomaría la responsabilidad de entregar o transferir el mensaje ulteriormente.

Para una mayor eficacia, un ATM puede generar un informe único, combinado, que sirva para varias copias de un único mensaje con múltiples destinatarios, del cual es responsable. Pueden combinarse conjuntamente tanto los informes-entrega como los informes-no-entrega. Sin embargo, para combinar los informes de esta manera, debe realizarse la misma conversión de contenido, si ha lugar, en los mensajes de todos los destinatarios a que se refiere el informe.

Los informes que se refieren a copias del mismo mensaje con múltiples destinatarios pero que fueron generados por ATM diferentes no se combinan en ningún ATM intermedio, sino que permanecen separados.

Cuando se necesite, un ATM puede realizar una conversión de contenido. Cuando ni la petición del usuario-STRM originador, ni la del usuario-STRM destinatario prohíben la conversión, un ATM puede realizar la conversión implícita de los tipos-información-codificada de un mensaje para adaptarse a los tipos-información-codificada a los que puede recibir el usuario-STRM destinatario. El usuario STRM originador puede solicitar explícitamente la conversión de los tipos-información-codificada específicos para un determinado usuario-STRM destinatario.

Las puertas-remisión, -entrega y -administración de un ATM que resultan igualmente visibles en la frontera del STRM se definen en la sección 2 de esta Recomendación. Los restantes puntos de esta sección definen el puerto-transferencia de un ATM, y los procedimientos realizados por los ATM para garantizar una correcta operación distribuida del STRM.

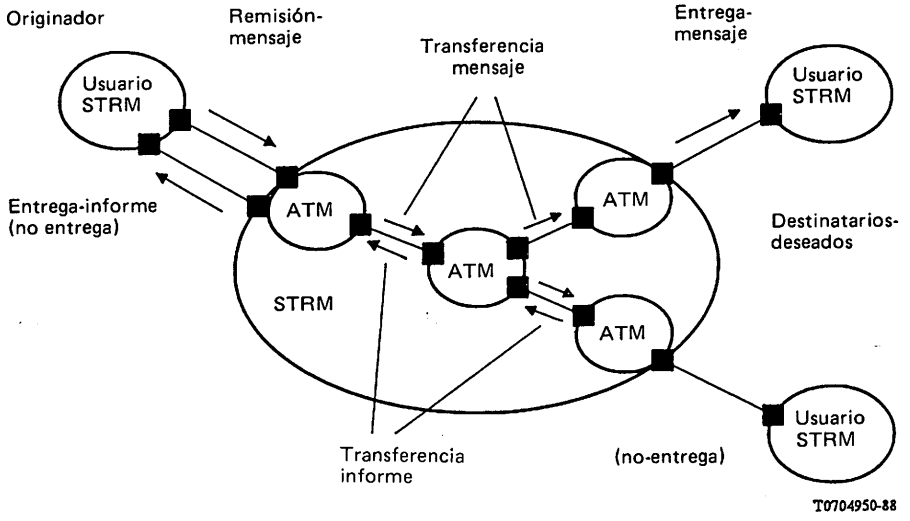


FIGURA 3/X.411

Modelo perfeccionado del sistema de transferencia de mensajes

11 Visión de conjunto del servicio abstracto del agente de transferencia de mensajes

En la sección 2 se define el servicio abstracto STRM proporcionado por los puertos-remisión, -entrega y -administración de un ATM. En este punto, se definen las operaciones-abstractas siguientes que proporcionan los puertos-transferencia de los ATM:

Vinculación-ATM y desvinculación-ATM

a) vinculación-ATM

b) desvinculación-ATM.

Operaciones-abstractas de puerto de transferencia

c) transferencia-mensaje

d) transferencia-sonda

e) transferencia-informe.

11.1 *Vinculación-ATM y desvinculación-ATM*

Vinculación-ATM permite a un ATM establecer una asociación con otro ATM. En el contexto de una asociación establecida pueden invocarse únicamente operaciones-abstractas distintas de vinculación-ATM.

Desvinculación-ATM permite liberar una asociación establecida por el iniciador de la asociación.

11.2 *Operaciones-abstractas de puerto de transferencia*

La operación-abstracta **transferencia-mensaje** permite a un ATM transferir un mensaje a otro ATM.

La operación-abstracta **transferencia-sonda** permite a un ATM transferir una sonda a otro ATM.

La operación abstracta **transferencia-informe** permite a un ATM transferir un informe a otro ATM.

12 Definición del servicio abstracto de agente de transferencia de mensajes

En el § 8 se define el servicio abstracto de STRM. En este punto, se define la semántica de los parámetros del servicio abstracto proporcionados por los puertos-transferencia de los ATM.

En el § 12.1 se define vinculación-ATM y desvinculación-ATM. El § 12.2 define el puerto-transferencia. En el § 12.3 se definen algunos tipos de parámetros comunes.

La sintaxis-abstracta del servicio abstracto de ATM se define en el § 13.

12.1 *Vinculación-ATM y desvinculación-ATM*

Este punto define los servicios-abstractos utilizados para establecer y liberar asociaciones entre ATM.

12.1.1 *Vinculación-abstracta y desvinculación-abstracta*

Este punto define las siguientes vinculación-abstracta y desvinculación-abstracta:

a) vinculación-ATM
b) desvinculación-ATM.

12.1.1.1 *Vinculación-ATM*

Vinculación-ATM permite a un ATM establecer una asociación con otro ATM.

Vinculación-ATM establece las **credenciales** de los ATM para interaccionar, y el **contexto-aplicación** y el **contexto-seguridad** de la asociación. Únicamente el iniciador de una asociación puede liberarla (utilizando desvinculación-ATM).

Las operaciones-abstractas diferentes de vinculación-ATM pueden invocarse únicamente en el contexto de una asociación establecida.

La finalización con éxito de vinculación-ATM significa el establecimiento de una asociación.

La interrupción de vinculación-ATM por un error-vinculación indica que la asociación no se ha establecido.

12.1.1.1.1 *Argumentos*

El cuadro 27/X.411 enumera los argumentos de vinculación-ATM y para cada argumento califica su presencia e indica el punto donde se define el argumento.

CUADRO 27/X.411

Argumento de vinculación-ATM

Argumento	Presencia	Punto
Argumentos de vinculación		
Nombre-iniciador	F	12.1.1.1.1.1
Credenciales-iniciador	F	12.1.1.1.1.2
Contexto-seguridad	F	12.1.1.1.1.3

12.1.1.1.1.1 *Nombre-iniciador*

Este argumento contiene un nombre para el iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

El nombre es un **nombre-ATM**.

12.1.1.1.1.2 *Credenciales-iniciador*

Este argumento contiene las **credenciales** del iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

Las **credenciales-iniciador** pueden utilizarse por el respondedor para autenticar la identidad del iniciador (véase Recomendación X.509).

Si se propone únicamente una autenticación-simple, las **credenciales-iniciador** constan de una contraseña simple asociada al **nombre-iniciador**.

Si se utiliza una autenticación-fuerte, las **credenciales-iniciador** constan de un **distintivo-vinculación-iniciador** y, opcionalmente un **certificado-iniciador**.

El **testigo-vinculación-iniciador** es un **testigo** generado por el iniciador de la asociación. Si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**, los **datos firmados** incluyen un **número-aleatorio**. Los **datos cifrados** de un **testigo-asimétrico** pueden utilizarse para transportar información secreta relativa-seguridad (por ejemplo, una o más claves-cifrados-simétricas) utilizadas para asegurar la asociación, o pueden estar ausentes de **testigo-vinculación-iniciador**.

El **certificado-iniciador** es un **certificado** del iniciador de la asociación, generado por una fuente de confianza (por ejemplo una autoridad-certificación). Puede ser suministrado por el iniciador de la asociación, si el **testigo-vinculación-iniciador** es un **testigo-asimétrico**. El **certificado-iniciador** puede utilizarse para transportar una copia verificada de la clave-cifrados-asimétrica-pública (**clave-pública-sujeto**) del iniciador de la asociación. La clave-cifrado-pública-asimétrica del iniciador puede ser utilizada por el respondedor para calcular el **testigo-vinculación-respondedor**. Si se sabe que el respondedor posee, o tiene acceso al **certificado** del iniciador (por ejemplo a través de la guía), puede omitirse el **certificado-iniciador**.

12.1.1.1.1.3 *Contexto-seguridad*

Este argumento indica el **contexto-seguridad** que propone para funcionar el iniciador de la asociación. Puede ser generado por el iniciador de la asociación.

El **contexto-seguridad** consta de una o más **etiquetas-seguridad** que definen la sensibilidad de las interacciones que pueden producirse entre los ATM durante la duración de la asociación, en línea con la política-seguridad en vigor. El **contexto-seguridad** debe ser uno de los autorizados por las **etiquetas-seguridad** asociadas a los DG (ATM).

Si no se establecen los **contextos-seguridad** entre los ATM, la sensibilidad de las interacciones que pueden producirse entre los ATM puede quedar a la discreción del invocador de una operación abstracta.

12.1.1.1.2 *Resultados*

El cuadro 28/X.411 enumera los resultados de vinculación-ATM, y para cada resultado califica su presencia e indica el punto donde se define el resultado.

CUADRO 28/X.411

Resultados de vinculación-ATM

Resultado	Presencia	Punto
Resultados de vinculación		
Nombre-respondedor	F	12.1.1.1.2.1
Credenciales-respondedor	F	12.1.1.1.2.2

12.1.1.1.2.1 *Nombre-respondedor*

Este argumento contiene un nombre para el respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

El nombre es un **nombre-ATM**.

12.1.1.1.2.2 *Credenciales-respondedor*

Este argumento contiene las **credenciales** del respondedor de la asociación. Puede ser generado por el respondedor de la asociación.

Las **credenciales-respondedor** pueden utilizarse por el iniciador para autenticar la identidad del respondedor (véase Recomendación X.509).

Si se propone únicamente una autenticación-simple, las **credenciales-respondedor** constan de una **contraseña** simple asociada al **nombre-respondedor.**

Si se utiliza una autenticación-fuerte, las **credenciales-respondedor** constan de un **testigo-vinculación-respondedor**. El **testigo-vinculación-respondedor** es un **testigo** generado por el respondedor de la asociación. El **testigo-vinculación-respondedor** debe ser del mismo tipo de **testigo** que el **testigo-vinculación-iniciador**. Si el **testigo-vinculación-respondedor** es un **testigo-asimétrico**, los **datos-firmados** incluyen un **número-aleatorio**, (que puede estar relacionado con el **número-aleatorio** proporcionado en el **distintivo-vinculación-iniciador**). Los **datos-cifrados** de un **testigo-asimétrico** pueden utilizarse para transportar información relativa-seguridad (por ejemplo, una o más claves-cifrado-simétricas) utilizadas para proporcionar seguridad a la asociación, o pueden estar ausentes del **testigo-vinculación-respondedor**.

12.1.1.1.3 *Errores-vinculación*

Los errores-vinculación que pueden interrumpir la operación vinculación-ATM se definen en el § 12.1.2.

12.1.1.2 *Desvinculación-ATM*

Desvinculación-ATM permite liberar una asociación establecida por el iniciador de la asociación.

12.1.1.2.1 *Argumentos*

El servicio desvinculación-ATM no tiene argumentos.

12.1.1.2.2 *Resultados*

El servicio desvinculación-ATM devuelve un resultado vacío como indicación de la liberación de la asociación.

12.1.1.2.3 *Errores-desvinculación*

No existen errores-desvinculación que puedan interrumpir la operación desvinculación-ATM.

12.1.2 *Errores-vinculación*

Esta cláusula define los siguientes errores-vinculación:

a) error-autenticación
b) ocupado
c) modo-diálogo-inaceptable
d) contexto-seguridad-inaceptable.

12.1.2.1 *Error-autenticación*

El error-vinculación de error-autenticación notifica que no puede establecerse una asociación debido a un error de autenticación; las **credenciales** del iniciador no son aceptables o están indebidamente especificadas.

El error-vinculación de error-autenticación no tiene parámetros.

12.1.2.2 *Ocupado*

El error-vinculación ocupado informa que una asociación no puede establecerse porque el respondedor está ocupado.

El error-vinculación ocupado no tiene parámetros.

12.1.2.3 *Modo-diálogo-inaceptable*

El error-vinculación modo-diálogo-inaceptable informa que el modo-diálogo propuesto por el iniciador de la asociación resulta inaceptable para el respondedor (véase el § 12 de la Recomendación X.419).

El error-vinculación de modo-diálogo-inaceptable no tiene parámetros.

12.1.2.4 *Contexto-seguridad-inaceptable*

El error-vinculación contexto-seguridad-inaceptable informa que el **contexto-seguridad** propuesto por el iniciador de la asociación resulta inaceptable para el respondedor.

El error-vinculación contexto-seguridad inaceptable no tiene parámetros.

12.2 *Puerto de transferencia*

Este punto define las operaciones-abstractas y los errores-abstractos que se producen en un puerto-transferencia.

12.2.1 *Operaciones-abstractas*

Este punto define las siguientes operaciones-abstractas de puerto-transferencia:

a) transferencia-mensaje
b) transferencia-sonda
c) transferencia-informe.

12.2.1.1 *Transferencia-mensaje*

La operación-abstracta transferencia-mensaje permite a un ATM transferir un mensaje a otro ATM.

12.2.1.1.1 *Argumentos*

El cuadro 29/X.411 enumera los argumentos de la operación-abstracta transferencia-mensaje y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

12.2.1.1.1.1 *Identificador-mensaje*

Este argumento consta de un **identificador-STRM** que distingue el mensaje de los restantes mensajes, sondas e informes en el interior del STRM. Deberá ser generado por el ATM-que-origina del mensaje, y tendrá el mismo valor que el **identificador-remisión-mensaje** suministrado al originador del mensaje cuando se remitió éste, y que el **identificador-entrega-mensaje** suministrado a los destinatarios del mensaje cuando se entrega el mensaje.

Al hacer copias de un mensaje para encaminarlo a múltiples destinatarios a través de diferentes ATM, cada copia del mensaje lleva el **identificador-mensaje** del original. Pueden distinguirse las copias entre sí mediante el **número-destinatario-especificado-originalmente** y los correspondientes argumentos de **responsabilidad**, que especifican a qué destinatario o destinatarios ha de entregarse cada copia.

12.2.1.1.1.2 *Información-bilateral-por-dominio*

Este argumento contiene la información destinada a los DG que encontrará el mensaje al ser transferido a través del STRM. Puede ser generado por el DG-originador del mensaje.

Este argumento puede contener cero o más elementos, cada uno de los cuales incluye:

– la **información-bilateral** destinada a un DG;
– el **nombre-país**, el **nombre-dominio-administración** y, opcionalmente, el **identificador-dominio-privado** del DG al que va destinado la **información-bilateral**.

12.2.1.1.1.3 *Información-rastreo*

Este argumento documenta las acciones realizadas sobre el mensaje (o sonda o informe) por cada DG a través del cual pasa el mensaje al ser transferido a través del STRM (véase el § 12.3.1). Debe ser generado por cada DG a través del cual pasa el mensaje (o sonda o informe).

12.2.1.1.1.4 *Información-rastreo-interna*

Este argumento documenta las acciones realizadas sobre el mensaje (o sonda o informe) por cada ATM a través del cual pasa el mensaje (o sonda o informe) al ser transferido en el interior de un DG (véase el § 12.3.1). Debe ser generado por cada ATM a través del cual pasa el mensaje (o sonda o informe) en el interior de un DG.

Este argumento no será suministrado por el invocador de la operación-abstracta transferencia-mensaje al transferir un mensaje a otro DG a menos que se deba a un acuerdo bilateral entre DG.

12.2.1.1.1.5 *Número-destinatario-especificado-originalmente*

Este argumento, combinado con el **identificador-mensaje**, identifica sin ambigüedad la copia del mensaje entregada a cada destinatario. Debe ser generado por el ATM-que-origina del mensaje. Se especifica un valor diferente de este argumento para cada destinatario de este mensaje.

El **número-destinatario-especificado-originalmente** es un valor entero en el intervalo comprendido entre uno y el número de destinatarios-especificados-originalmente.

CUADRO 29/X.411

Argumentos de transferencia-mensaje

Argumento	Presencia	Punto
Argumentos de retranmisión		
Identificador-mensaje	O	12.2.1.1.1.1
Información-bilateral-por-dominio	C	12.2.1.1.1.2
Información-rastreo	O	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Historia-ampliación-LD	C	8.3.1.1.1.7
Argumento del originador		
Nombre-originador	O	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	O	8.2.1.1.1.2
Número-destinatario-especificado-originalmente	O	12.2.1.1.1.5
Responsabilidad	O	12.2.1.1.1.6
Ampliación-LD-prohibida	C	8.2.1.1.1.6
Revelación-de-destinatarios	C	8.2.1.1.1.7
Argumentos de redireccionamiento		
Destinatario-alternativo-autorizado	C	8.2.1.1.1.3
Reasignación-destinatario-prohibida	C	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	C	8.2.1.1.1.5
Nombre-destinatario-deseado	C	8.3.1.1.1.4
Motivo-redireccionamiento	C	8.3.1.1.1.5
Argumento de prioridad		
Prioridad	C	8.2.1.1.1.8
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Conversión-explícita	C	8.2.1.1.1.11
Argumentos de tiempo de entrega		
Tiempo-entrega-diferida	C	12.2.1.1.1.7
Último-tiempo-entrega	C	8.2.1.1.1.13
Argumento de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumentos de entrega física		
Envío-físico-prohibido	C	8.2.1.1.1.15
Petición-dirección-envío-físico	C	8.2.1.1.1.16
Modos-entrega-física	C	8.2.1.1.1.17
Tipo-correo-certificado	C	8.2.1.1.1.18
Número-destinatario-para-aviso	C	8.2.1.1.1.19
Atributos-reproducción-física	C	8.2.1.1.1.20
Dirección-devolución-originador	C	8.2.1.1.1.21
Argumentos de petición de informe de entrega		
Petición-informe-originador	O	8.2.1.1.1.22
Petición-informe-ATM-que-origina	O	12.2.1.1.1.8
Petición-devolución-contenido	C	8.2.1.1.1.23
Petición-informe-entrega-física	C	8.2.1.1.1.24
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Testigo-mensaje	C	8.2.1.1.1.26
Identificador-algoritmo-confidencialidad-contenido	C	8.2.1.1.1.27
Verificación-integridad-contenido	C	8.2.1.1.1.28
Verificación-autenticación-origen-mensaje	C	8.2.1.1.1.29
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Petición-prueba-de-entrega	C	8.2.1.1.1.32
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	O	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido	O	8.2.1.1.1.37

Existe una relación biunívoca entre un determinado valor del **número-destinatario-especificado-originalmente** y un determinado **nombre-destinatario** en el momento de la remisión-mensaje; no debería suponerse que esta es una relación singular en el momento de la entrega-mensaje. Es decir, puede utilizarse un valor del **número-destinatario-especificado-originalmente** para distinguir un **nombre-destinatario** especificado originalmente, pero no un destinatario real que recibirá el mensaje.

12.2.1.1.1.6 *Responsabilidad*

Este argumento indica si el ATM-receptor debe tener la responsabilidad de entregar el mensaje a un destinatario o de transferirlo a otro ATM para su entrega subsiguiente al destinatario. Debe ser generado por el ATM-emisor. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tener uno de los siguientes valores: **responsable** o **no responsable**.

12.2.1.1.1.7 *Tiempo-entrega-diferida*

Este argumento se define en el § 8.2.1.1.1.12. Puede aparecer en un mensaje en el puerto-transferencia si existe un acuerdo bilateral de que un ATM distinto del ATM-que-origina del mensaje diferirá la entrega del mensaje.

12.2.1.1.1.8 *Petición-informe-ATM-que-origina*

Este argumento indica el tipo de informe solicitado por el ATM-que-origina. Debe ser generado por el ATM-que-origina del mensaje. Puede especificarse un valor diferente de este argumento para cada destinatario del mensaje.

Este argumento puede tomar uno de los siguientes valores:

- **informe-no-entrega**: se devuelve un informe únicamente en el caso de no-entrega, y contiene únicamente la **última-información-rastreo**;
- **informe**: se devuelve un informe tanto en el caso de entrega como de no-entrega y contiene únicamente la **última-información-rastreo**;
- **informe-auditado**: se devuelve un informe tanto en el caso de entrega como de no-entrega, y contiene toda la **información-rastreo**.

El argumento de **petición-informe-ATM-que-origina** deberá especificar al menos el nivel del informe especificado en el argumento de **petición-informe-originador**, siendo el orden creciente de los niveles de informe: **no-informe, informe-no-entrega, informe, informe-auditado.**

12.2.1.1.2 *Resultados*

La operación-abstracta transferencia-mensaje no devuelve resultado.

12.2.1.1.3 *Errores-abstractos*

No existen errores-abstractos que puedan interrumpir la operación- abstracta transferencia-mensaje.

12.2.1.2 *Transferencia-sonda*

La operación-abstracta transferencia-sonda permite a un ATM transferir una sonda a otro ATM.

12.2.1.2.1 *Argumentos*

El cuadro 30/X.411 enumera los argumentos de la operación-abstracta transferencia-sonda y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

12.2.1.2.1.1 *Identificador-sonda*

Este argumento contiene un **identificador-STRM** que distingue la sonda de otros mensajes, sondas e informes en el interior del STRM. Debe ser generado por el ATM-que-origina de la sonda, y debe tener el mismo valor que el **identificador-remisión-sonda** suministrado al originador de la sonda cuando se remitió ésta.

12.2.1.2.2 *Resultados*

La operación-abstracta transferencia-sonda no devuelve resultados.

12.2.1.2.3 *Errores-abstractos*

No existen errores-abstractos que puedan interrumpir la operación-abstracta transferencia-sonda.

CUADRO 30/X.411

Argumentos de transferencia-sonda

Argumento	Presencia	Punto
Argumentos de retransmisión		
Identificador-sonda	O	12.2.1.2.1.1
Información-bilateral-por-dominio	C	12.2.1.1.1.2
Información-rastreo	O	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Historia-ampliación-LD	C	8.3.1.1.1.7
Argumento del originador		
Nombre-originador	O	8.2.1.1.1.1
Argumentos del destinatario		
Nombre-destinatario	O	8.2.1.1.1.2
Número-destinatario-especificado-originalmente	O	12.2.1.1.1.5
Responsabilidad	O	12.2.1.1.1.6
Ampliación-LD-prohibida	C	8.2.1.1.1.6
Argumentos de redireccionamiento		
Destinatario-alternativo-autorizado	C	8.2.1.1.1.3
Reasignación-destinatario-prohibida	C	8.2.1.1.1.4
Destinatario-alternativo-solicitado-originador	C	8.2.1.1.1.5
Nombre-destinatario-deseado	C	8.3.1.1.1.4
Motivo-redireccionamiento	C	8.3.1.1.1.5
Argumentos de conversión		
Conversión-implícita-prohibida	C	8.2.1.1.1.9
Conversión-con-pérdida-prohibida	C	8.2.1.1.1.10
Conversión-explícita	C	8.2.1.1.1.11
Argumentos de método de entrega		
Método-entrega-solicitado	C	8.2.1.1.1.14
Argumento de entrega física		
Atributos-reproducción-física	C	8.2.1.1.1.20
Argumentos de petición de informe		
Petición-informe-originador	O	8.2.1.1.1.22
Petición-informe-ATM-que-origina	O	12.2.1.1.1.8
Argumentos de seguridad		
Certificado-originador	C	8.2.1.1.1.25
Verificación-autenticación-origen-sonda	C	8.2.1.2.1.1
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	O	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Longitud-contenido	C	8.2.1.2.1.2

12.2.1.3 *Transferencia-informe*

La operación-abstracta transferencia-informe permite a un ATM transferir un informe a otro ATM.

12.2.1.3.1 *Argumentos*

El cuadro 31/X.411 enumera los argumentos de la operación-abstracta transferencia-informe, y para cada argumento califica su presencia e identifica el punto donde se define el argumento.

12.2.1.3.1.1 *Identificador-informe*

Este argumento contiene un **identificador-STRM** que distingue el informe de otros mensajes, sondas e informes en el interior del STRM. Debe ser generado por el ATM-que-origina del informe.

12.2.1.3.1.2 *Nombre-destino-informe*

Este argumento contiene el **nombre-O/D** del destino inmediato del informe. Debe ser generado por el ATM-que-origina del informe, y modificado subsiguientemente por los puntos-ampliación de LD si se ha ampliado alguna LD para añadir destinatarios al sujeto.

El ATM-que-origina del informe debe fijar este argumento en el **nombre-originador** del sujeto si éste no tiene una **historia-ampliación-LD**, o en el último **nombre-O/D** de la **historia-ampliación-LD** si está presente en el sujeto.

Un punto-ampliación de LD puede sustituir su propio **nombre-O/D** en este argumento, por el **nombre-O/D** que precede inmediatamente a su propio **nombre-O/D** en el **originador-e-historia-ampliación-LD** del informe o por algún otro **nombre-O/D** según la política-informadora de la LD.

12.2.1.3.1.3 *Identificador-sujeto*

Este argumento contiene el **identificador-mensaje** (o el **identificador- sonda**) del sujeto (**identificador-STRM**). Debe ser generado por el ATM-que-origina del sujeto.

12.2.1.3.1.4 *Información-rastreo-intermedia-sujeto*

Este argumento contiene la **información-rastreo** presente en el sujeto cuando se transfirió al DG-informador. Debe estar presente si, y únicamente si se solicitó un informe auditado y confirmado por el ATM-que-origina del sujeto. Puede ser generado por el ATM-informador.

Nota – La inclusión en la **información-rastreo-intermedia sujeto** de la **información-rastreo-interna** presente en el sujeto cuando se transfirió al ATM-informador queda para ulterior estudio.

12.2.1.3.1.5 *Tiempo-llegada*

Este argumento contiene el **tiempo** en que el sujeto indicó al DG que hiciera el informe. Debe ser generado por el DG-originador del informe. Puede especificarse un valor diferente de este argumento para cada destinatario del sujeto a que se refiere el informe.

12.2.1.3.1.6 *Información adicional*

La especificación del contenido de este argumento se realiza mediante acuerdo bilateral entre DG.

12.2.1.3.2 *Resultados*

La operación-abstracta transferencia-informe no devuelve resultados.

12.2.1.3.3 *Errores abstractos*

No existen errores-abstractos que pueden interrumpir la operación-abstracta transferencia-informe.

12.2.2 *Errores abstractos*

El puerto-transferencia no tiene errores abstractos.

CUADRO 31/X.411

Argumentos de transferencia-informe

Argumento	Presencia	Punto
Argumentos de retransmisión		
Identificador-informe	O	12.2.1.3.1.1
Información-rastreo	O	12.2.1.1.1.3
Información-rastreo-interna	C	12.2.1.1.1.4
Argumento de destino del informe		
Nombre-destino-informe	O	12.2.1.3.1.2
Argumento de petición del informe		
Petición-informe-originador	O	8.2.1.1.1.22
Argumentos de rastreo del sujeto		
Identificador-sujeto	O	12.2.1.3.1.3
Número-destinatario-especificado-originalmente	O	12.2.1.1.1.5
Información-rastreo-intermedia-sujeto	C	12.2.1.3.1.4
Tiempo-llegada	O	12.2.1.3.1.5
Originador-e-historia-ampliación-LD	C	8.3.1.2.1.3
Nombre-LD-informadora	C	8.3.1.2.1.4
Argumento de conversión		
Tipos-información-codificada-convertidos	C	8.3.1.2.1.5
Argumentos de información suplementaria		
Información-suplementaria	C	8.3.1.2.1.6
Dirección-envío-físico	C	8.3.1.2.1.7
Argumentos de redireccionamiento del sujeto		
Nombre-destinatario-real	O	8.3.1.2.1.2
Nombre-destinatario-deseado	C	8.3.1.1.1.4
Motivo-redireccionamiento	C	8.3.1.1.1.5
Argumentos de contenido		
Tipos-información-codificada-originales	C	8.2.1.1.1.33
Tipo-contenido	C	8.2.1.1.1.34
Identificador-contenido	C	8.2.1.1.1.35
Correlador-contenido	C	8.2.1.1.1.36
Contenido-devuelto	C	8.3.1.2.1.14
Argumentos de entrega		
Tiempo-entrega-mensaje	C	8.3.1.2.1.8
Tipo-de usuario-STRM	C	8.3.1.2.1.9
Argumentos de no-entrega		
Código-motivo-no-entrega	C	8.3.1.2.1.10
Código-diagnóstico-no-entrega	C	8.3.1.2.1.11
Argumentos de seguridad		
Certificado-destinatario	C	8.3.1.1.2.1
Prueba-de-entrega	C	8.3.1.1.2.2
Certificado-ATM-que-informa	C	8.3.1.2.1.12
Verificación-autenticación-origen-informe	C	8.3.1.2.1.13
Etiqueta-seguridad-mensaje	C	8.2.1.1.1.30
Argumento de información adicional		
Información-adicional	C	12.2.1.3.1.6

12.3 *Tipos de parámetros comunes*

Este punto define cierto número de tipos de parámetros comunes del servicio abstracto de ATM.

12.3.1 *Información-rastreo e información-rastreo-interna*

La **información-rastreo** documenta las acciones efectuadas sobre un mensaje, sonda o informe por cada DG, a través del cual pasa al ser transferido a través del STRM.

La **información-rastreo-interna** documenta las acciones efectuadas sobre un mensaje, sonda o informe por cada ATM, a través del cual pasa al ser transferido a través de un DG. La **información-rastreo-interna** deberá ser eliminada del mensaje, sonda o informe antes de ser transferido fuera de un DG, a menos que exista un acuerdo bilateral entre las DG.

La **información-rastreo** (o **información-rastreo-interna**) consta de una secuencia de **elementos-información-rastreo** (o **elementos-información-rastreo-interna**). El primer **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) es el suministrado por el DG-(o ATM-) que-origina del mensaje, sonda o informe. El segundo **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) es el suministrado por el siguiente DG (o ATM) encontrado por el mensaje, sonda o informe, y así sucesivamente. Cada DG (o ATM) añade su elemento **información-rastreo** (o **elemento-información-rastreo-interna**) al final de la secuencia existente. La **información-rastreo** la añade el primer ATM que encuentren el mensaje, la sonda o el informe en cada DG por el que atraviesen.

Cada **elemento-información-rastreo** incluye el **identificador-dominio-global** del DG que suministra el **elemento-información-rastreo**.

Cada **elemento-información-rastreo-interna** incluye el **nombre-ATM** del ATM que suministra el **elemento-información-rastreo-interna** y el **identificador-dominio-global** del DG al que pertenece el ATM.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) incluye el **tiempo-llegada** en el cual el mensaje, sonda o informe entró en el DG (o ATM). En el caso del DG-(o ATM-) que-origina del mensaje, sonda o informe, el **tiempo-llegada** es el tiempo de la remisión-mensaje, remisión-sonda o generación del informe, respectivamente.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) especifica la **acción-encaminamiento** que el DG (o ATM) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) adoptó respecto del mensaje, sonda o informe. **Retransmitido** constituye la **acción-encaminamiento** normal de transferencia de mensaje, sonda o informe a otro DG o ATM. **Reencaminado** indica que se había realizado previamente un intento de reencaminar el mensaje, sonda o informe hacia un **dominio-deseado** (o **ATM-deseado**); se incluye el **identificador-dominio-global** del **dominio-deseado** en el **elemento-información-rastreo**; si el intento de reencaminamiento iba dirigido hacia otro ATM dentro del mismo DG, se incluye entonces el **nombre-ATM** del **ATM-deseado** en el **elemento-información-rastreo-interna**; si el intento de reencaminamiento iba dirigido hacia otro DG se incluye en el **elemento-información-rastreo-interna** el **identificador-dominio-global** en vez de un **nombre-ATM**.

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) especifica igualmente cualquier **acción-adicional** que el DG (o ATM) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) efectuó con respecto al mensaje, sonda o informe. Las indicaciones de cualquiera de estas **acciones-adicionales** que aparecen en los **elementos-información-rastreo-interna** durante la travesía de un DG deberán reflejarse igualmente en los **elementos-información-rastreo** correspondientes a la travesía del DG.

Si la entrega diferida provocó que el DG (o ATM) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) retuviera el mensaje durante un periodo de tiempo, el **tiempo-diferido** en que inició el tratamiento del mensaje para su entrega o transferencia se incluye igualmente en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Este parámetro no está presente en los **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) de las sondas e informes.

Si el DG (o ATM) que suministra el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) somete un mensaje a conversión, los **tipos-información-codificada-convertidos** resultantes de la conversión se incluyen igualmente en **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Para una sonda, un DG que hubiera convertido el mensaje-sujeto indica en su **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) los **tipos-información-codificada** que el mensaje-sujeto contendría después de la conversión. Este parámetro no está presente en la **información-rastreo** (o **elemento-información-rastreo-interna**) de los informes.

Si el DG (o ATM) redirige un mensaje o una sonda (a cualquiera, pero no necesariamente a todos los destinatarios de un mensaje o una sonda), se indica **redirigido** en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Este parámetro no está presente en la **información-rastreo** (o **información-rastreo-interna**) de los informes.

Si el DG (o ATM) amplía la LD de un mensaje o de una sonda, se indica **ampliada** en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**). Si el DG (o ATM) es un punto-ampliación de LD y sustituye su propio **nombre-O/D** en el **nombre-destino-informe** de un informe por otro **nombre-O/D** (véase el § 12.2.1.3.1.2), se indica **ampliada** en el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) del informe.

Un DG (o ATM) realiza la detección y supresión de un bucle cuando se recibe un mensaje, sonda o informe procedente de otro DG (o ATM). Los mensajes, sondas e informes pueden volver a entrar legítimamente en un DG (o ATM) debido a varias razones (**reencaminado**, etc.) y en consecuencia, un mensaje, sonda o informe puede tener **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) disjuntos procedentes del mismo DG (o ATM). Cada vez que un mensaje, sonda o informe se transfiere a través de un DG (o ATM), la generación de los **elementos-información-rastreo** (o **elementos-información-rastreo-interna**) se ejecuta de la forma siguiente:

i) se agrega un **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) marcado como **retransmitido**;

ii) si se ha de producir una tentativa de reencaminamiento, el **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) añadido en i) se cambia por **reencaminado** [y el **número de elemento-información-rastreo** (o **elementos-información-rastreo-interna**) añadidos por el DG (o ATM) para esta travesía del DG (o ATM) permanece en uno];

iii) si se producen tentativas subsiguientes de reencaminamiento, se añade un nuevo **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) (marcado como **reencaminado**) para reflejar cada nueva tentativa de reencaminamiento.

Pueden producirse varias tentativas de reencaminamiento hacia el mismo DG (o ATM).

Cada **elemento-información-rastreo** (o **elemento-información-rastreo-interna**) añadido por un DG (o ATM) puede contener indicaciones de **acciones-adicionales** realizadas por el DG (o ATM) sobre el mensaje o sonda [es decir **tiempo-diferido** (no presentes en **información-rastreo** (**información-rastreo-interna**) en las sondas), **tipos-información-codificada-convertidos**, **redirigidos** o **ampliados**].

13 Definición de la sintaxis abstracta de agente de transferencia de mensajes

La sintaxis-abstracta del servicio abstracto del ATM se define en la figura 4/X.411.

La sintaxis-abstracta del servicio abstracto de ATM se define utilizando la notación de sintaxis-abstracta (NSA.1) definida en la Recomendación X.208, y los convenios de definición del servicio-abstracto definidos en la Recomendación X.407.

La definición de sintaxis-abstracta del servicio abstracto ATM tiene las siguientes partes principales:

- *Prólogo*: declaraciones de las exportaciones desde el módulo de servicio abstracto ATM, y las importaciones a éste (figura 4/X.411, parte 1).
- *Perfeccionamiento del STRM, objetos y puertos*: perfeccionamiento del objeto del STRM, definiciones del objeto del ATM, y su puerto-transferencia (figura 4/X.411, parte 2).
- *Vinculación-ATM y desvinculación-ATM*: definiciones de vinculación-ATM y desvinculación-ATM utilizadas para establecer y liberar asociaciones entre ATM (figura 4/X.411, parte 3).
- *Puerto de transferencia*: definiciones de las operaciones-abstractas de puerto-transferencia: transferencia-mensaje, transferencia-sonda, transferencia-informe (figura 4/X.411, parte 4).
- *Sobre de transferencia de mensaje*: definición del sobre-transferencia-mensaje (figura 4/X.411, partes 5 y 6).
- *Sobre de transferencia de sonda*: definición del sobre-transferencia-sonda (figura 4/X.411, parte 7).
- *Sobre y contenido de transferencia de informe*: definición del sobre-transferencia-informe y del contenido-transferencia-informe (figura 4/X.411, parte 8).
- *Campos de sobre y contenido del informe*: definiciones de campos de sobre y de contenido del informe (figura 4/X.411, partes 9 y 10).
- *Campos de ampliación*: definiciones de los campos-ampliación (figura 4/X.411, partes 11 a 12).
- *Tipos de parámetros comunes*: definiciones de los tipos de parámetros comunes (figura 4/X.411, parte 13).

Nota – El módulo implica ciertos cambios en el protocolo P1 definido en la Recomendación X.411 (1984). Estos cambios se señalan mediante subrayado.

Cada **campo-ampliación** definido en la figura 4/X.411 (partes 12 y 13) transporta consigo una indicación sobre su criticidad para la remisión, transferencia y entrega. El mecanismo de **criticidad** se describe en el § 9.1 y los procedimientos relativos a los **campos-ampliación** y a las indicaciones de su **criticidad** se definen ulteriormente en el § 14.

```
MTAAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) mta-abstract-service(2) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exportar todo


IMPORTS
        -- Macros del servicio abstracto
        REFINE, OBJECT, PORT, ABSTRACT-BIND, ABSTRACT-UNBIND, ABSTRACT-OPERATION
                FROM AbstractServiceNotation { joint-iso-ccitt mhs-motis(6) asdc(2) modules(0)
                    notation(1) }

        -- Parámetros del servicio abstracto del STRM
        mTS, submission, delivery, administration, InitiatorCredentials, SecurityContext,
        ResponderCredentials, OriginalEncodedInformationTypes, ContentTypes, ContentIdentifier,
        Priority, PerMessageIndicators, DeferredDeliveryTime, CountryName, AdministrationDomainName,
        PrivateDomainIdentifier, ExplicitConversion, ContentLength, ConvertedEncodedInformationTypes,
        ReportType, SupplementaryInformation, EXTENSION, EXTENSIONS, recipient-reassignment-prohibited,
        dl-expansion-prohibited, conversion-with-loss-prohibited, latest-delivery-time,
        requested-delivery-method, physical-forwarding-prohibited, physical-forwarding-address-request,
        physical-delivery-modes, registered-mail-type, recipient-number-for-advice, physical-rendition-attributes,
        originator-return-address, physical-delivery-report-request, originator-certificate, message-token,
        content-confidentiality-algorithm-identifier, content-integrity-check, message-origin-authentication-check,
        message-security-label, proof-of-delivery-request, content-correlator, probe-origin-authentication-check,
        redirection-history, dl-expansion-history, originator-and-dl-expansion-history, reporting-dl-name,
        physical-forwarding-address, recipient-certificate, proof-of-delivery, reporting-MTA-certificate,
        report-origin-authentication-check, Content, MTSIdentifier, GlobalDomainIdentifier, MTAName, Time,
        ORAddressAndOptionalDirectoryName
                FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    mts-abstract-service(1) }

        -- Identificadores de objetos
        id-ot-mta, id-pt-transfer
                FROM MTSObjectIdentifiers { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    object-identifiers(0) }

        -- Límites superiores
        ub-bit-options, ub-dl-expansions, ub-integer-options, ub-recipients, ub-redirections, ub-transfers
                FROM MTSUpperBounds { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    upper-bounds(3) };
```

FIGURA 4/X.411 (Parte 1 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Perfeccionamiento del STRM
MTSRefinement ::= REFINE mTS AS
        mTA RECURRING
                submission      [S] VISIBLE
                delivery        [S] VISIBLE
                administration  [S] VISIBLE
                transfer            PAIRED WITH mTA

-- Objetos
mTA OBJECT
        PORTS { submission [S], delivery [S], administration [S], transfer }
        ::= id-ot-mta

-- Puertos
transfer PORT
        ABSTRACT OPERATIONS { MessageTransfer, ProbeTransfer, ReportTransfer }
        ::= id-pt-transfer
```

FIGURA 4/X.411 (Parte 2 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Vinculación-ATM y desvinculación-ATM
MTABind ::= ABSTRACT-BIND
        TO { transfer }
        BIND
        ARGUMENT CHOICE {
                NULL,           -- if no authentication is required
                [1] SET {       -- if authentication is required
                    initiator-name [0] MTAName,
                    initiator-credentials [1] InitiatorCredentials,
                    security-context [2] SecurityContext OPTIONAL } }
        RESULT CHOICE {
                NULL,           -- if no authentication is required
                [1] SET {       -- if authentication is required
                    responder-name [0] MTAName,
                    responder-credentials [1] ResponderCredentials } }
        BIND-ERROR INTEGER {
                busy (0),
                authentication-error (2),
                unacceptable-dialogue-mode (3)
                unacceptable-security-context (4) } (0 . . ub-integer-options)
MTAUnbind ::= ABSTRACT-UNBIND
        FROM { transfer }
```

FIGURA 4/X.411 (Parte 3 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Puerto de transferencia

MessageTransfer ::= ABSTRACT-OPERATION
        ARGUMENT Message

ProbeTransfer ::= ABSTRACT-OPERATION
        ARGUMENT Probe

ReportTransfer ::= ABSTRACT-OPERATION
        ARGUMENT Report

Message ::= SEQUENCE {
        envelope MessageTransferEnvelope,
        content Content }

Probe ::= ProbeTransferEnvelope

Report ::= SEQUENCE {
        envelope ReportTransferEnvelope,
        content ReportTransferContent }
```

FIGURA 4/X.411 (Parte 4 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Sobre de transferencia de mensaje

MessageTransferEnvelope ::= SET {
        COMPONENTS OF PerMessageTransferFields,
        per-recipient-fields [2] SEQUENCE SIZE (1 . . ub-recipients) OF
                PerRecipientMessageTransferFields }

PerMessageTransferFields ::= SET {
        message-identifier MessageIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        priority Priority DEFAULT normal,
        per-message-indicators PerMessageIndicators DEFAULT {},
        deferred-delivery-time [0] DeferredDeliveryTime OPTIONAL,
        per-domain-bilateral-information [1] SEQUENCE OF PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extension [3] EXTENSIONS CHOSEN FROM {
                recipient-reassignment-prohibited,
                dl-expansion-prohibited,
                conversion-with-loss-prohibited,
                latest-delivery-time,
                originator-return-address,
                originator-certificate,
                content-confidentiality-algorithm-identifier,
                message-origin-authentication-check,
                message-security-label,
                content-correlator,
                dl-expansion-history,
                internal-trace-information} DEFAULT {} }
```

FIGURA 4/X.411 (Parte 5 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
PerRecipientMessageTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extension [3] EXTENSIONS CHOSEN FROM {
                originator-requested-alternate-recipient,
                requested-delivery-method,
                physical-forwarding-prohibited,
                physical-forwarding-address-request,
                physical-delivery-modes,
                registered-mail-type,
                recipient-number-for-advice,
                physical-rendition-attributes,
                physical-delivery-report-request,
                message-token,
                content-integrity-check,
                proof-of-delivery-request,
                redirection-history } DEFAULT {} }
```

FIGURA 4/X.411 (Parte 6 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Sobre de transferencia de la sonda

ProbeTransferEnvelope ::= SET {
        COMPONENTS OF PerProbeTransferFields,
        per-recipient-field [2] SEQUENCE SIZE (1 .. ub-recipients) OF PerRecipientProbeTransferFields }

PerProbeTransferFields ::= SET {
        probe-identifier ProbeIdentifier,
        originator-name OriginatorName,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type-ContentType,
        content-identifier ContentIdentifier OPTIONAL,
        content-length [0] ContentLength OPTIONAL,
        per-message-indicators PerMessageIndicators DEFAULT {},
        per-domain-bilateral-information [1] SEQUENCE SIZE (1 .. ub-transfers) OF
                PerDomainBilateralInformation OPTIONAL,
        trace-information TraceInformation,
        extensions [3] EXTENSIONS CHOSEN FROM {
                recipient-reassignment-prohibited,
                dl-expansion-prohibited,
                conversion-with-loss-prohibited,
                originator-certificate,
                message-security-label,
                content-correlator,
                probe-origin-authentication-check,
                dl-expansion-history,
                internal-trace-information} DEFAULT {} }

PerRecipientProbeTransferFields ::= SET {
        recipient-name RecipientName,
        originally-specified-recipient-number [0] OriginallySpecifiedRecipientNumber,
        per-recipient-indicators [1] PerRecipientIndicators,
        explicit-conversion [2] ExplicitConversion OPTIONAL,
        extensions [3] EXTENSIONS CHOSEN FROM {
                originator-requested-alternate-recipient,
                requested-delivery-method,
                physical-rendition-attributes,
                redirection-history } DEFAULT {} }
```

FIGURA 4/X.411 (Parte 7 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Sobre de transferencia del informe

ReportTransferEnvelope ::= SET {
        report-identifier ReportIdentifier,
        report-destination-name ReportDestinationName,
        trace-information TraceInformation,
        extensions [1] EXTENSIONS CHOSEN FROM {
                message-security-label,
                originator-and-DL-expansion-history,
                reporting-DL-name,
                reporting-MTA-certificate,
                report-origin-authentication-check,
                internal-trace-information} DEFAULT {} }


-- Contenido de transferencia del informe

ReportTransferContent ::= SET {
        COMPONENTS OF PerReportTransferFields,
        per-recipient-fields [0] SEQUENCE SIZE (1 . . ub-recipients) OF
                PerRecipientReportTransferFields }

PerReportTransferFields ::= SET {
        subject-identifier SubjectIdentifier,
        subject-intermediate-trace-information SubjectIntermediateTraceInformation OPTIONAL,
        original-encoded-information-types OriginalEncodedInformationTypes OPTIONAL,
        content-type ContentType OPTIONAL,
        content-identifier ContentIdentifier OPTIONAL,
        returned-content [1] Content OPTIONAL,
        additional-information [2] AdditionalInformation OPTIONAL,
        extensions [3] EXTENSIONS CHOSEN FROM {
                content-correlator } DEFAULT {} }

PerRecipientReportTransferFields ::= SET {
        actual-recipient-name [0] ActualRecipientName,
        originally-specified-recipient-number [1] OriginallySpecifiedRecipientNumber,
        per-recipient-indicator [2] PerRecipientIndicators,
        last-trace-information [3] LastTraceInformation,
        originally-intended-recipient-name [4] OriginallyIntendedRecipientName OPTIONAL,
        supplementary-information [5] SupplementaryInformation OPTIONAL,
        extensions [6] EXTENSIONS CHOSEN FROM {
                redirection-history,
                physical-forwarding-address,
                recipient-certificate,
                proof-of-delivery } DEFAULT {} }
```

FIGURA 4/X.411 (Parte 8 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Campos de sobre y contenido del informe

MessageIdentifier ::= MTSIdentifier

OriginatorName ::= ORAddressAndOptionalDirectoryName

PerDomainBilateralInformation ::= SEQUENCE {
        country-name CountryName,
        CHOICE {
                administration-domain-name AdministrationDomainName,
                SEQUENCE {
                    administration-domain-name [0] AdministrationDomainName,
                    private-domain-identifier [1] PrivateDomainIdentifier OPTIONAL } },
        bilateral-information BilateralInformation }

BilateralInformation ::= ANY        --maximum ub-bilateral-info octets including all encoding

RecipientName ::= ORAddressAndOptionalDirectoryName

OriginallySpecifiedRecipientNumber ::= INTEGER (SIZE (1 . . ub-recipients))

PerRecipientIndicators ::= BIT STRING {
        responsibility (0),
        -- reponsible 'one', not-responsible 'zero'
        originating-MTA-report (1),
        originating-MTA-non-delivery-report (2),
        -- either originating-MTA-report, or originating-MTA-non-delivery-report, or both, shall be 'one':
        -- originating-MTA-report bit 'one' requests a 'report';
        -- originating-MTA-non-delivery-report bit 'one' requests a 'non-delivery-report';
        -- both bits 'one' requests and 'audited-report';
        -- bits 0-2 'don't care' for Report Transfer Content
        originator-report (3),
        originator-non-delivery-report (4),
        -- at most one bit shall be 'one':
        -- originator-report bit 'one' requests a 'report';
        -- originator-non-delivery-report bit 'one' requests a 'non-delivery-report';
        -- both bits 'zero' requests 'no-report'
        reserved-5 (5),
        reserved-6 (6),
        reserved-7 (7),
        -- reserved-bits 5-7 shall be 'zero' -- } (SIZE (8 . . ub-bit-options))

ProbeIdentifier ::= MTSIdentifier
```

FIGURA 4/X.411 (Parte 9 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
ReportIdentifier ::= MTSIdentifier

ReportDestinationName ::= ORAddressAndOptionalDirectoryName

SubjectIdentifier ::= MessageOrProbeIdentifier

MessageOrProbeIdentifier ::= MTSIdentifier

SubjectIntermediateTraceInformation ::= TraceInformation

AdditionalInformation ::= ANY        -- maximum ub-additional-info octets including all encoding

ActualRecipientName ::= ORAddressAndOptionalDirectoryName

LastTraceInformation ::= SET {
        arrival-time [0] ArrivalTime,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        report-type [1] ReporType }

OriginallyIntendedRecipientName ::= ORAddressAndOptionalDirectoryName
```

FIGURA 4/X.411 (Parte 10 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Campos de ampliación
originator-requested-alternate-recipient EXTENSION
        OriginatorRequestedAlternateRecipient
        ::= 2

OriginatorRequestedAlternateRecipient ::= ORAddressAndOptionalDirectoryName

internal-trace-information EXTENSION
        InternalTraceInformation
        ::= 38
```

FIGURA 4/X.411 (Parte 11 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
InternalTraceInformation ::= SEQUENCE SIZE (1 . . ub-transfers) OF InternalTraceInformationElement

InternalTraceInformationElement ::= SEQUENCE {
        global-domain-identifier GlobalDomainIdentifier,
        mta-name MTAName,
        mta-supplied-information MTASuppliedInformation }

MTASuppliedInformation ::= SET {
        arrival-time [0] ArrivalTime,
        routing-action [2] RoutingAction,
        attempted CHOICE {
                mta MTAName,
                domain GlobalDomainIdentifier } OPTIONAL,
        -- additional-actions-- COMPONENTS OF InternalAdditionalActions }

InternalAdditionalActions ::= AdditionalActions
```

FIGURA 4/X.411 (Parte 12 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

```
-- Tipos de parámetros comunes

TraceInformation ::= [APPLICATION 9] SEQUENCE (SIZE (1 . . ub-transfers) OF TraceInformationElement

TraceInformationElement ::= SEQUENCE {
        global-domain-identifier GlobalDomainIdentifier,
        domain-supplied-information DomainSuppliedInformation }

DomainSuppliedInformation ::= SET {
        arrival-time [0] ArrivalTime,
        routing-action [2] RoutingAction,
        attempted-domain GlobalDomainIdentifier OPTIONAL,
        -- additional-actions-- COMPONENT OF AdditionalActions }

AdditionalActions ::= SET {
        deferred-time [1] DeferredTime OPTIONAL,
        converted-encoded-information-types ConvertedEncodedInformationTypes OPTIONAL,
        other-actions [3] OtherActions DEFAULT {} }

RoutingAction ::= ENUMERATED {
        relayed (0),
        rerouted (1) }

DeferredTime ::= Time

ArrivalTime ::= Time

OtherActions ::= BIT STRING {
        redirected (0),
        dl-operation (1) } (SIZE (0 . . ub-bit-options))

END  -- de servicio abstracto STRM
```

FIGURA 4/X.411 (Parte 13 de 13)

Definición de la sintaxis abstracta del servicio abstracto de ATM

14 Procedimientos de funcionamiento distribuido del STRM

En este punto, se especifican los procedimientos para el funcionamiento distribuido del STRM, que ejecutan los ATM. Cada ATM aplica individualmente los procedimientos descritos a continuación; la acción colectiva de todos los ATM presta el servicio abstracto de STRM a los usuarios del STRM.

Aunque los procedimientos incluyen la mayoría de las acciones importantes requeridas de un ATM, se ha omitido gran cantidad de detalles para una mayor claridad de exposición y para evitar cualquier redundancia innecesaria. Para un tratamiento definitivo de las acciones del ATM deberían consultarse las definiciones del servicio-abstracto.

14.1 *Visión de conjunto del modelo del ATM*

14.1.1 *Organización y técnica de realización de los modelos*

La descripción de los procedimientos para un ATM único se basa en el modelo mostrado en las figuras 5/X.411 a 11/X.411 que se describe a continuación. Debe observarse que se incluye el modelo con fines expositivos únicamente y no se pretende limitar en modo alguno la realización de un ATM.

Ni los procedimientos mostrados ni el orden de los pasos de procesamiento en ellos, implican necesariamente características específicas de un ATM real.

El modelo distingue entre *módulos* y *procedimientos*. Los *módulos*, en el sentido en que se utilizan aquí, son entidades de proceso autónomas que pueden ser invocadas por otros módulos u otros sucesos externos al ATM, los cuales pueden a su vez invocar otros módulos o generar otros sucesos externos. Los módulos no están unidos entre sí mediante una estructura de control descrita explícitamente; sino que la estructura de control entre los módulos surge de su esquema de invocaciones recíprocas. Los módulos corresponden a *objetos* en el sentido de la programación orientada-objeto.

Se utilizan aquí los *procedimientos* en el sentido convencional de programación. Los procedimientos están orientados a tareas o funciones. Los procedimientos pueden llamar a otros procedimientos, en forma de subrutinas, con devolución de control al procedimiento llamante cuando ha finalizado el procedimiento llamado. Tales llamadas pueden anidarse hasta una profundidad arbitraria, pudiendo, asimismo, autollamarse el procedimiento de forma recurrente. Los procedimientos están unidos entre sí mediante estructuras de control definidas explícitamente, construidas a partir de llamadas a procedimientos y de dispositivos de programación convencional como iteracciones y ejecuciones condicionales.

En el modelo, existen procedimientos dentro de los módulos. Cada módulo contiene al menos un procedimiento y puede contener varios. En el último caso, los procedimientos y la estructura de control de gobierno se describen explícitamente. En el primer caso, la existencia de un procedimiento único de módulos se trata generalmente como implícita.

Utilizando estas técnicas para la realización de modelos, puede perfeccionarse un proceso de aplicación del ATM de la forma siguiente: para cada operación-abstracta (tanto usuaria como suministradora) que puede existir entre un ATM y los usuarios-STRM que sirve, o entre un ATM y los otros ATM con los que coopera, hay un módulo único denominado *módulo externo*. El conjunto de módulos externos es responsable de la entrada y salida de mensajes, sondas e informes al ATM y del soporte de operaciones tales como vinculación-STRM, desvinculación-STRM, registro, control-remisión y control-entrega. Los módulos externos se muestran en la figura 5/X.411 y se describen en los § 14.5 a 14.10, agrupados por puertos.

Para realizar las diferentes operaciones-abstractas de las cuales es responsable, un ATM debe ejecutar ciertas operaciones de proceso sobre cada mensaje, sonda o informe que entra o se origina en él. En el modelo, esto es competencia de los *módulos internos*, mostrados en figura 6/X.411 y descritos en los § 14.2 a 14.4.

Los módulos externos e internos se relacionan entre sí de la forma siguiente: un módulo externo se comunica únicamente con un módulo interno, y no con otro módulo externo o directamente con un procedimiento dentro de un módulo interno. Así, los módulos internos no sólo soportan el volúmen de proceso dentro de un ATM, sino que sirven igualmente como enlaces entre sus módulos externos. Además de los módulos internos, la figura 6/X.411 muestra igualmente los módulos con los que se comunican.

El ATM está dirigido por sucesos en el sentido que permanece en reposo hasta que se detecta un suceso en una de sus puertas. Muchos de los sucesos, tales como la invocación de una operación-abstracta vinculación-STRM, control-remisión, control-entrega o registro por parte de un usuario-STRM u otro ATM se tratan directa y

completamente por el módulo asignado a esta operación-abstracta. Sin embargo, otros sucesos arrancan un proceso que puede reverberar a través del ATM, perdurar durante un cierto tiempo y finalmente provocar uno o más sucesos de salida. Estos sucesos hacen intervenir los módulos de proceso internos y son:

a) un mensaje o sonda originado por un usuario-STRM soportado localmente entra a través del puerto-remisión;

b) un mensaje, sonda o informe retransmitido desde otro ATM entra a través del puerto-transferencia.

Puesto que el proceso en el interior de un ATM puede resultar bastante complejo, especialmente para mensajes con múltiples destinatarios, el módulo supone, como dispositivo interno de contabilidad, que cada mensaje transporta consigo un conjunto de instrucciones, una para el mensaje en su conjunto y una para cada destinatario. Estas instrucciones ayudan a guiar un mensaje a través de los pasos de proceso y transportan la información entre los módulos y procedimientos internos al ATM.

Nota 1 – Los procedimientos descritos aquí están dirigidos al proceso de un mensaje único. Esto resulta adecuado para todos los efectos menos para uno: la disposición en cola de mensajes y la prioridad relativa de invocación de los procedimientos están gobernados explícitamente por el argumento **prioridad** en el caso de un mensaje que entra a través del puerto-remisión o puerto-transferencia, o implícitamente (de prioridad urgente) en el caso de un informe o una prueba que se genera internamente o que entra a través del puerto-transferencia.

Nota 2 – Un ATM puede especificar por defecto varias ventanas de tiempo de entrega para cada prioridad de mensaje (por ejemplo, aquellos valores definidos en las Recomendaciones de la serie F.400). El STRM y por tanto, cada ATM afectado debería tener en cuenta dichos valores durante el proceso del mensaje. Por ejemplo, el ATM puede aplicar un plazo máximo de entrega. Si este periodo de tiempo expira antes de la entrega, el ATM genera un informe-no-entrega y descarta el mensaje. Las acciones requeridas en este caso son idénticas a las acciones requeridas cuando se alcanza el **último-tiempo-entrega.**

Nota 3 – El examen de la información-rastreo es incompleto debido a su naturaleza compleja. Se señalan algunos detalles importantes pero el tratamiento completo y definitivo del informe-rastreo aparece en el § 12.3.1.

14.2 *Módulo de entrega diferida*

Este módulo proporciona el elemento-de-servicio de entrega diferida. Es invocado por los módulos de remisión-mensaje y entrada-mensaje que pasan un mensaje para comprobar la petición de entrega diferida y retenerla, si es necesario. Invoca el módulo principal, pasando sucesivamente el mensaje hasta la finalización de su procedimiento interno único.

14.2.1 *Procedimiento de entrega-diferida*

14.2.1.1 *Argumentos*

Un mensaje para comprobación de la petición de entrega diferida y retención, si es necesario.

14.2.1.2 *Resultados*

Se devuelve el mensaje después de expirar el **tiempo-entrega-diferida**. Si se ha producido ésta, el mensaje va acompañado de un estampillado de fecha.

14.2.1.3 *Errores*

Ninguno.

14.2.1.4 *Descripción del procedimiento*

Se comprueba en el mensaje la presencia del campo de **tiempo-entrega-diferida**. Si está ausente, el procedimiento devuelve el mensaje y finaliza. Si está presente, se compara el **tiempo-entrega-diferida** con el tiempo presente. Si el **tiempo-entrega-diferida** ha expirado, el procedimiento devuelve el mensaje y finaliza.

Por el contrario, en el caso de un mensaje retransmitido, el ATM comprueba la existencia de un acuerdo bilateral que le obligue a proporcionar la entrega diferida de este mensaje. Si está ausente, el procedimiento devuelve el mensaje y finaliza.

En caso contrario, según los acuerdos bilaterales o políticas en ese respecto, se anota el instante actual como instante de llegada del mensaje, y se retiene éste hasta la expiración del **tiempo-entrega-diferida**. Seguidamente, y como resultado, se devuelven el mensaje y el estampillado de fecha. Finaliza entonces el procedimiento.

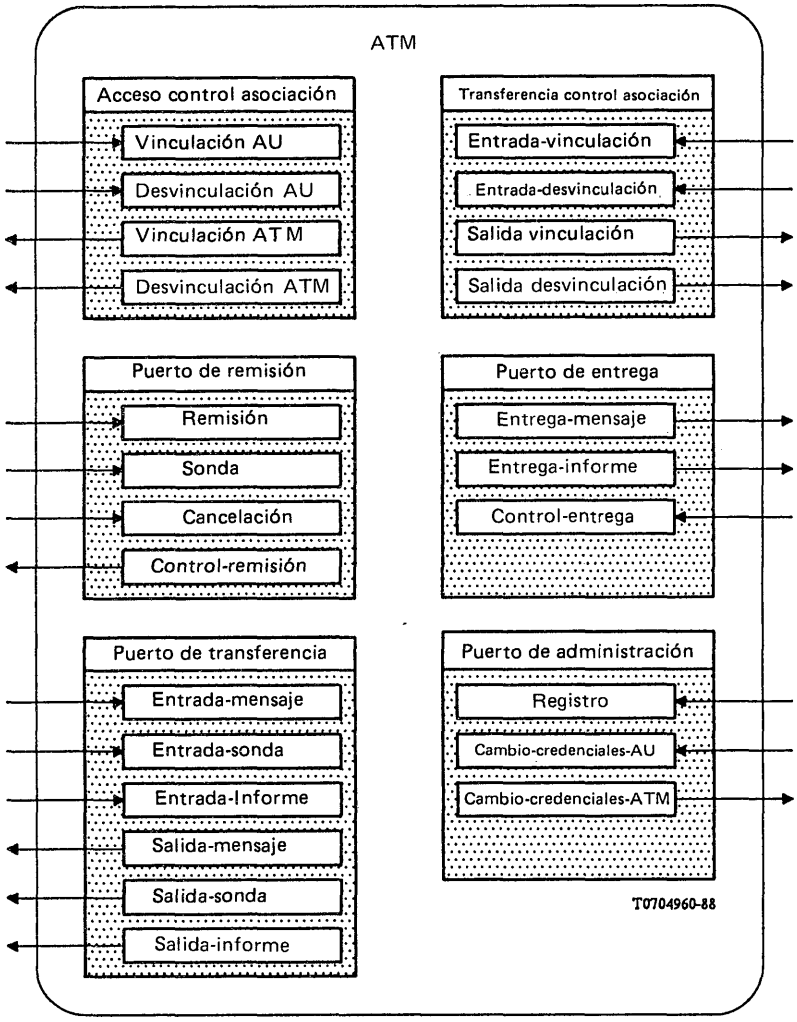


FIGURA 5/X.411

Puertas y módulos de un ATM

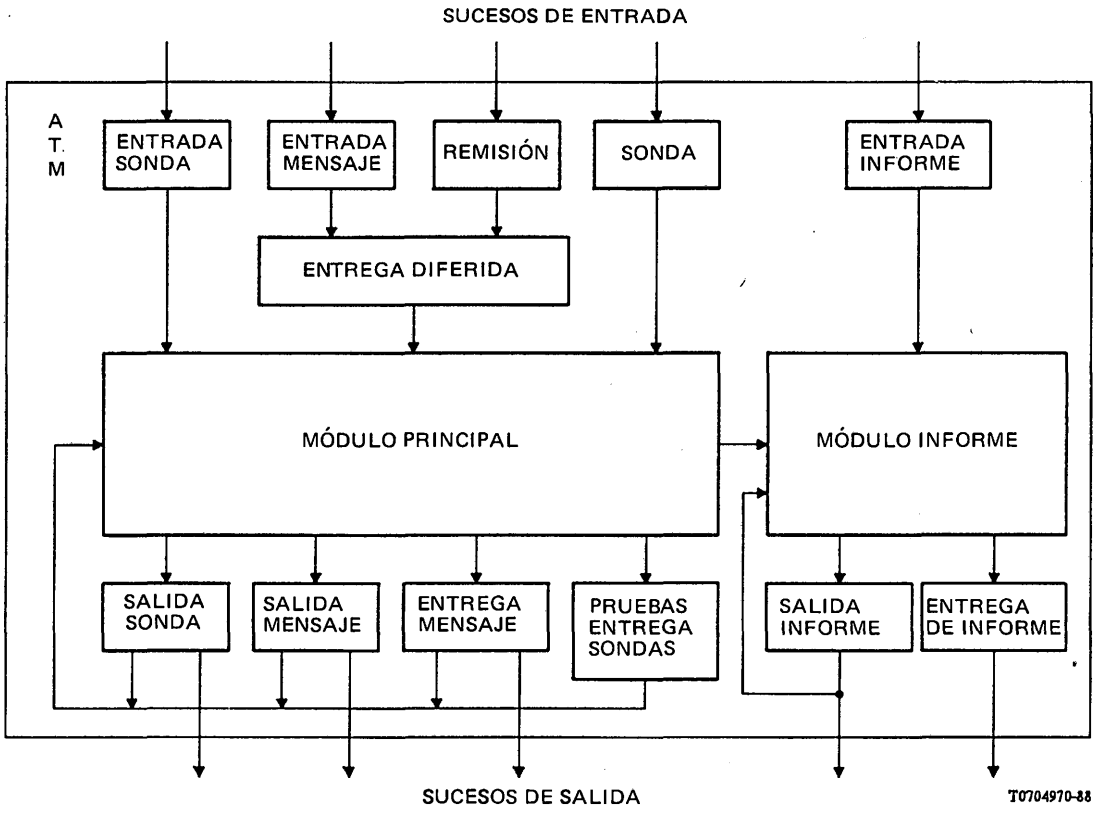


FIGURA 6/X.411

Relación entre los módulos internos y externos

14.3 *Módulo principal*

El módulo principal ejecuta el grueso de tratamiento de los mensajes y sondas que entran en el ATM. La figura 6/X.411 muestra las relaciones entre el módulo principal y los módulos que puede invocar o por los que puede ser invocado. El módulo principal está sujeto a la invocación por:

1) el módulo entrada-sonda, que transfiere una sonda;
2) el módulo entrega-diferida, que transfiere un mensaje;
3) el módulo sonda, que transfiere una sonda.

En el caso de una condición de error o de la necesidad de un informe positivo de entrega, el módulo principal puede ser invocado igualmente por:

4) el módulo de salida-mensaje, que cursa un mensaje con una instrucción por-mensaje que indica el problema encontrado;
5) el módulo salida-sonda, que cursa una sonda con una instrucción por-mensaje que indica el problema encontrado;
6) el módulo entrega-mensaje, que cursa un mensaje con instrucciones por-destinatario que indica el problema o problemas o el suceso o sucesos encontrados;
7) el módulo prueba-entrega-sonda, que cursa una sonda con instrucciones por-destinatario que indica el problema o problemas o el suceso o sucesos encontrados.

El módulo principal contiene procedimientos que, colectivamente, proporcionan las siguientes funciones:

- Procesamiento de rastreo
- Detección de bucle
- Encaminamiento y reencaminamiento
- Redireccionamiento del destinatario
- Conversión de contenido
- Ampliación de lista de distribución
- Réplica del mensaje
- Autenticación del origen de los mensajes y de las sondas
- Resolución del nombre.

Los procedimientos que ejecutan estas funciones se llaman mediante el procedimiento de control único que guía el tratamiento de cada mensaje o sonda recibido por el módulo principal. La figura 7/X.411 muestra la organización de los procedimientos de control y subsidiarios dentro del módulo principal; la figura 8/X.411 muestra el flujo de información a través de estos procedimientos.

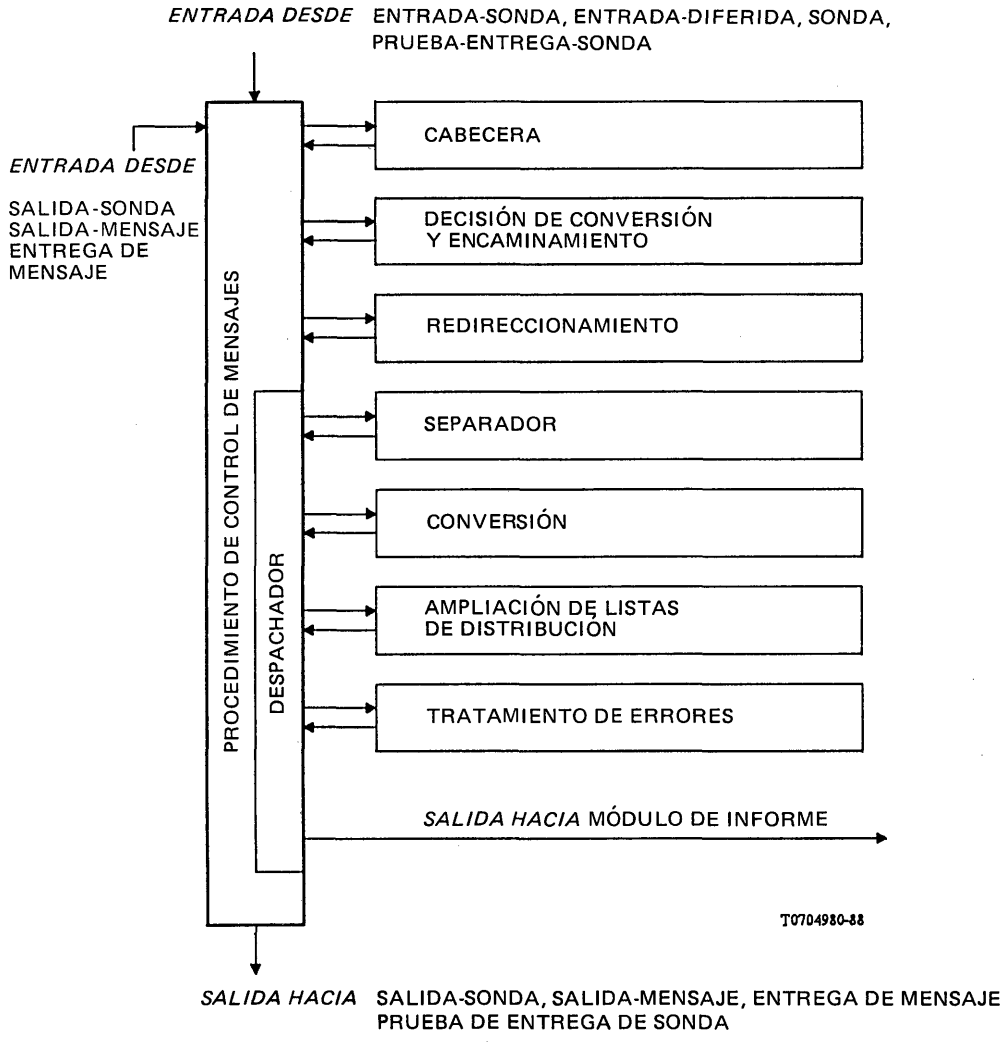
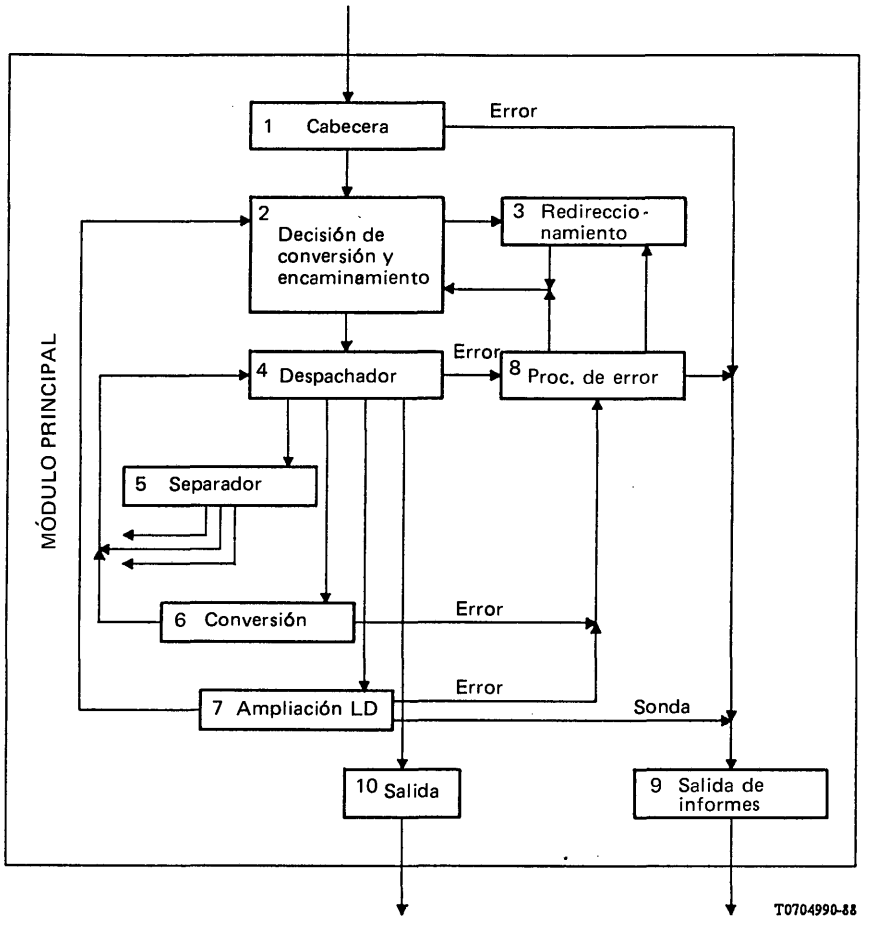


FIGURA 7/X.411

Organización de los procedimientos en el módulo principal



Nota – En esta figura, los números hacen referencia a los pasos numerados de la lógica del procedimiento de control (§ 14.3.1.4).

FIGURA 8/X.411

Flujo de información dentro del módulo principal

Para cada mensaje o sonda recibido, el módulo principal llama al procedimiento de control con dicho mensaje o sonda como argumento. Como resultado, el procedimiento de control devuelve una o más réplicas del mensaje o sonda con las instrucciones apropiadas adjuntas. Dependiendo de la naturaleza de esas instrucciones el módulo principal invoca entonces:

1) el módulo de salida-mensaje, al cual cursa cada mensaje con una instrucción de transferencia por-mensaje;
2) el módulo de salida-sonda, al cual cursa cada sonda con una instrucción de transferencia por-mensaje;
3) el módulo de entrega-mensaje, al cual cursa cada mensaje con una o más instrucciones de entrega por-destinatario;
4) el módulo de prueba-entrega-sonda, al cual cursa cada sonda con una o más instrucciones de entrega por-destinatario;
5) el módulo de informe, al cual cursa cada mensaje o sonda con una instrucción por-mensaje y/o una o más instrucciones por-destinatario que indican la generación de un informe.

14.3.1 *Procedimiento de control*

Este procedimiento dirige cada mensaje o sonda entrantes a través de los procedimientos restantes del módulo principal. El flujo global de información se muestra en la figura 8/X.411.

14.3.1.1 *Argumentos*

Uno de los siguientes (estos argumentos corresponden a los mensajes y sondas que pueden cursarse al módulo principal, después de invocación):

1) un mensaje o sonda sin instrucciones (procedentes del módulo de entrada-sonda o sonda);
2) un mensaje sin instrucciones, pero con estampillado opcional de instante de llegada (procedente del módulo de entrega diferida);
3) un mensaje o sonda con una instrucción por-mensaje que describe un problema de transferencia (procedente del módulo de salida-mensaje o salida-sonda);
4) un mensaje o sonda con instrucciones por-destinatario que describen los problemas de entrega o los éxitos (procedente del módulo de entrega-mensaje o prueba-entrega-sonda).

14.3.1.2 *Resultados*

1) Una o más réplicas del argumento del mensaje o de la sonda, cada una acompañada por una instrucción por-mensaje que indica la transferencia, y/o
2) una o más réplicas del argumento del mensaje o sonda, cada una de ellas acompañada por una o más instrucciones por-destinatario que indican la entrega o la prueba de entrega, y/o
3) una o más réplicas del argumento del mensaje o sonda, cada una acompañada por una o más instrucciones por-destinatario que indican la generación de un informe.

14.3.1.3 *Errores*

Ninguno. Las condiciones de error se tienen en cuenta en los resultados descritos anteriormente.

14.3.1.4 *Descripción del procedimiento*

1) Mensaje o sonda sin instrucciones:

   Se llama primero al procedimiento de cabecera para efectuar la inicialización del rastreo y varias comprobaciones mensaje por mensaje, como la de expiración de mensaje y la detección de bucle de encaminamiento.

   Al recibir una devolución con instrucción de informe que indique un problema en relación con el mensaje, el proceso continúa en el paso 9.

   En todas las otras devoluciones el procedimiento continúa como sigue:

2) Se llama al procedimiento de decisión-conversión-y-encaminamiento para calcular las instrucciones de encaminamiento y conversión por-destinatario. (Son instrucciones completas que dirigirán el mensaje o sonda a través del resto de los procedimientos.)

   Si se indica una instrucción de redireccionamiento (por ejemplo, destinatario-alternativo-solicitado-destinatario), el proceso continúa en el paso 3.

   En los demás casos restantes, el proceso continúa en el paso 4 (despachador.)

3) Se llama al redireccionamiento. Al recibir una devolución con éxito, el proceso continúa en el paso 2.

   En el caso de una devolución infructuosa, el proceso continúa en el paso 8 (manipulador-error.)

4) Despachador. El despachador actúa sobre las instrucciones generadas y transfiere el control al primero de los siguientes procedimientos que resulte aplicable:
   - división (paso 5);
   - conversión (paso 6);
   - ampliación-lista-distribución (paso 7);
   - tratamiento-error (paso 8) en el caso en que el proceso de decisión encontró un problema, por ejemplo, error de encaminamiento;
   - salida (paso 10).

5) Se llama al divisor para la realización de réplicas, cuando se solicita en las instrucciones por-destinatario generadas en el procedimiento de decisión-conversión-y-encaminamiento. Para cada réplica el proceso continúa por separado en el paso 4 (despachador.)

6) Se llama a la conversión para cada mensaje o sonda que necesite conversión.

   Al devolver con éxito el mensaje o sonda, el proceso continúa en el paso 4 (despachador.)

   Después de una devolución con instrucción de informe que indica un error de conversión, el proceso continúa en el paso 8 (manipulador-error.)

7) Se llama al procedimiento de ampliación-LD.

Después de la devolución con éxito de un mensaje, el proceso continúa en el paso 2 de forma que los destinatarios resultantes de la ampliación de la LD puedan tratarse convenientemente.

Si se devuelve una copia del mensaje con instrucciones de informe de entrega, en lugar de, o además de, la devolución anterior, el proceso continúa en el paso 9.

Una sonda que retorna con éxito llevará instrucciones de informe; el proceso continúa en el paso 9 (generación-informe.)

Después de la devolución de un mensaje o sonda con una instrucción de informe que indique una ampliación de LD, el proceso-error continúa en el paso 8.

8) Este es el punto de recogida que alcanza el proceso al detectar que un mensaje o sonda no puede ser tratado por los procedimientos de línea principales. Se llama al procedimiento de proceso-error para buscar otro método de entrega o un destinatario-alternativo. Después de una devolución con éxito, el procedimiento de proceso-error indica el nuevo destinatario en una instrucción al procedimiento de decisión-conversión-y-encaminamiento (paso 2), donde continúa el proceso.

Si no es posible el redireccionamiento, el mensaje o sonda se pasa al generador del informe (paso 9).

9) El procedimiento de control finaliza en este punto y devuelve un mensaje o sonda con las instrucciones de generación de informe.

10) Cuando un mensaje o sonda alcanza este punto, finaliza el procedimiento de control.

14.3.2 *Procedimiento de cabecera*

Este procedimiento efectúa la iniciación del rastreo, la detección de la expiración del mensaje, la comprobación inicial de seguridad, la detección de bucles y la comprobación de la criticidad.

14.3.2.1 *Argumentos*

Un mensaje o sonda y un estampillado opcional de instante de llegada.

14.3.2.2 *Resultados*

El mensaje o sonda con información inicializada de rastreo para este ATM.

14.3.2.3 *Errores*

El mensaje o sonda con instrucciones de generación del informe que detalla el problema encontrado.

14.3.2.4 *Descripción del procedimiento*

1) Si el mensaje ha cruzado una frontera entre dominios, se añade un **elemento-información-rastreo** de este dominio a la **retransmisión** como acción. Si el mensaje va acompañado de un tiempo-llegada, es que ha habido dilación de entrega; se fija entonces **tiempo-diferido** en el instante actual, y **tiempo-llegada** en el valor del estampillado de fecha acompañante. En caso contrario, no ha habido dilación, y se fija **tiempo-llegada** al valor del instante actual. Se añade igualmente un **elemento-información-rastreo-interno** tanto si el mensaje ha cruzado la frontera entre dominios como si no lo ha hecho.

2) Si lo requiere la política de seguridad en vigor y/o si la **verificación-autenticación-origen-mensaje** es incorrecta, el procedimiento devuelve una instrucción de generación de informe. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se fijan en **incapaz-de-transferir** y **error-mensajería-segura**, respectivamente.

3) Si alguno de los campos de extensión está marcado como crítico para la retransmisión pero el ATM no lo entiende semánticamente, el procedimiento devuelve una instrucción de generación de informe. El **código-motivo-no-entrega** se pone en **fallo-transferencia** y el **código-diagnóstico-no-entrega** en **función-crítica-no-soportada**. Finaliza entonces el procedimiento.

4) Si se ha sobrepasado el **último-tiempo-entrega**, o si ha transcurrido el máximo tiempo de tránsito del sistema para la **prioridad** del mensaje, el procedimiento devuelve una instrucción de generación de informe. El **código-motivo-no-entrega** se pone en **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone a **tiempo-máximo-expirado**. Finaliza entonces el procedimiento.

5) Se realiza la detección de bucles. El algoritmo de detección de bucles se encuentra fuera del alcance de esta Recomendación. Sin embargo, en el § 14.3.11 se facilita un ejemplo de algoritmo combinado de encaminamiento y de detección de bucles. Si se detecta un bucle, el procedimiento devuelve una instrucción de generación de informe. El **código-motivo-no-entrega** se pone en **fallo-transferencia** y el **código-diagnóstico-no-entrega** se pone en **bucle-detectado**. Finaliza entonces el procedimiento.

14.3.3 *Procedimiento de decisión-conversión-encaminamiento*

Para cada destinatario de un mensaje o sonda cuyo responsable es el ATM, este procedimiento determina las acciones de encaminamiento y conversión, si ha lugar, que ha de tomar este ATM. Las acciones se registran como instrucciones por-destinatario asociadas al mensaje. Las acciones se llevan a cabo subsiguientemente mediante otros sub-procedimientos dentro del procedimiento interno o en cualquier otro lugar del ATM.

Nota – Para cada mensaje particular, es posible invocar más de una vez este procedimiento. En ese caso, el procedimiento ignora las instrucciones por destinatario generadas por anteriores invocaciones que aún no se han hecho actuar sobre ningún otro ente.

14.3.3.1 *Argumentos*

1) Un mensaje o sonda con **responsabilidad** verdadera para aquellos destinatarios bajo la tutela de este ATM.

14.3.3.2 *Resultados*

El mensaje o sonda que formaron el argumento del procedimiento más las instrucciones por-destinatario nuevas o revisadas que indican el encaminamiento y la posible acción de conversión que debería emprender este ATM.

14.3.3.3 *Errores*

Ninguno. Las condiciones de error, si las hay, se señalan en las instrucciones por-destinatario.

14.3.3.4 *Descripción del procedimiento*

Se considera cada vez un destinatario. Si la **responsabilidad** es falsa, se ignora el destinatario. En caso contrario, se llama a los procedimientos de decisión-conversión y decisión-encaminamiento para cada destinatario. Cuando se han considerado todos los destinatarios se finaliza el procedimiento. Véase la figura 9/X.411.

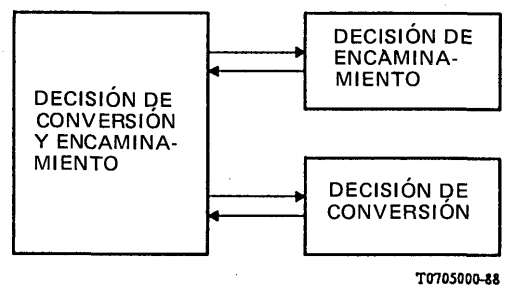


FIGURA 9/X.411

Organización de los procedimientos dentro del procedimiento de decisión de conversión y encaminamiento

14.3.4 *Procedimiento de decisión-encaminamiento*

Este procedimiento genera una instrucción de encaminamiento para un destinatario único del mensaje.

14.3.4.1 *Argumentos*

1) Un destinatario de mensaje más la instrucción por-destinatario, si la hay, aplicable a este destinatario.

2) La instrucción por-mensaje, si la hay, aplicable a este mensaje. Otros campos de mensaje resultan igualmente accesibles al procedimiento si se necesitan.

14.3.4.2 *Resultados*

Una instrucción de encaminamiento nueva o posiblemente revisada aplicable a este destinatario. Las posibles instrucciones son:

a) retransmisión a otro ATM;

b) entrega a un destinatario local;

c) ampliar la lista de distribución representada por este destinatario;

d) generar un informe que indique el fallo de la entrega. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** se incluyen en la instrucción;

e) redirigir a un destinatario alternativo especificado por un destinatario.

14.3.4.3 *Errores*

Ninguno. Las condiciones de error se registran en la instrucción de encaminamiento.

14.3.4.4 *Descripción del procedimiento*

El procedimiento se describe según los siguientes pasos.

Nota – Para garantizar que no se viole la política-seguridad durante el encaminamiento se debería comprobar que la **etiqueta-seguridad-entrega** resulta apropiada respecto del **contexto-seguridad**.

1) Si existe una instrucción por-mensaje que indica un fallo previo de retransmisión, el procedimiento calcula entonces un destino alternativo del próximo salto para este destinatario. La elección del algoritmo de encaminamiento está fuera del alcance de esta Recomendación. Sin embargo, en el § 14.3.11 se incluye un ejemplo de algoritmo aplicable. Si tuvo éxito, la **información-rastreo-interna** del mensaje se actualiza con una acción reencaminamiento **reencaminado** para reflejar el hecho de que se ha reencaminado el mensaje (véase el § 12.3.1). Si el menaje tuviera que haber cruzado una frontera de dominio se actualizaría, la **información-rastreo** en consecuencia. El procedimiento devuelve una instrucción de retransmisión al destino alternativo y finaliza.

   Si no existe un siguiente salto alternativo disponible o todos los saltos siguientes disponibles han sido ensayados infructuosamente o están prohibidos, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** se pone a **fallo-transferencia** y el **código-diagnóstico-no-entrega** se pone en consonancia con el fallo de retransmisión encontrado. El procedimiento finaliza entonces.

2) Si la instrucción por-destinatario indica un fallo de entrega, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** son los suministrados por el procedimiento de entrega-mensaje o entrega-informe. El procedimiento finaliza entonces.

3) Si el destinatario es una lista de distribución para la cual este ATM sirve como punto de ampliación, se examina entonces el argumento de **ampliación-LD-prohibida** del mensaje. Si el valor es **ampliación-LD-autorizada** el procedimiento devuelve una instrucción de encaminamiento (sujeta a la política-seguridad en vigor) para ampliar la lista de distribución y finaliza.

   Si el valor es **ampliación-LD-prohibida** o la política-seguridad prohibe la utilización de una LD, el procedimiento devuelve entonces una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** se pone a **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** a **ampliación-LD-prohibida**. El procedimiento finaliza entonces.

   En todos los demás casos, se siguen los siguientes pasos.

4) Si el destinatario resulta ser local, es decir, un usuario-STRM directamente soportado por este ATM, se siguen los siguientes pasos:

   a) Se comprueba la **dirección O/D** para garantizar que especifica sin ambigüedad un destinatario real local. En caso contrario, el procedimiento devuelve una instrucción de generación de informe para este destinatario. El **código-motivo-no-entrega** se pone a **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone a **nombre-O/D-no-reconocido** o **nombre O/D-ambiguo** según convenga. El procedimiento finaliza entonces.

   b) Si la **dirección O/D** especifica un destinatario local real, se comprueban los parámetros de registro del destinatario en relación con el destinatario-alternativo-solicitado-destinatario. En la determinación de un destinatario-alternativo, debería comprobarse la **etiqueta-seguridad-usuario** respecto de la **etiqueta-seguridad-mensaje** para garantizar que no se produce ninguna violación de la política-seguridad.

Si el **destinatario-alternativo-asignado-destinatario** está de hecho autorizado por el campo de **reasignación-destinatario-prohibida** y permitido por la política-seguridad, se genera entonces una instrucción de redireccionamiento y finaliza el procedimiento.

En caso contrario, el procedimiento devuelve una instrucción de informe para este destinatario y finaliza. El **código-motivo-no-entrega** se pone a **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone según convenga.

c) Si el **destinatario-alternativo-asignado-destinatario** no está vigente, se comprueba entonces el mensaje respecto de los parámetros restantes del registro del destinatario. Por ejemplo, se compara la longitud del contenido del mensaje con la **longitud-máxima-contenido-entregable**, el **tipo-contenido** del mensaje con los **tipos-contenido-entregables** del destinatario, etc. Si no se encuentra ningún problema, el procedimiento de decisión-encaminamiento devuelve una instrucción de entrega para este destinatario y finaliza.

Si existe un problema entre el mensaje de los parámetros del registro, el procedimiento devuelve una instrucción de generación de informe a este destinatario. El **código-motivo-no-entrega** se pone en **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone en consonancia con el problema del mensaje encontrado. Finaliza entonces el procedimiento.

5) Si el destinatario no es local para éste ATM, el procedimiento de decisión-encaminamiento intenta determinar una siguiente instrucción de salto (sujeta a la política-seguridad en vigor) para este destinatario. Si tiene éxito, se devuelve una instrucción de retransmisión al siguiente salto y finaliza el procedimiento.

Si no puede determinarse el salto siguiente, el procedimiento devuelve una instrucción de generación de informe a este destinatario. El **código-motivo-no-entrega** se pone en **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** se pone en consonancia con el problema encontrado. Finaliza entonces el procedimiento.

14.3.5 *Procedimiento de decisión-conversión*

Este procedimiento genera una instrucción de conversión para un destinatario único del mensaje.

14.3.5.1 *Argumentos*

1) Un destinatario de un mensaje o sonda más la instrucción por destinatario, si existe, aplicable a este destinatario.
2) Otros campos de mensaje son considerados igualmente por el procedimiento:
   a) **tipos-información-codificada-original,**
   b) **conversión-implícita-prohibida,**
   c) **conversión-con-pérdida-prohibida,**
   d) **conversión-explícita.**

14.3.5.2 *Resultados*

1) Una instrucción de conversión de contenido aplicable a este destinatario y, posiblemente,
2) una instrucción revisada de encaminamiento que indica la salida-retransmisión o salida-sonda hacia un ATM capaz de realizar la conversión-requerida o, en lugar de los 1 y 2 anteriores,
3) una instrucción para generar un informe que indica un fallo de entrega. El **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** se incluyen en esta instrucción.

14.3.5.3 *Errores*

Ninguno. Las condiciones de error se registran en la instrucción de encaminamiento.

14.3.5.4 *Descripción del procedimiento*

Nota – Como las circunstancias bajo las cuales ATM realiza la conversión se dejan para un estudio ulterior, no resulta práctico describir un procedimiento para decidir qué EIT se requieren para la salida de la conversión. Por ejemplo, si un ATM intermedio desarrolla la conversión, no existe ningún camino normalizado para conocer los EIT que puede manejar un usuario-STRM. En consecuencia, las siguientes cláusulas suponen que el ATM conoce los EIT para la conversión.

1) Si se requiere una conversión explícita para este destinatario, el procedimiento comienza en el paso 6.
2) Si se requiere una conversión implícita pero el destinatario no está abonado a la facilidad de conversión implícita, el procedimiento devuelve una instrucción de informe negativo en el **código-motivo-no-entrega** de **conversión-no-realizada** y el **código-diagnóstico-no-entrega** de **conversión-implícita-no-abonada**. Finaliza entonces el procedimiento.

3) Si la conversión requerida no resulta práctica, el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada** y el **código-diagnóstico-no-entrega** de **conversión-no-práctica**. Finaliza entonces el procedimiento.

4) Si se requiriese, la conversión del mensaje pero estuviese prohibida, el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada**, y el **código-diagnóstico-no- entrega** de **conversión-prohibida**. Finaliza entonces el procedimiento.

5) Si la conversión requerida causara una pérdida de información y el campo de **conversión-con-pérdida-prohibida** adopta el valor de **con-pérdida-prohibido**; el procedimiento genera una instrucción de informe negativo con el **código-motivo-no-entrega** de **conversión-no-realizada** y uno de los siguientes **código-motivo-no-entrega**, según proceda:

   – **línea-demasiado-larga**,
   – **página-partida**,
   – **pérdida-símbolo-pictórico**,
   – **pérdida-símbolo-puntuación**,
   – **pérdida-carácter-alfabético**, o
   – **pérdida-información-múltiple**.

   Seguidamente, termina el procedimiento.

6) Si la conversión requerida resulta admisible, y no puede ser realizada por este ATM, pero puede ser realizada por un ATM conocido de este ATM, se genera entonces una instrucción de no conversión. La instrucción de encaminamiento previamente generada se cambia por salida-transferencia o salida-sonda, con un destino del próximo salto apropiado para el ATM en cuestión. Seguidamente, termina el procedimiento.

7) Si la conversión requerida puede ser efectuada por ese ATM, el procedimiento devuelve una instrucción de efectuar la conversión, y finaliza.

14.3.6 *Procedimiento de proceso-error*

Cuando otro procedimiento encuentra un error de capacidad de entrega o encaminamiento, se llama a este procedimiento para determinar si pueden lograrse la entrega o el encaminamiento mediante la reasignación del destinatario o eligiendo una dirección-O/D diferente para el mismo destinatario. En caso contrario, debe señalarse la no-entrega al módulo de informe. Los errores que provocan una llamada a este procedimiento son:

– **nombre-destinatario** que no identifica un usuario-STRM;
– fallo de entrega;
– un ATM que es incapaz de realizar la conversión necesaria;
– problemas del trayecto de transferencia;
– problemas de ampliación-LD;
– violaciones de seguridad;
– conflicto con parámetros de registro.

Nota – La acción emprendida en relación con el proceso-error deberá estar sujeta a la política-seguridad en vigor.

14.3.6.1 *Argumentos*

1) Un mensaje o sonda con los campos por-destinatario que provocaron el problema.
2) Instrucciones de informe que indican el error.

14.3.6.2 *Resultados*

El mensaje o sonda en cuestión con un campo de **nombre-destinatario**, actualizado, o

1) el mensaje o sonda en cuestión;
2) instrucciones de informe.

14.3.6.3 *Errores*

Ninguno.

14.3.6.4 *Descripción del procedimiento*

Nota – Un determinado destinatario puede llamar a este procedimiento múltiples veces. Ocasionalmente agotará todas las alternativas y ejecutará el paso 5 para informar del fallo.

1) Los argumentos se comprueban respecto de un **nombre-guía**. Si está presente, el procedimiento realiza una consulta a la guía para determinar una nueva **dirección-O/D**. La **dirección-O/D**, si la hay, así extraída de la guía se comprueba para ver si satisface el argumento del **método-entrega-solicitado**, si existe. Si la comprobación tiene éxito, se sustituye la nueva **dirección-O/D** por la antigua y finaliza el procedimiento.

   Nota – Tras la sustitución de la nueva **dirección-O/D** por la original, el mensaje puede legítimamente ser encaminado hacia una DG/ATM que ya haya visitado. Queda para ulterior estudio la técnica para evitar la detección prematura de un bucle de reencaminamiento.

2) En caso contrario, el procedimiento determina si se especificó un **destinatario-alternativo-solicitado-destinatario** para el destinatario en cuestión. Si es así, se llama al procedimiento de redireccionamiento junto con el mensaje, indicados los campos pertinentes como argumento. Al volver satisfactoriamente del redireccionamiento, el procedimiento finaliza devolviendo como resultado el mensaje ahora redirigido.

3) En caso contrario, el procedimiento efectúa una comprobación para el error de entrega y si está presente comprueba la causa del error examinando el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega**. Si la **dirección-O/D** del destinatario no identifica un usuario-STRM, se comprueban los **indicadores-por-mensaje** en relación con el **destinatario-alternativo-autorizado**. Si el valor encontrado resulta ser **destinatario-alternativo-autorizado** y se ha configurado el ATM con la dirección de un destinatario alternativo para esta clase de destinatario, se llama entonces al redireccionamiento para dirigir el mensaje al destinatario-alternativo. Al volver satisfactoriamente del redireccionamiento, finaliza el procedimiento devolviendo entonces como resultado el mensaje redirigido.

4) La manipulación de los errores que pueden resolverse, pero que son debidos a problemas del direccionamiento constituye un asunto local, por ejemplo, el encaminamiento a otro ATM dentro del dominio debido a problemas de conversión.

5) Si el error de entrega es de otro tipo diferente de los citados anteriormente, o si el valor del **destinatario-alternativo-autorizado** es un **destinatario-alternativo-prohibido**, o si no existe ningún destinatario-alternativo-especificado-DG que resulte adecuado, el procedimiento devuelve una instrucción de informe y finaliza.

14.3.7 *Procedimiento de redireccionamiento*

Este procedimiento redirecciona un mensaje a un destinatario-alternativo.

Nota – La utilización de las facilidades de redireccionamiento deberá ajustarse a la política-seguridad en vigor.

14.3.7.1 *Argumentos*

1) El **nombre-OD** del destinatario-alternativo a quien se ha de redirigir el mensaje.
2) Los campos del mensaje por-destinatario para el destinatario que va a ser sustituido por uno alternativo.
3) El mensaje o sonda que ha de redirigirse.
4) Motivo del redireccionamiento.

14.3.7.2 *Resultados*

El mensaje o sonda suministrado en el tercer argumento con el destinatario identificado en el segundo argumento sustituido por el destinatario-alternativo especificado en el primer argumento.

14.3.7.3 *Errores*

Indicación de que se ha detectado un bucle de redireccionamiento.

14.3.7.4 *Descripción del procedimiento*

1) El procedimiento garantiza primero que el redireccionamiento al destinatario alternativo especificado no provocará un bucle de redireccionamiento. El **nombre-O/D** del destinatario-alternativo suministrado en el argumento 1 se compara con cada **nombre-destinatario-deseado** de la secuencia de la **historia-redireccionamiento** procedente de los campos por-destinatario identificados en el argumento 2. Después de una concordancia, el procedimiento finaliza indicando que se ha detectado un bucle de redireccionamiento.

2) Se añade un elemento a la **historia-redireccionamiento** (que se crea si no está presente), utilizando el **nombre-destinatario** del argumento 2 para formar el **nombre-destinatario-deseado**, obteniendo el **motivo-redireccionamiento** a partir del argumento 4 e incluyendo el instante en que se efectúa ese redireccionamiento. El **nombre-O/D** suministrado por el primer argumento se sustituye entonces por ese **nombre-destinatario**.

3) En el campo de **otras-acciones** de la **información-rastreo** vigente, el valor **redirigido** se fija en verdadero.

4) El sobre de transferencia del mensaje se actualiza de la forma siguiente:

nombre-destinatario:
sustituido

información-rastreo:
indica **redirigido**

historia-redireccionamiento:
añadir **nombre-destinatario** previo y **motivo-redireccionamiento**

destinatario-alternativo-solicitado-originador:
suprimido si y sólo si el **motivo-redireccionamiento** indica el **destinatario-alternativo-solicitado-originador**

14.3.8 *Procedimiento de división*

El divisor produce réplicas de los mensajes y de las sondas según se necesiten para un proceso ulterior. Se modifican estas réplicas según proceda, para indicar la distribución de la responsabilidad para los diferentes destinatarios procedentes del original. Cada réplica se acompaña de una instrucción por-mensaje que indica su disposición ulterior dentro del ATM.

Nota – La utilización de las facilidades del divisor deberá ajustarse a la política-seguridad en vigor.

14.3.8.1 *Argumentos*

Un mensaje o sonda. Para cada destinatario con **responsabilidad** verdadera, acompaña al mensaje una instrucción de encaminamiento/conversión.

14.3.8.2 *Resultados*

Una o más réplicas del mensaje original o de la sonda con la responsabilidad convenientemente indicada, y una instrucción por mensaje que indique la ulterior disposición de la réplica dentro del ATM.

14.3.8.3 *Errores*

Ninguno.

14.3.8.4 *Descripción del procedimiento*

El separador examina las instrucciones generadas por el procedimiento de decisión-encaminamiento-y-conversión para segregar (conceptualmente) los destinatarios con **responsabilidad** verdadera en grupos. Se crea una réplica para cada grupo. El proceso posterior para dichas réplicas (en otros procedimientos) depende de las instrucciones de conversión y encaminamiento aplicables al grupo que representa.

Nota 1 – En un ATM se necesita una réplica del módulo debido al tratamiento posiblemente diferenciador que necesitan los diferentes destinatarios de un mensaje. Estas diferencias surgen de la necesidad de más de un trayecto de retransmisión para salir de un ATM, de la necesidad de llevar a cabo más de una conversión sobre el contenido del mensaje y de la necesidad de ampliar las listas de distribución. Por ejemplo, cuando existe más de un trayecto de retransmisión, debe crearse una copia separada del mensaje para cada uno de dichos trayectos, con los valores de **responsabilidad** adecuados para los destinatarios que se encuentran a lo largo del trayecto.

Nota 2 – La determinación de cuáles son las réplicas que se necesitan es un asunto local, que se realiza de forma que se reduzca al mínimo el número total de las réplicas creadas. Los párrafos siguientes sugieren un enfoque pero no pretenden en forma alguna imponer limitaciones al método seguido en una aplicación real.

Nota 3 – Para mayor sencillez de exposición, se describe el divisor como un algoritmo de un solo-paso. Es decir, se crean todas las réplicas necesarias antes de cualquier proceso posterior. Una optimización importante consistiría en dividir de forma mínima el mensaje para conversión, y completar entonces la separación de las copias convertidas.

1) El procedimiento considera primero aquellos destinatarios para los cuales existen instrucciones de conversión de contenido. Estos destinatarios se agrupan de forma que los miembros de cada grupo estén sujetos a instrucciones de conversión idénticas. Se crea una réplica para cada grupo con **responsabilidad** verdadera para los destinatarios de este grupo y falsa para todos los demás.
2) Se examinan entonces los destinatarios para los cuales existen instrucciones de ampliación-LD. Se crea una réplica para cada destinatario de dicha LD con **responsabilidad** para todos los destinatarios excepto para la única LD que produjo la réplica.
3) Se subdividen posteriormente los grupos en base a las llamadas de instrucciones de encaminamiento por-destinatario para salida-transferencia o salida-sonda. Estos destinatarios se agrupan de forma que cada grupo comparta un destino común para el próximo salto. Se crea una réplica para cada uno de estos grupos con **responsabilidad** verdadera para los destinatarios del grupo, falsa para todos los restantes. Para todos los destinatarios de cada uno de estos grupos, éste será el primer intento de retransmisión o un intento de reencaminamiento. En el último caso, se modifica la información-rastreo para el mensaje o sonda con el fin de indicar que éste es el primer reencaminamiento o uno subsiguiente.
4) Finalmente, las instrucciones de encaminamiento para algunos destinatarios llamarán a entrega-mensaje o a generación-informe. Se crea una réplica para cada uno de estos subgrupos con **responsabilidad** verdadera para los destinatarios del grupo y falsa para todos los demás.
5) Finaliza entonces el procedimiento.

14.3.9 *Procedimiento-conversión*

Este procedimiento realiza conversiones sobre mensajes e indica aquellas conversiones que habrían sido realizadas sobre las sondas.

14.3.9.1 *Argumentos*

Un mensaje o sonda con indicación de la conversión o conversiones requeridas.

14.3.9.2 *Resultados*

El mensaje o sonda con conversiones realizadas e indicadas (sólo indicadas en el caso de una sonda).

14.3.9.3 *Errores*

El mensaje o sonda con instrucciones de informe que detallan los problemas de conversión encontrados.

14.3.9.4 *Descripción del procedimiento*

1) Para un mensaje, se realizan los procedimientos de conversión para EIT incorporados según se define en la Recomendación X.408. Los procedimientos de conversión entre los EIT definidos externamente y entre los EIT incorporados y los definidos externamente están fuera del alcance de esta Recomendación.
2) Después de la conversión, se actualiza la **información-rastreo** del mensaje o de la sonda para este dominio para mostrar los EIT convertidos. Finaliza entonces el procedimiento.

14.3.10 *Procedimiento de ampliación-lista-distribución*

Este procedimiento toma un mensaje con un único destinatario de la LD y devuelve un mensaje cuya lista de destinatarios incluye los miembros de la LD. Para una sonda, verifica si se produciría una ampliación-LD, si ésta se solicita.

Nota – La utilización de la ampliación-LD deberá estar sujeta a la política-seguridad en vigor.

14.3.10.1 *Argumentos*

1) Un mensaje con información que indique la LD de destinatarios que debe ampliarse, o
2) una sonda con información que indique la LD de destinatarios cuya ampliación ha de verificarse.

14.3.10.2 *Resultados*

1) El mensaje con cero o más destinatarios que representan los miembros de la LD. Pueden actualizarse otros campos según se indica a continuación en la descripción del procedimiento;

2) opcionalmente, el mensaje con instrucciones para generación de informe que indica una entrega con éxito, o

3) la sonda con instrucciones para generación de informe.

14.3.10.3 *Errores*

1) Una instrucción de informe que indica un fallo de entrega. Los valores para el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** son los indicados en la descripción del siguiente procedimiento.

2) En el caso de una LD recurrente, el procedimiento finaliza sin devolver ni errores ni resultados.

14.3.10.4 *Descripción del procedimiento*

1) Para un mensaje (no para una sonda), hacer la detección de recurrencia: se examinan los componentes del campo de la **historia-ampliación-LD** para detectar la aparición del nombre de un destinatario de la LD. Obsérvese que se utiliza un **nombre-O/D** distinguido de la LD para la detección de recurrencia, y que cada punto de ampliación es responsable de garantizar que sólo se coloca este **nombre O/D** en la **historia-ampliación-LD**.

   Si el nombre de los destinatarios de la LD se encuentra presente en la **historia-ampliación-LD**, se define la LD de forma recurrente y no deberá ser ampliada ulteriormente. Se descarta el mensaje y no se devuelven ni informes ni otros resultados. Finaliza el procedimiento de ampliación.

2) Adquisición de la LD: el procedimiento de ampliación intenta adquirir los atributos de la LD.

   Si no tiene éxito, el procedimiento devuelve una instrucción de informe con el **código-motivo-no-entrega** y el **código-diagnóstico-no-entrega** que procedan. Finaliza entonces el procedimiento.

3) Verificación del permiso de remisión: si se trata de un mensaje (no de una sonda), el último elemento del campo de la **historia-ampliación-LD** (si ha lugar) diferente del **nombre-originador** se considera como el emisor del mensaje. Para una sonda, el originador es el emisor del mensaje.

   El nombre del emisor se compara con los componentes del permiso-remisión-LD. Si no existe coincidencia, se devuelve una instrucción de informe con el **código-motivo-no-entrega** de **incapaz-de-transferir** y el **código-diagnóstico-no-entrega** de **no-permiso-remisión-LD**. Finaliza entonces el procedimiento.

4) Para una sonda: si ninguna otra política local impidiera una entrega deseada, se devolvería entonces una instrucción de informe para indicar la entrega con éxito. Finaliza entonces el procedimiento.

5) Para un mensaje: la bandera de **responsabilidad** de los destinatarios de la LD se pone en falso y se añaden los miembros de la LD como nuevos destinatarios del mensaje. Los campos por-destinatario para cada nuevo destinatario se copian de los del destinatario de la LD, excepto en los casos siguientes:

   – **Nombre destinatario**: miembro de la LD.

   Los siguientes campos por-destinarario se copian o cambian según la política de LD local:

   – **Ampliación-LD-prohibida**

   – **Petición-informe-ATM-que-origina** (véase la nota 1)

   – **Petición-informe-originador** (véase la nota 1)

   – **Destinatario-alternativo-solicitado-originador** (véase la nota 2)

   – **Conversión-explícita**.

   Nota 1 – Se copia sólo si la política-LD lo requiere y el originador no reciba informes no solicitados.

   Nota 2 – El **destinatario-alternativo-solicitado-originador** puede eliminarse o sustituirse, según la política de la LD local, o copiarse, pero sólo si la política de LD local lo exige explícitamente.

   Nota 3 – Cualquiera de los miembros-LD que identifican las LD que aparecen en la **historia-ampliación-LD** puede ser excluido de la ampliación de la LD y no ser incluido entre los nuevos destinatarios del mensaje.

6) En el campo de **otras-acciones** de la **información-rastreo** vigente, el valor de la **operación-LD** se pone en verdadero.

7) El valor distinguido del **nombre-O/D** de la LD (incluyendo su **dirección-O/D)** y el instante en que se ha producido la expansión se añaden al campo de **historia-ampliación-LD** del mensaje.

Nota – La utilización de un valor distinguido del **nombre-O/D** de la LD no se refiere aquí a los **nombres-guía** distinguidos sino a un **nombre-O/D** específico de la LD que el punto de ampliación eligió para fines de comparación.

8) Si los valores de la nueva petición de informe (determinados en el paso 5) o la política local de LD impiden que el originador reciba de los miembros de la LD un informe de entrega solicitado, se construye una copia del mensaje, con instrucciones de petición del informe de entrega para la LD ampliada, y se devuelve junto con el mensaje.

9) El procedimiento devuelve el mensaje revisado y la petición de informe facultativa, tras lo cual finaliza.

14.3.11 *Algoritmos de detección de bucle y de encaminamiento*

Los algoritmos de encaminamiento y de detección de bucle para su utilización entre dominios y dentro de un dominio se encuentran fuera del alcance de esta Recomendación. Para exponer los aspectos que deben considerarse, la parte restante de este punto define un método para el encaminamiento y la detección de bucle. Este texto no forma parte de la Recomendación.

Los párrafos que siguen describen un método sencillo de detección de bucle junto con un algoritmo de encaminamiento mínimo. El algoritmo es mínimo en el sentido de que presupone únicamente un conocimiento mínimo de cada DG y realiza los pasos de transferencia para evitar bucles (en el sentido que se indica a continuación). Por supuesto, este algoritmo puede mejorarse cuando un DG conoce mejor la topología de la red de los DG.

El algoritmo reconoce el hecho de que, en general, está legitimado (es decir, no deberían detectarse bucles) para entrar de nuevo en un DG si otro DG ha realizado una operación específica desde el último paso a través del DG antes de entrar de nuevo en él. Las operaciones legítimas son: conversión, ampliación-LD y redireccionamiento.

1) Notación: La secuencia de información de rastreo está constituida por **elementos-información-rastreo** designados de una forma simplificada como [DG, acción-encaminamiento, operación], donde el DG es el nombre de un DG, la acción de encaminamiento es «retransmitido» o «reencaminado», la operación es «conversión», «operación-LD», «redireccionamiento» o «nada». M designa el mensaje que hay que transferir. DG(o) designa el DG vigente (aquel que detecta en ese momento el bucle). Los vecinos representan el conjunto de los DG adyacentes seleccionados [vecinos del DG(o)] que constituyen posibles DG-retransmisores para M info-rastreo* y es el sufijo del info-rastreo obtenido al considerar la cola de la secuencia info de rastreo que comienza con el último elemento de info de rastreo [DG, r, op] donde op no es nada (nada indica que no ha sido realizada ninguna operación por ningún DG).

2) Detección de bucle: Se examina info-rastreo para los bucles. Se detecta un bucle si la secuencia de info-rastreo contiene un sufijo [DG(o), retransmitido, op(o)] ... [DG(p), retransmitido, op(p)] donde para todos los j tales que $o < j \leqslant p$ el elemento de info de rastreo asociado es [DG(j), retransmitido, op(j)] y op(j) = nada. Es decir, se detecta un bucle si M llega a un DG que lo ha retransmitido ya y después cada DG lo ha retransmitido igualmente sin realizar ninguna otra operación que no sea la de encaminamiento. Si se detecta un bucle, entonces el algoritmo devuelve un error que indica el problema y finaliza.

3) Establecimiento del encaminamiento: Si no se detecta ningún bucle, se ajusta el conjunto, vecinos, si procede, para los pasos de transferencia de evitar-bucle en el contexto del presente mensaje (el ajuste no afecta a ningún otro mensaje).

   a) Si no existe ningún bucle ni ninguna aparición de [DG(o), r, op] en info-rastreo* no se modifica de vecinos.

   b) Si no existe ningún bucle pero hay una aparición de [DG(o), r, op] en info-rastreo* se eliminan de vecinos todos los DG que aparezcan en este sufijo del info-rastreo* que comienza con [DG(o), r, op]. Se modifica el elemento de info de rastreo añadido por el dominio vigente para mostrar reencaminado como acción de reencaminar. Se añade un parámetro DG-previo determinado de la forma siguiente: se coloca el último elemento de info de rastreo [DG(o), r, op] en info de rastreo. El DG-previo es el DG que aparece en el primer elemento de info de rastreo después del último elemento de info de rastreo de [DG(o), r, op].

   c) En los casos a) y b) si vecinos está vacío, el algoritmo devuelve un error indicando el problema y finaliza.

4) Acción de reencaminamiento. Se selecciona un próximo salto desde vecinos para cada destinatario que haya de ser retransmitido.

14.4 *Módulo del informe*

El módulo del informe puede ser invocado por:

1) el módulo de entrada-informe, que transfiere un informe, o
2) el módulo principal, que transfiere un mensaje o una sonda con instrucciones de informe,
3) el módulo de salida-informe, que transfiere un informe con descripción de fallo.

Si se encuentra un error mediante los procedimientos internos de este módulo, no se genera ninguna salida. En caso contrario, el módulo de informe invoca el módulo de salida-informe o entrega-informe, que pasa un informe con instrucciones de transferencia o entrega, respectivamente. Véase la figura 10/X.411.

Nota – La utilización de los informes deberá estar sujeta a la política-seguridad en vigor.

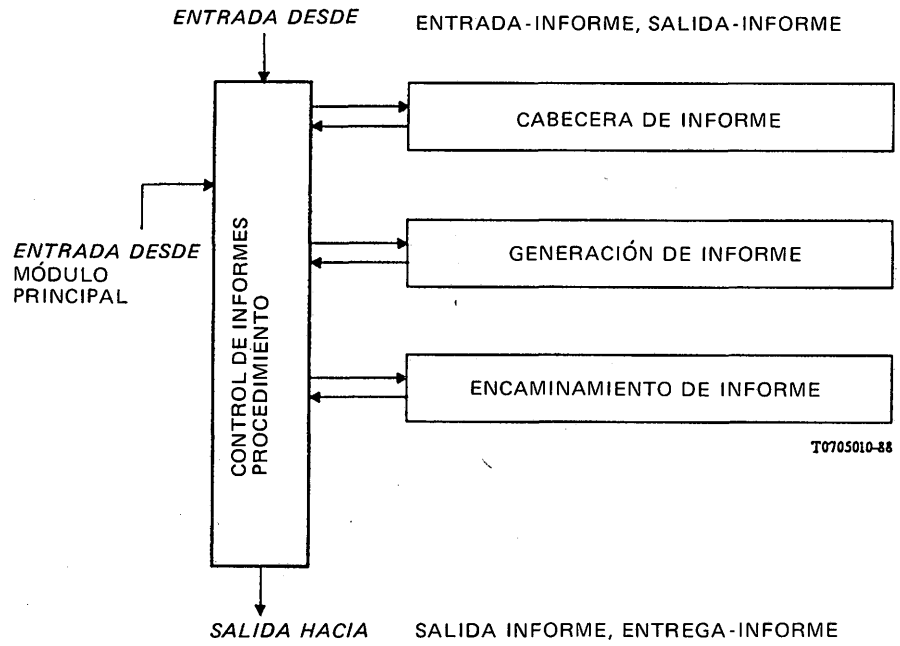


FIGURA 10/X.411

Organización de los procedimientos dentro del módulo del informe

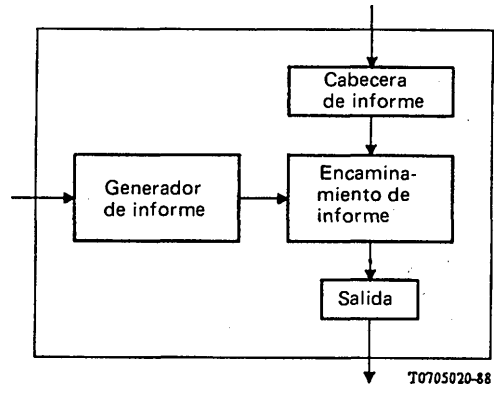


FIGURA 11/X.411

Flujo de información dentro del módulo de informe

14.4.1 *Procedimiento de control*

14.4.1.1 *Argumentos*

1) Un informe, o
2) un mensaje o sonda con instrucción de informe.

14.4.1.2 *Resultados*

1) Un informe con instrucciones de retransmisión o entrega, o
2) ningún resultado en el caso de encontrarse un error.

14.4.1.3 *Errores*

Ninguno. El informe, mensaje o sonda se descarta si se encuentra un error.

14.4.1.4 *Descripción del procedimiento*

1) Para un informe procedente de entrada-informe se llama primero al procedimiento de cabecera-informe para realizar la iniciación del rastreo y varios pasos iniciales de verificación. Una devolución nula indica un error; se descarta el informe y termina el proceso. En caso contrario, el proceso continúa en el paso 3 siguiente.
2) Para un mensaje o sonda se llama primero al procedimiento de generación-informe para crear un informe. Una devolución nula indica un error; se descarta el mensaje o la sonda y termina el proceso. Si se devuelve un informe el proceso continúa en el paso 3 siguiente.
3) Se llama al procedimiento de encaminamiento-informe para generar una instrucción de encaminamiento para el informe. Una devolución nula indica un error; se descarta el informe y termina el proceso. En el caso de una devolución positiva, se llama al procedimiento de actualización del rastreo para indicar el paso a través de este ATM. El procedimiento de control devuelve el informe finalizado junto con la instrucción de encaminamiento y termina, sujeto a la política-seguridad.

14.4.2 *Procedimiento de cabecera-informe*

Este procedimiento realiza la inicialización de traza, la detección de las violaciones de la expiración-mensaje, la comprobación inicial de seguridad, la detección de bucles y la comprobación de criticidad.

14.4.2.1 *Argumentos*

Un informe.

14.4.2.2 *Resultados*

El informe con la **información-rastreo** iniciada para este ATM.

14.4.2.3 *Errores*

Ninguno. Si se detecta un error se descarta el informe.

14.4.2.4 *Descripción del procedimiento*

1) Si el informe ha cruzado una frontera entre dominios, se añade un **elemento-información-rastreo** para este dominio con el tiempo presente como **tiempo-llegada** y **retransmisión** como **acción**. Se añade igualmente un **elemento-información-rastreo-interna** indicando si el informe ha cruzado o no una frontera de dominio.
2) Si la política-seguridad en vigor lo requiere, y/o si la **comprobación-autenticación-origen-informe** resulta incorrecta, se descarta el informe y se termina el proceso.
3) Si alguno de los campos de ampliación es marcado como crítico para la transferencia pero el ATM no lo entiende semánticamente, se descarta el informe. Finaliza entonces el procedimiento.
4) Se realiza la detección de bucles. El algoritmo de detección de bucles está fuera del alcance de esta Recomendación. Sin embargo, en el § 14.3.11 figura, como ejemplo, un algoritmo combinado de encaminamiento y de detección de bucles. Si se detecta un bucle, se descarta el informe y finaliza el procedimiento.

14.4.3 *Procedimiento de generación-informe*

Este procedimiento genera un informe que describe el éxito y/o el fallo de las operaciones deseadas por parte del ATM.

14.4.3.1 *Argumentos*

Un mensaje o sonda. Para cada destinatario con **responsabilidad** verdadera, se incluye una instrucción por-destinatario que indica el éxito o el problema encontrado.

14.4.3.2 *Resultados*

Un informe que describe los éxitos y fallos que hay que comunicar.

14.4.3.3 *Errores*

Ninguno.

14.4.3.4 *Descripción del procedimiento*

Si el campo de **petición-informe-ATM-que-origina** del sujeto así lo indica, se construye el informe con los argumentos descritos en el cuadro 31/X.411, ampliado posteriormente por lo siguiente.

Se toman los argumentos de entrega (**tiempo-entrega-diferida**, **tipo-de-usuario-STRM** o argumentos de no-entrega (**código-motivo-no-entrega**, **código-diagnóstico-no-entrega**) para cada destinatario a partir de las instrucciones pro-destinatario que acompañaban al mensaje sujeto. En el caso de un informe de entrega, el **tiempo-entrega-mensaje** se toma de la información de rastreo del mensaje o de la sonda. Si se comunica un fallo para un destinatario de una LD, el **tipo-de-usuario-STRM** se pone a **LD**. El **nombre-destinatario-informe** es el último elemento de la **historia-ampliación-LD**, si dicho elemento existe. Para mensajes sin **historia-ampliación-LD** y para todas las sondas, el **nombre-destino-informe** es el **nombre-originador** del sujeto. El **originador-y-ampliación-LD** contendrá el **nombre-originador** y el **tiempo-presentación-mensaje** del sujeto seguido del contenido de la **historia-ampliación-LD**.

Nota – No se genera el **nombre-LD-informadora** bajo ninguna de estas condiciones.

En el caso en que las instrucciones reflejen múltiples fallos, el informe debería reflejar el problema original, en vez del fallo de las acciones de recuperación subsiguientes.

Obsérvese que el ATM designa valores de **criticidad** para campos copiados del sujeto (asunto). Estos nuevos valores reflejan la criticidad con respecto al informe, no al asunto. El ATM no copiará en el informe ninguna función crítica que no admita.

14.4.4 *Procedimiento de encaminamiento-informe*

Este procedimiento determina la acción de encaminamiento, si ha lugar, que ha de adoptarse en un informe. El encaminamiento-informe refleja las condiciones especiales que requiere un procedimiento de encaminamiento diferente del aplicable a los mensajes o sondas:

1) Un informe tiene un solo destinatario – el originador del mensaje que constituye el sujeto del informe, un punto-de-ampliación de LD, o, si la política local lo permite, un propietario de LD.
2) Fallos insuperables encontrados al encaminar un informe hacen que se descarte el informe. No se hace ningún intento para generar un informe ulterior, sobre la dificultad encontrada.

Las acciones de proceso que exigen estas condiciones, se describen en los puntos siguientes. Debería observarse que el encaminamiento de los informes está sujeto a la política-seguridad.

14.4.4.1 *Argumentos*

Uno de los siguientes:

1) un informe transferido a este ATM desde otro ATM y procesado con éxito por el procedimiento de cabecera-informe;
2) un informe creado por el procedimiento generación-informe interno a este ATM;
3) un informe devuelto desde el procedimiento de salida-informe junto con una descripción del fallo de transferencia encontrado.

14.4.4.2 *Resultados*

Uno de los siguientes:

1) el informe, junto con las instrucciones de retransmisión para el ATM del próximo salto;
2) el informe, junto con una indicación del usuario-STRM soportado localmente que debe recibir la entrega-informe.

14.4.4.3 *Errores*

Ninguno. Si no puede determinarse ningún destinatario local o ningún próximo salto, se descarta el informe

14.4.4.4 *Descripción del procedimiento*

1) Los informes retransmitidos a este ATM o generados localmente reciben una atención de encaminamiento normal como se decribe a continuación.

   a) Si el destino-informe no es local en este ATM, se necesita la retransmisión. El encaminamiento-informe intenta determinar la dirección del próximo salto. En esta determinación se compara la **etiqueta-seguridad-mensaje** del informe con el **contexto-seguridad** para garantizar que no se reproducen violaciones de la política-seguridad. Si tiene éxito, se devuelve el informe, junto con esta información como resultado del procedimiento. Finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento de salida-informe.

   Si no puede determinarse la dirección del próximo salto, se descarta entonces el informe y finaliza el procedimiento sin devolver ningún resultado.

   b) Si el destino-informe es un usuario-STRM local en este ATM, y el campo de **petición-informe-originador** lo indica, se solicita la entrega-informe (sujeta a la política-seguridad en vigor). El encaminamiento-informe intenta determinar la dirección-O/D del destino del informe. Si tiene éxito, se devuelve entonces el informe, junto con esta información, como resultado del procedimiento, finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento, de entrega-informe.

   Si no se solicitó el informe o no puede determinarse la dirección de destino del informe, se descarta éste y el procedimiento finaliza sin devolver ningún resultado.

   c) Si el **nombre-destino-informe** corresponde a una LD local en este ATM, este informe se encuentra en el proceso de encaminamiento hacia atrás a lo largo de un trayecto de sucesivos puntos-ampliación de la LD. En el campo de **otras-acciones** del **elemento-información-rastreo**, el valor **operación-LD** se pone en verdadero.

   Cualquier proceso basado en una política de LD local podría producirse aquí; por ejemplo, puede construirse una copia del informe y enviarla al propietario de la LD. En este caso el **nombre-destino-informe** será el del propietario de la LD y se construirá el **nombre-LD-informadora** para que contenga el nombre de la LD del sujeto. Esta copia del informe no deberá contener el **contenido-devuelto**. Además se puede realizar aquí la supresión de los informes.

   Nota – La posibilidad de que un propietario LD sea en sí mismo una LD se deja para ulterior estudio.

   Si no se va a suprimir el informe, el ATM sustituye el **nombre O/D** existente en el campo de **nombre-destino-informe** por el **nombre O/D** que precede inmediatamente al del campo del **originador-e-historia-ampliación-LD**. De esta forma, el informe adquiere, como nuevo destino, la nueva entrada junto con la cadena de entradas del campo del **originador-e-historia-ampliación-LD**:

   Nombre-destino-informe:
   Nombre-O/D previo de la LD de la copia procedente de **originador-e-historia-ampliación-LD**.

   Nombre-LD-informadora:
   Generado únicamente en el caso de informes al propietario de la LD.

   Para encaminar el informe a su nuevo destino el procedimiento de encaminamiento-informe se llama ahora a sí mismo de forma recurrente. Se devuelve el resultado devuelto procedente de esta llamada recurrente, si lo hay y finaliza el procedimiento.

2) Un informe devuelto por el procedimiento de salida-informe ha encontrado un fallo de transferencia en el procedimiento de retransmisión a otro ATM. El procedimiento de encaminamiento-informe intenta reencaminar dicho informe, es decir, calcula una dirección alternativa para el próximo salto (sujeta a la política-seguridad en vigor). Si se encuentra una dirección alternativa para el próximo salto, se devuelve entonces el informe, junto con esta información y la información de rastreo convenientemente modificada, a modo de resultado del procedimiento. Finaliza entonces el procedimiento. A continuación se pasa el informe al procedimiento de salida-informe.

   Si no puede determinarse una dirección alternativa para el próximo salto, se descarta entonces el informe y finaliza el procedimiento sin devolver ningún resultado.

14.5 *Vinculación-STRM y desvinculación-STRM*

14.5.1 *Procedimiento de vinculación-STRM iniciado por usuario-STRM*

Este punto describe el comportamiento del ATM cuando un usuario-STRM invoca vinculación-STRM.

14.5.1.1 *Argumentos*

Los argumentos de vinculación-STRM se definen en el § 8.1.1.1.1.

14.5.1.2 *Resultados*

Los resultados de vinculación-STRM se definen en el § 8.1.1.1.2.

14.5.1.3 *Errores*

Los errores-vinculación se definen en el § 8.1.2.

14.5.1.4 *Descripción del procedimiento*

1) Si los recursos de los ATM no permiten normalmente el establecimiento de una nueva asociación, el procedimiento devuelve un error-vinculación de ocupado y finaliza.
2) En caso contrario, si la política-seguridad exige autenticación, el ATM intenta tanto autenticar el usuario-STRM a través de las **credenciales-iniciador** suministradas, como comprobar la posibilidad de aceptación del **contexto-seguridad**. Si no pueden autenticarse las **credenciales-iniciador**, el procedimiento devuelve un error-autenticación y finaliza. Si el **contexto-seguridad** no resulta aceptable, el procedimiento devuelve un error-vinculación de contexto-seguridad-inaceptable y finaliza.
3) Si la autenticación tiene éxito y el **contexto-seguridad** resulta aceptable, el ATM acepta la asociación solicitada. El procedimiento devuelve el **nombre-ATM** y las **credenciales-respondedor**. Se devuelven igualmente los **mensajes-esperando** si el usuario-STRM está abonado al elemento-de-servicio retención para entrega. Finaliza entonces el procedimiento.
4) Si no se requiere autenticación, se devuelve una espera-mensaje si el **usuario-STRM** se abona al elemento-de-servicio retención para entrega, y el procedimiento finaliza.

14.5.2 *Procedimiento de desvinculación-STRM iniciado por usuario-STRM*

Este punto describe el comportamiento del ATM cuando un usuario-STRM invoca desvinculación-STRM para liberar una asociación existente establecida por el usuario-STRM.

14.5.2.1 *Argumentos*

Ninguno.

14.5.2.2 *Resultados*

El procedimiento de desvinculación-STRM devuelve un resultado vacío como indicación de la liberación de la asociación.

14.5.2.3 *Errores*

Ninguno.

14.5.2.4 *Descripción del procedimiento*

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.5.3 *Procedimiento de vinculación-STRM iniciado por ATM*

Este punto describe los pasos dados por el ATM cuando emprende la tarea de establecer una asociación con un usuario-STRM.

14.5.3.1 *Argumentos*

Los argumentos de vinculación-STRM se definen en el § 8.1.1.1.1.

14.5.3.2 *Resultados*

Un identificador interno para la asociación establecida.

14.5.3.3 *Errores*

El procedimiento devuelve una indicación de fallo en el caso de que no pudiera establecerse la asociación.

14.5.3.4 *Descripción del procedimiento*

1) El procedimiento establece los valores para los argumentos definidos en el § 8.1.1.1.1. Pueden suministrarse **mensajes-esperando** si el usuario-STRM está abonado al elemento-de-servicio de retención para entrega. Se toman los valores del **nombre-iniciador**, **contexto-seguridad** y **credenciales-iniciador** de la información interna.
2) El procedimiento determina la **dirección-usuario** del usuario-STRM e intenta establecer una asociación con los argumentos del § 8.1.1.1.1. Si no tiene éxito, se devuelve una indicación de fallo y finaliza el procedimiento.
3) Si tiene éxito, se examinan los resultados devueltos por el usuario-STRM (definidos en el § 8.1.1.1.2). Se comprueba la corrección del **nombre-respondedor** y se realiza un intento de autenticar el usuario-STRM a través de las **credenciales-respondedor** devueltas. Si la comprobación falla, el procedimiento cierra la conexión, devuelve una indicación de fallo y finaliza.
4) Si ambas comprobaciones tienen éxito, el procedimiento devuelve el identificador de la asociación y finaliza.

14.5.4 *Procedimiento de desvinculación-STRM iniciado por el ATM*

Se llama a este procedimiento para liberar una asociación con un usuario-STRM.

14.5.4.1 *Argumentos*

El identificador interno para la asociación que ha de liberarse.

14.5.4.2 *Resultados*

El procedimiento de desvinculación-STRM devuelve un resultado vacío como indicación de la liberación de la asociación.

14.5.4.3 *Errores*

Ninguno.

14.5.4.4 *Descripción del procedimiento*

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.6 *Puerto de remisión*

14.6.1 *Procedimiento de remisión-mensaje*

Este punto describe el comportamiento del ATM cuando el usuario-STRM invoca la operación-abstracta de remisión-mensaje en un puerto de remisión.

14.6.1.1 *Argumentos*

Los argumentos de remisión-mensaje enumerados en el cuadro 3/X.411 y descritos en los puntos indicados en este cuadro.

14.6.1.2 *Resultados*

1) Los resultados de remisión-mensaje enumerados en el cuadro 5/X.411 y descritos en los puntos indicados en dicho cuadro se devuelven al usuario-STRM.
2) Se invoca el módulo de entrega diferida y se transfiere el mensaje remitido.

14.6.1.3 *Errores*

Véase el § 8.2.1.1.3 para las descripciones de los errores-abstractos pertinentes.

14.6.1.4 *Descripción del procedimiento*

1) Comprobación de errores

El procedimiento de remisión-mensaje comprueba las condiciones de error. Si se encuentra alguna, se devuelve el error-abstracto indicado y termina todo proceso ulterior. El ATM no acepta la responsabilidad del mensaje deseado.

Errores de interés especial:

a) Errores de seguridad. Si la **etiqueta-seguridad-mensaje** no es compatible con el **contexto-seguridad** o, si procede, la **comprobación-autenticación-origen-mensaje** resulta incorrecta se genera un error-seguridad.

b) Errores de criticidad. Si alguno de los campos de ampliación es marcado como **crítico-para-remisión**, pero el ATM no lo entiende semánticamente, se devuelve un error-función-crítica-no-permitida.

Si no se encuentran errores en esta etapa, continúa el proceso en el paso 2. Pueden encontrarse errores adicionales en estas últimas etapas del proceso, en cuyo caso el ATM adopta las medidas descritas anteriormente.

2) Procesamiento del nombre

El procedimiento siguiente se aplica al **nombre-originador**, al **nombre-destinatario** y al **destinatario-alternativo-solicitado-originador**, a menos que se señale lo contrario.

a) Si el **nombre-O/D** contiene únicamente un **nombre-guía**, el ATM intenta obtener la **dirección-O/D**.

En el caso del **nombre-destinatario**, el ATM puede emplear el **método-entrega-solicitada**, si está presente, como indicación de cuál sea la forma de **dirección-O/D** con la que que debe ponerse en correspondencia el **nombre-guía**. Si no es posible encontrar una forma de **dirección-O/D** apropiada para el **método-entrega-solicitado**, el ATM devuelve un error-abstracto de especificado-indebidamente-destinatario.

b) Si el **nombre-O/D** contiene tanto el **nombre-guía** como la **dirección-O/D** no es necesario dar validez a su asociación. Si se encuentra posteriormente que la **dirección-O/D** es inválida, el ATM procede como si no se hubiera suministrado la **dirección-O/D** en el **nombre-O/D**. El procedimiento descrito en el a) anterior se utiliza para obtener la **dirección-O/D**, que, caso de ser válida, sustituye a la **dirección-O/D** suministrada en el **nombre-O/D**.

Si la **dirección-O/D** obtenida es inválida se devuelve un error-abstracto como se describe en a) anterior.

c) Si un **nombre-destinatario** contiene una **dirección-O/D** de una forma no apropiada para el **método-entrega-solicitada**, si está presente, el ATM devuelve el error-abstracto **destinatario-impropiamente-especificado**.

d) La validación de la **dirección-O/D**, tanto si se pasó como argumento de la remisión-mensaje como si se obtuvo resolviendo el **nombre-guía**, consta de dos pasos. El primer paso da validez a que la **dirección-O/D** implicada tiene la combinación de atributos necesarios para ser una **dirección-O/D** válida (véase el § 8.5.5). El segundo paso, que se aplica únicamente al **nombre-originador** da validez a que la **dirección-O/D** es, de hecho, la **dirección-O/D** del usuario-STRM que remite el mensaje.

3) Transferencia de responsabilidad, devolución de resultados

Si no se detecta ningún error en el proceso anterior, el ATM acepta la responsabilidad del mensaje y así lo indica devolviendo los resultados de la remisión-mensaje al usuario-STRM. Los resultados de la remisión-mensaje se describen en el § 8.2.1.1.2. El ATM construye los argumentos del **identificador-remisión-mensaje** y del **tiempo-remisión-mensaje** según proceda. El **identificador-contenido** es idéntico al argumento correspondiente de remisión-mensaje. Si lo solicitó el originador, el ATM-que-origina genera la **prueba-de-remisión** utilizando el algoritmo identificado por **identificador-algoritmo-prueba-de-remisión** y los argumentos definidos en el § 8.2.1.1.2.4. Además se devuelve el **certificado-ATM-que-origina**.

4) Construcción del mensaje

Se construye un mensaje a partir de los argumentos de remisión-mensaje, posiblemente modificados en los pasos anteriores del proceso, más los argumentos adicionales sumnistrados por el ATM, especificados en el § 12.2.1.1.

Cuando está finalizado, el procedimiento de remisión-mensaje termina y se pasa el mensaje al módulo de entrega diferida para un proceso ulterior.

14.6.2 *Procedimiento de remisión sonda*

Este punto describe el comportamiento del ATM cuando el usuario-STRM invoca la operación-abstracta de usuario-STRM en un puerto de remisión.

14.6.2.1 *Argumentos*

Los argumentos de remisión sonda enumerados en el cuadro 7/X.411 y descritos en los puntos indicados en este cuadro.

14.6.2.2 *Resultados*

1) Los resultados de remisión-sonda enumerados en el cuadro 8/X.411 y descritos en los puntos indicados en dicho cuadro se devuelven al usuario-STRM.
2) Se invoca el módulo principal y se transfiere la sonda remitida.

14.6.2.3 *Errores*

Véase el § 8.2.1.2.3 para las descripciones de los errores-abstractos pertinentes.

14.6.2.4 *Descripción del procedimiento*

1) Comprobación de errores

   El procedimiento de remisión-sonda comprueba las condiciones de error. Si se encuentra alguna, se devuelve el error-abstracto indicado. El ATM no acepta la responsabilidad de la sonda deseada.

   Errores de interés especial:

   a) Errores de seguridad. Si la **etiqueta-seguridad-mensaje** no es compatible con el **contexto-seguridad** o si la **comprobación-autenticación-origen-sonda** resulta incorrecta se genera un error-seguridad.

   b) Errores de criticidad. Si uno de los argumentos externos resulta ser **crítico-para-remisión**, pero el ATM no lo entiende semánticamente, se devuelve un error-función-crítica-no-permitida.

   Si no se encuentran errores en esta etapa, continúa el proceso en el paso 2. Pueden encontrarse errores adicionales en estas últimas etapas del proceso, en cuyo caso el ATM adopta las medidas descritas anteriormente.

2) Procesamiento del nombre

   Se aplica el procedimiento siguiente al **nombre-originador**, **nombre-destinatario** y **destinatario-alternativo-solicitado-originador**, a menos que se señale lo contrario.

   a) Si el **nombre-O/D** contiene únicamente un **nombre-guía**, el ATM intenta obtener la **dirección-O/D**.

      En el caso del **nombre-destinatario**, el ATM puede utilizar el **método-entrega-solicitado**, de haberlo, para indicar con que forma de **dirección-O/D**, ha de hacerse corresponder el **nombre-guía**. Si no puede encontrarse una forma de **dirección-O/D** apropiada para el **método-entrega-solicitado**, el ATM devuelve un error-abstracto de destinatario-especificado-indebidamente.

   b) Si el **nombre-O/D** contiene tanto el **nombre guía** como la **dirección-O/D**, no es necesario dar validez a su asociación. Si se encuentra posteriormente que la **dirección-O/D** es inválida, el ATM procede como si no se hubiera suministrado la **dirección-O/D** en el **nombre-O/D**. El procedimiento descrito en el punto a) anterior se utiliza para obtener la **dirección-O/D**, que, en caso de ser válida, sustituye a la **dirección-O/D** suministrada en el **nombre-O/D**.

      Si la **dirección-O/D** obtenida es inválida, se devuelve un error-abstracto como se describe en el punto a) anterior.

   c) Si un **nombre-destinatario** contiene una **dirección-O/D** que sea de una forma inapropiada para el **método-entrega-solicitado**, de haberlo, el ATM devuelve el error-abstracto-destinatario-especificado-impropiamente.

   d) La validación de la **dirección-O/D**, tanto si se transfirió como argumento de remisión-sonda, como si se obtuvo resolviendo el **nombre-guía**, consta de dos pasos. El primer paso da validez a que la **dirección-O/D** implicada tiene la combinación de atributos necesarios para ser una **dirección-O/D** válida (véase el § 8.5.5). El segundo paso, que se aplica únicamente al **nombre originador**, da validez a que la **dirección-O/D** es, de hecho, la **dirección-O/D** del usuario-STRM que remite el mensaje.

3) Transferencia de responsabilidad, devolución de resultados

   Si no se detecta ningún error en los pasos anteriores, el ATM acepta la responsabilidad del mensaje y así lo indica devolviendo los resultados de remisión-sonda al usuario-STRM. Los resultados de remisión-sonda se describen en el § 8.2.1.2.2. El ATM construye los argumentos de **identificador-remisión-sonda** y del **tiempo-remisión-sonda** según convenga. El **identificador-contenido** es idéntico al argumento correspondiente a remisión-sonda.

4) Construcción de la sonda

Se construye una sonda a partir de los argumentos de remisión-sonda, posiblemente modificados en los pasos anteriores del proceso, más los argumentos adicionales suministrados por el ATM.

Cuando está finalizado, el procedimiento de remisión-sonda termina y se pasa la sonda al módulo principal para un proceso ulterior.

14.6.3 *Procedimiento de cancelación-entrega-diferida*

Este punto describe el comportamiento del ATM cuando el usuario-STRM invoca la operación-abstracta de cancelación-entrega-diferida en un puerto de remisión para cancelar la entrega diferida de un mensaje previamente remitido al ATM.

14.6.3.1 *Argumentos*

Los argumentos de cancelación-entrega-diferida enumerados en el cuadro 10/X.411 y descritos en los puntos indicados en este cuadro.

14.6.3.2 *Resultados*

Como indicación de cancelación satisfactoria, se transfiere al usuario-STRM un resultado vacío.

14.6.3.3 *Errores*

Véase el § 8.2.1.3.3 para las descripciones de los errores-abstractos pertinentes.

14.6.3.4 *Descripción del procedimiento*

1) Si ya ha sido proporcionada una **prueba-de-remisión**, el ATM devuelve el error abstracto de demasiado-tarde-para-cancelar. No se cancela la entrega del mensaje.
2) Si el ATM reconoce el argumento del **identificador-remisión-mensaje** como válido y asociado con un mensaje que está reteniendo el ATM para su entrega-diferida, el ATM descarta este mensaje como cancelado y supone que ya no tiene ninguna responsabilidad sobre él.
3) Si el ATM reconoce el argumento del **identificador-remisión-mensaje** como válido pero referido a un mensaje ya entregado a otro ATM, el ATM invoca el error-abstracto demasiado-tarde-para-cancelar. No se cancela la entrega diferida del mensaje.
4) Si no se reconoce como válido el argumento del **identificador-remisión-mensaje** (porque el ATM nunca asignó dicho valor o porque el ATM ya no tiene depositado el registro histórico de un mensaje de entrega diferida que ha sido transferido o entregado) el ATM devuelve entonces el error-abstracto de identificador-remisión-mensaje-inválido o demasiado-tarde-para-cancelar, siendo la elección un asunto local.

14.6.4 *Procedimiento control-remisión*

Este punto describe el comportamiento del ATM al invocar la operación-abstracta de control-remisión en un puerto-remisión, para limitar transitoriamente las operaciones-abstractas del puerto-remisión que puede invocar el usuario-STRM. Estos controles permanecen en vigor durante la asociación presente, a menos que sean anulados por una operación-abstracta del control-remisión.

Nota – La utilización de control-remisión deberá estar sujeta a la política-seguridad en vigor. El argumento de control-remisión de **contexto-seguridad-permisible** limita el **contexto-seguridad** establecido durante la vinculación-STRM.

14.6.4.1 *Argumentos*

Los argumentos de control-remisión enumerados en el cuadro 12/X.411 y descritos en los puntos indicados en este cuadro.

14.6.4.2 *Resultados*

El usuario-STRM devuelve al ATM los resultados de control-remisión enumerados en el cuadro 13/X.411 y descritos en los puntos indicados en este cuadro.

14.6.4.3 *Errores*

El usuario-STRM puede devolver un error-seguridad. Véase el § 8.2.1.4.3 para la descripción de este error-abstracto.

14.6.4.4 *Descripción del procedimiento*

Las circunstancias que hacen que un ATM invoque la operación-abstracta de control-remisión son asunto local, como lo son las medidas adoptadas durante y después de su consecución.

14.7 *Puerto de entrega*

14.7.1 *Procedimiento de entrega-mensaje*

Este punto describe los pasos dados por un ATM cuando se encarga de entregar un mensaje a uno o más usuarios-STRM.

La mayoría de las disposiciones de este punto se aplicarán igualmente al caso en que el ATM haya recibido una sonda con uno o más destinatarios locales. A menos que se señale lo contrario, todos los pasos del procedimiento, excepto la entrega física, se aplican al manejo de las sondas.

Nota – La generación de informes estará sujeta a la política-seguridad.

14.7.1.1 *Argumentos*

1) Un mensaje desde el módulo principal con instrucciones por-destinatatrio para entregar a uno o más usuarios-STRM locales.
2) Los argumentos de entrega-mensaje enumerados en el cuadro 15/X.411 y descritos en los puntos indicados en este cuadro se pasan al usuario-STRM destinatario.

14.7.1.2 *Resultados*

1) Un resultado vacío o, si se solicita, una **prueba-de-entrega** y, opcionalmente, un **certificado-destinatario** devuelto por el usuario-STRM como indicación de una entrega con éxito sin requisitos de información.
2) Si se requiere un informe, se invoca el módulo principal y se pasa el mensaje con instrucciones por-destinatario describiendo los problemas de entrega encontrados y/o indicando las entregas con éxito sobre las que hay que informar.

14.7.1.3 *Errores*

Los errores-abstractos de entrega-mensaje que pueden ser devueltos por el usuario-STRM al ATM se describen en el § 8.3.1.1.3. Estas condiciones de error se comunican al módulo principal en los resultados descritos anteriormente.

14.7.1.4 *Descripción del procedimiento*

1) Si se alcanza la expiración del mensaje, se genera una instrucción de informe para cada destinatario local. Los valores de **código-motivo-no-entrega** y **código-diagnóstico-no-entrega** son respectivamente **incapaz-de-transferir** y **máximo-tiempo-expirado**. Finaliza entonces el procedimiento.
2) Si cualquiera de los **campos-ampliación** por-mensaje se pone en **crítico-para-entrega** pero el ATM no lo entiende semánticamente, se genera una instrucción de informe por cada destinatario local. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen en **incapaz-de-transferir** y **función-crítica-no-permitida** respectivamente.
3) En caso contrario, se establecen los valores para aquellos argumentos de la operación-abstracta entrega-mensaje que se aplican a todos los destinatarios (los argumentos de entrega-mensaje se describen en el § 8.3.1.1.1).
4) Para cada destinatario con **responsabilidad** verdadera se ejecutan los pasos 4-15. Finaliza entonces el procedimiento.
5) Para garantizar que durante la entrega, no se viola la política-seguridad, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si la política-seguridad impide la entrega entonces, con sujeción a la política de seguridad, se genera una instrucción de informe para ese destinatario. Los valores de **código-motivo-no-entrega** y **código-diagnóstico-no-entrega** son **incapaz-de-transferir** y **error-mensajería-segura**, respectivamente.

6) Si las restricciones impuestas por una operación-abstracta de registro o de control-entrega impiden la entrega, el ATM entonces, sujeto a la política-seguridad en vigor, retendrá el mensaje hasta que se levanten la restricción o las restricciones aplicables.

7) Si expira el máximo tiempo de retención para un mensaje retenido (siendo el valor máximo de este tiempo un asunto local) con las restricciones aplicables todavía en vigor, se genera una instrucción de informe para este destinatario. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen respectivamente en **incapaz-de-transferir** y **destinatario-indisponible**. Termina entonces el proceso para este destinatario.

Nota – Los pasos de proceso (5 y 6 anteriores) asociados con las restricciones de control no se aplican en el caso de las sondas.

8) Si se hace cumplir la entrega restringida, y el destinatario está en la categoría de remitente no autorizado, entonces se genera una instrucción de informe para ese destinatario. Se fija **código-motivo-no-entrega** en el valor **entrega-restringida**. En ese momento, termina el procesamiento para ese destinatario.

9) El ATM establece los argumentos de la operación-abstracta de entrega-mensaje que se aplican únicamente al destinatario individual: los valores **identificador-entrega-mensaje** y **tiempo-entrega-mensaje** se describen en los § 8.3.1.1.1.1 y 8.3.1.1.1.2. Todos los restantes argumentos se toman directamente de los campos correspondientes del mensaje a entregar. Con las excepciones indicadas a continuación, todos los argumentos indicados en el cuadro 11/X.411 se incluyen en cada invocación de entrega-mensaje.

10) Si **revelación-de-destinatarios** tiene el valor **revelación-de-destinatarios-autorizada**, el ATM incluye en el argumento de **nombre-otro-destinatario** todos los destinatarios, que estén especificados por el originador, excepto el presente.

Obsérvese que si el destinatario es un miembro de una lista de distribución, en el argumento de **nombre-otro-destinatario** no deben incluirse otros miembros de esta lista de distribución. El destinatario es un miembro de la lista de distribución si el campo de **historia-ampliación-LD** es no-vacío.

11) Si alguno de los **campos-ampliación** por-destinatario se pone en **crítico-para-entrega**, pero el ATM no lo entiende semánticamente, se genera una instrucción de informe para este destinatario. Los valores de **código-motivo-no-entrega** y de **código-diagnóstico-no-entrega** se ponen respectivamente en **incapaz-de-transferir** y **función-crítica-no-permitida**.

12) En el caso de entrega de una unidad de acceso de entrega física, los argumentos de entrega física se incluyen en la entrega-mensaje. Estos argumentos se describen en los § 8.2.1.1.1.14 a 8.2.1.1.1.23.

13) Una vez satisfechas todas las condiciones para una entrega con éxito, el ATM entregará físicamente el mensaje. La consecución de la entrega a un usuario-STRM destinatario coubicado es un asunto local. En el caso de un usuario-STRM destinatario distante, el ATM establece una asociación con este usuario-STRM (o utiliza uno existente) e invoca la operación-abstracta de entrega-mensaje a través de esta asociación. Al realizar una entrega con éxito, la responsabilidad distante o local del mensaje pasa del ATM al usuario-STRM destinatario.

14) Al realizar una entrega con éxito, si la **petición-informe-entrega-ATM-que-origina** tiene el valor de **informe** o de **informe auditado**, se genera una instrucción de informe señalando la entrega con éxito. Se termina el proceso para este destinatario.

15) En el caso de un usuario-STRM destinatario distante, si no existe o no puede establecerse inicialmente una asociación o si existe un fallo de transferencia a través de la asociación, el ATM puede repetir el intento de establecimiento de asociación y/o transferir, siendo el número máximo y/o la duración de las repeticiones un asunto local. Si, después de repetidas tentativas no se ha conseguido la transferencia, el mensaje es considerado como inentregable y, se genera una instrucción de informe, sujeta a la política-seguridad en vigor. Los valores del **código-motivo-no-entrega** y del **código-diagnóstico-no-entrega** son respectivamente **fallo-transferencia** y **destinatario-indisponible**. Termina entonces el proceso para este destinatario.

Nota – Los pasos del proceso asociados con la transferencia física de un mensaje al usuario-STRM destinatario no se aplican en el caso de la sonda.

16) Devolución de los resultados y errores por el usuario-STRM

Si la operación-abstracta de entrega-mensaje tiene éxito, el usuario-STRM devuelve como indicación de éxito o bien un resultado vacío o bien, si se solicitase, una **prueba-de-entrega** y un certificado-destinatario-facultativo.

Si la operación-abstracta de entrega-mensaje viola uno o más de los controles impuestos por la operación-abstracta de control-entrega o de registro, el usuario-STRM devuelve un error de control-entrega-violado. Si el **contexto-seguridad** dicta que el usuario-STRM no puede admitir la operación-abstracta solicitada porque violaría la política-seguridad, el usuario-STRM devuelve entonces un error-seguridad. En este caso, la invocación de la entrega-mensaje ha fracasado y el ATM conserva la responsabilidad del mensaje respecto de este destinatario. El mensaje es retenido para hacer un reintento a continuación, o es enviado al módulo principal para la generación de un informe. Termina entonces el proceso para este destinatario.

14.7.2 *Procedimiento de prueba-entrega-sonda*

Este punto describe los pasos dados por un ATM cuando emprende la tarea de comprobar la posibilidad de entregar una sonda.

Nota – La utilización de informes estará sujeta a la política-seguridad.

14.7.2.1 *Argumentos*

1) Sonda del procedimiento interno con instrucciones por-destinatario para la prueba-entrega-sonda a uno a más usuarios STRM locales.

14.7.2.2 *Resultados*

Se invoca el módulo principal y se transfiere la sonda con instrucciones por destinatario que describen si habría ocurrido o no la entrega ficticia, y si no, por qué motivo.

14.7.2.3 *Errores*

Ninguno.

14.7.2.4 *Descripción de procedimiento*

En el § 14.7.1 se describe la lógica de la entrega-mensaje. Se ejecutan todos los pasos de este punto, excepto aquellos indicados específicamente como no aplicables a la sonda.

14.7.3 *Procedimiento de entrega-informe*

Este punto describe los pasos dados por un ATM cuando se encarga de entregar un informe al usuario-STRM. Se llama a la entrega-informe cuando un ATM recibe un informe, procedente de la entrada-informe o al generarse dentro del ATM, cuyo campo de **nombre originador** especifica un usuario-STRM servido por este ATM.

14.7.3.1 *Argumentos*

1) Un informe del módulo de informe con instrucciones por-destinatario para entregarlas a un destinatario local.
2) Los argumentos de entrega-informe enumerados en el cuadro 18/X.411 y descritos en los puntos indicados en dicho cuadro se tranfieren al usuario-STRM destinatario.

14.7.3.2 *Resultados*

Un resultado vacío devuelto por el usuario-STRM como indicación de una entrega con éxito.

14.7.3.3 *Errores*

Los errores de entrega-informe que pueden devolver el usuario-STRM al TM se describen en el § 8.3.1.2.3.

14.7.3.4 *Descripción del procedimiento*

1) Para garantizar que no se viola la política-seguridad durante la entrega-informe, se comprueba la **etiqueta-seguridad-mensaje** respecto del contexto-seguridad. Si la entrega-informe está prohibida por la política-seguridad, se descarta el informe.
2) Si las restricciones impuestas por una operación-abstracta de registro o control-entrega invocada previamente prohiben la entrega-informe, el ATM retendrá, sujeto a la política-seguridad en vigor, el informe hasta que cesen la restricción o las restricciones aplicables. Los argumentos de la operación-abstracta de control-entrega o de registro establecen las restricciones según se describe en el § 8.3.1.3.1.

   Si expira el máximo tiempo de retención para un informe retenido (siendo el valor máximo de este tiempo un asunto local) con las restricciones aplicables todavía en vigor, se descarta el informe.
3) Los argumentos para la operación-abstracta de entrega-informe se toman de los correspondientes campos del informe.
4) Si cualquiera de los **campos-ampliación** por-mensaje o por-destinatario se pone en **crítico-para-entrega**, pero no es entendido semánticamente por el ATM, se descarta el informe.

5) La consecución de la entrega-informe a un usuario-STRM coubicado es un asunto local. En el caso de un usuario-STRM distante, el ATM establece una asociación con dicho usuario-STRM (o utiliza uno existente) e invoca la operación-abstracta de entrega-informe a través de la asociación. Al tener éxito una entrega-informe, la responsabilidad distante o local del informe pasa del ATM al usuario-STRM.

6) En el caso de un usuario-STRM distante, si no puede establecerse inicialmente una asociación, el ATM puede repetir la tentativa, siendo el número máximo y la duración de las repeticiones un asunto local. Si, después de varias tentativas no se ha establecido la asociación, el informe se considera inentregable y se descarta.

7) Devolución de resultados y errores por el usuario-STRM.

   Si la operación-abstracta de entrega-informe tiene éxito, el usuario-STRM devuelve un resultado vacío como indicación del éxito.

   Si la operación-abstracta de entrega-informe viola uno o más controles impuestos por una operación-abstracta de control-entrega o de registro, el usuario-STRM devuelve un error de control-entrega-violado. En este caso, la invocación de entrega-informe ha fracasado y el ATM conserva la responsabilidad del informe.

14.7.4 *Procedimiento de control-entrega*

Este apartado describe el comportamiento del ATM cuando un usuario-STRM servido por dicho ATM invoca la operación-abstracta de control-entrega. Esta última impone y levanta restricciones sobre las operaciones-abstractas de entrega-mensaje y entrega-informe. Estos controles permanecen vigentes durante la presente asociación, a menos que sean anulados por un control-entrega subsiguientes. Los controles-entrega limitan de forma transitoria el **contexto-seguridad**, pero no pueden provocar ninguna violación de la política-seguridad.

Estos controles no se aplican al tratamiento de las sondas por el ATM.

14.7.4.1 *Argumentos*

Los argumentos de control-entrega enumerados en el cuadro 20/X.411 y descritos en el § 8.3.1.3.1.

14.7.4.2 *Resultados*

1) Los resultados del control-entrega enumerados en el cuadro 21/X.411 que se describen en el § 8.3.1.3.2, son devueltos por el ATM al usuario-STRM.

2) Varios parámetros de control de usuario-STRM retenidos por este ATM se sustituyen por valores transportados en los argumentos de control-entrega.

14.7.4.3 *Errores*

Véase el § 8.3.1.3.3 para una descripción de los errores-abstractos pertinentes.

14.7.4.4 *Descripción del procedimiento*

1) Si el valor del argumento **restricción** es **eliminación**, todos los controles establecidos por cualquier control-entrega previo se eliminan; la operación-abstracta está terminada y se devuelve el resultado al usuario-STRM.

2) Si el valor del argumento **restricción** es **actualización**, y no existe ningún otro argumento presente, se considera válida la petición y se devuelve el resultado al usuario-STRM.

   En dichos casos todos los valores de control vigentes en ese momento permanecen sin modificación.

3) Si el valor del argumento **restricción** es **actualización**, y están presentes otros argumentos, se comprueba la compatibilidad de estos argumentos con las condiciones a largo plazo especificadas por la invocación más reciente de la operación-abstracta de restricción en el puerto-administración (véase el § 14.4.1). Si no se detecta ninguna incompatibilidad y está permitida la actualización dentro de la política-seguridad, se llevan a cabo las actualizaciones indicadas, la operación-abstracta finaliza y se devuelve el resultado al usuario-STRM.

4) Si se detecta alguna de las siguientes incompatibilidades con condiciones a largo plazo, el ATM devuelve un error-abstracto de control-viola-registro:

a) **Tipos-información-codificada-admisibles** tiene un tipo no especificado entre los permitidos a largo plazo.

b) **Tipos-contenido-admisibles** tiene un contenido no especificado entre los permitidos a largo plazo.

c) La **longitud-máxima-contenido-admisible** excede la longitud aurorizada a largo plazo.

d) Se viola el **contexto-seguridad-admisible**.

En cualquiera de estos casos de error, se descarta el control-entrega y no se lleva a cabo.

14.8 *Puerto de administración*

14.8.1 *Procedimiento de registro*

Este punto describe el comportamiento del ATM cuando un usuario-STRM servido por este ATM invoca la operación-abstracta de registro.

14.8.1.1 *Argumentos*

Los argumentos de registro enumerados en el cuadro 23/X.411 y descritos en los puntos indicados en dicho cuadro.

14.8.1.2 *Resultados*

1) El procedimiento de registro devuelve un resultado vacío al usuario-STRM como indicación de éxito.

2) Varios parámetros del usuario-STRM retenidos por el ATM se sustituyen por valores transportados en los argumentos de registro.

14.8.1.3 *Errores*

Un error rechazado-registro devuelto al usuario-STRM, como se describe en el § 8.4.1.1.3.

14.8.1.4 *Descripción del procedimiento*

1) Se comprueba la correcta especificación de los argumentos de registro. Si alguno está incorrectamente especificado, el procedimiento de registro devuelve un error rechazado-registro y finaliza.

2) Si los argumentos de registro están correctamente especificados, los valores de los parámetros del usuario-STRM se sustituyen por los argumentos de registro, y finaliza el procedimiento.

14.8.2 *Procedimiento de cambio-de-credenciales iniciado por el usuario-STRM*

Este punto describe el comportamiento del ATM cuando el usuario-STRM invoca la operación-abstracta de cambio-de-credenciales.

Nota – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

14.8.2.1 *Argumentos*

Los argumentos de cambio-de-credenciales enumerados en el cuadro 25/X.411 y descritos en el § 8.4.1.2.1.

14.8.2.2 *Resultados*

1) El procedimiento de cambio-de-credenciales devuelve un resultado vacío al usuario-STRM como indicación de éxito.

2) Las credenciales del usuario-STRM retenidas por el ATM se modifican de acuerdo con el argumento de **nuevas credenciales**.

14.8.2.3 *Errores*

El error-abstracto de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, descrito en el § 8.4.1.2.3 y enumerado en el cuadro 26/X.411.

14.8.2.4 *Descripción del procedimiento*

Nota – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

1) Si el valor del argumento de **antiguas-credenciales** no es el mismo que el de las credenciales retenidas por el ATM para el usuario-STRM que invoca la operación-abstracta, se devuelve al usuario-STRM un error de antiguas-credenciales-incorrectamente-especificadas y finaliza el procedimiento de cambio-de-credenciales.
2) En caso contrario, se comprueba la validez del argumento de **nuevas-credenciales**. Si se encuentra que es inválido (asunto local dictado por la política-seguridad) se devuelve al usuario-STRM un error de nuevas-credenciales-inaceptables y finaliza el procedimiento de cambio-de-credenciales.
3) En caso contrario, las credenciales del usuario-STRM retenidas por este ATM se sustituyen por el valor del argumento de las **nuevas-credenciales**, se devuelve un resultado vacío al usuario-STRM como indicación de éxito y finaliza el procedimiento de cambio-de-credenciales.

14.8.3 *Procedimiento de cambio-de-credenciales iniciado por el ATM*

Este punto describe el comportamiento del ATM al cambiar sus credenciales retenidas por un usuario-STRM soportado localmente.

Nota – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

14.8.3.1 *Argumentos*

Los argumentos de cambio-de-credenciales enumerados en el cuadro 25/X.411 y descrito en el § 8.4.1.2.1.

14.8.3.2 *Resultados*

El usuario-STRM devuelve un resultado vacío al procedimiento de cambio-de-credenciales como indicación de éxito.

14.8.3.3 *Errores*

El usuario-STRM puede devolver un error de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, según se describe en el § 8.4.1.2.3 y se enumera en el cuadro 26/X.411.

14.8.3.4 *Descripción del procedimiento*

Nota – Todos los cambios de credenciales estarán sujetos a la política-seguridad en vigor.

1) El procedimiento invoca la operación-abstracta de cambio-de-credenciales para cambiar las credenciales del ATM retenidas por un usuario-STRM soportado-localmente. Las condiciones que hacen que un ATM cambie sus credenciales constituyen un asunto local.
2) Si se recibe del usuario-STRM el error de nuevas-credenciales-inaceptables o antiguas-credenciales-incorrectamente-especificadas, el ATM debe suponer que sus credenciales no han cambiado. A nivel local se puede emprender una actuación ulterior, después de la cual finaliza el procedimiento.
3) Si se recibe la devolución de un resultado vacío procedente del usuario-STRM, el ATM puede suponer que el procedimiento ha tenido éxito y que sus credenciales han cambiado. El procedimiento termina.

14.9 *Vinculación-ATM y desvinculación-ATM*

14.9.1 *Procedimiento de entrada-vinculación-ATM*

Este punto describe el comportamiento del ATM cuando otro ATM invoca vinculación-ATM.

14.9.1.1 *Argumentos*

Los argumentos de vinculación-ATM se definen en el § 12.1.1.1.1 y se enumeran en el cuadro 27/X.411.

14.9.1.2 *Resultados*

Los resultados de vinculación-ATM se definen en el § 12.1.1.1.2 y se enumeran en el cuadro 28/X.411.

14.9.1.3 *Errores*

Los errores vinculación se definen en el § 12.1.2.

14.9.1.4 *Descripción del procedimiento*

1) Si los recursos de los ATM no permiten normalmente el establecimiento de una nueva asociación, el procedimiento devuelve un error-vinculación de ocupado y finaliza.
2) En caso contrario, si la política-seguridad exige la autenticación, el ATM intenta tanto autenticar el ATM llamante a través de las **credenciales-iniciador** suministradas como comprobar la posibilidad de aceptación del **contexto-seguridad**. Si no pueden autenticarse las **credenciales-iniciador**, el procedimiento devuelve un error-autenticación y finaliza. Si el **contexto-seguridad** no resulta aceptable, el procedimiento devuelve un error de contexto-seguridad-inaceptable y finaliza.
3) Si la autenticación es satisfactoria y el **contexto-seguridad** resulta aceptable, el ATM establece la asociación solicitada. El procedimiento devuelve el **nombre-ATM** y las **credenciales-respondedor**. Finaliza entonces el procedimiento.
4) Si no se requiere autenticación, no hay resultados que devolver y el procedimiento finaliza.

14.9.2 *Procedimiento de entrada-desvinculación-ATM iniciado por usuario-STRM*

Este punto describe el comportamiento del ATM cuando otro ATM invoca desvinculación-ATM para liberar una asociación existente establecida por el usuario-STRM.

14.9.2.1 *Argumentos*

Ninguno.

14.9.2.2 *Resultados*

El procedimiento de entrada-desvinculación-ATM devuelve un resultado vacío como indicación de la liberación de la asociación.

14.9.2.3 *Errores*

Ninguno.

14.9.2.4 *Descripción del procedimiento*

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.9.3 *Procedimiento de salida-vinculación-ATM*

Este punto describe los pasos dados por el ATM cuando emprende la tarea de establecer una asociación con otro ATM.

14.9.3.1 *Argumentos*

1) El **nombre-ATM** del ATM con quién se ha establecido la asociación.
2) El **contexto-seguridad** para la asociación.

14.9.3.2 *Resultados*

Un identificador interno para la asociación establecida.

14.9.3.3 *Errores*

El procedimiento devuelve una indicación de fallo en caso de no poderse establecer la asociación.

14.9.3.4 *Descripción del procedimiento*

1) El procedimiento establece los valores para los argumentos definidos en el § 12.1.1.1.1. Se toman los valores de **nombre-iniciador**, **contexto-seguridad** y **credenciales-iniciador** de la información interna.
2) El procedimiento determina la dirección del ATM e intenta establecer una asociación con los argumentos del § 12.1.1.1.1. Si no tiene éxito, se devuelve una indicación de fallo y finaliza el procedimiento.

3) Si tiene éxito, se examinan los resultados devueltos por el ATM llamado (definido en el § 12.1.1.1.2). Se comprueba la corrección del **nombre-respondedor** y se realiza un intento de autenticar el ATM a través de las **credenciales-respondedor** devueltas. Si alguna de las comprobaciones falla, el procedimiento cierra la conexión, devuelve una indicación de fallo y finaliza.
4) Si ambas comprobaciones tienen éxito, el procedimiento devuelve el identificador de la asociación y finaliza.

14.9.4 *Procedimiento de salida-desvinculación-ATM*

Se llama a este procedimiento para liberar una asociación con otro ATM.

14.9.4.1 *Argumentos*

El identificador interno de la asociación que ha de liberarse.

14.9.4.2 *Resultados*

El procedimiento de salida-desvinculación-ATM devuelve un resultado vacío como indicación de la liberación de la asociación.

14.9.4.3 *Errores*

Ninguno.

14.9.4.4 *Descripción del procedimiento*

El procedimiento libera la asociación, devuelve un resultado vacío y finaliza.

14.10 *Puerto de transferencia*

Nota – Las medidas adoptadas en el puerto-transferencia están sujetas a la política-seguridad en vigor.

14.10.1 *Procedimiento de entrada-mensaje*

Este punto describe el comportamiento del ATM cuando el otro ATM invoca la operación-abstracta de transferencia-mensaje en un puerto de transferencia.

14.10.1.1 *Argumentos*

Los argumentos de transferencia-mensaje enumerados en el cuadro 29/X.411 y descritos en los puntos indicados en este cuadro.

14.10.1.2 *Resultados*

1) Se invoca el módulo entrega-diferida y se pasa el mensaje transferido.

14.10.1.3 *Errores*

Ninguno.

14.10.1.4 *Descripción del procedimiento*

Al recibir un mensaje, mediante la consecución de una operación-abstracta de transferencia-mensaje (invocada desde un ATM vecino), se invoca el procedimiento de entrada-mensaje. Este procedimiento transfiere simplemente el mensaje al módulo entrega-diferida para determinar las acciones que debe emprender este ATM.

La responsabilidad sobre el mensaje pasa al ATM-receptor con la transferencia efectuada satisfactoriamente.

14.10.2 *Procedimiento de entrada-sonda*

Este punto describe el comportamiento del ATM cuando otro ATM invoca la operación-abstracta de transferencia-sonda en un puerto-transferencia.

14.10.2.1 *Argumentos*

Los argumentos de transferencia-sonda enumerados en el cuadro 30/X.411 y descritos en los puntos indicados en dicho cuadro.

14.10.2.2 *Resultados*

1) Se invoca el módulo principal y se pasa la sonda transferida.

14.10.2.3 *Errores*

Ninguno.

14.10.2.4 *Descripción del procedimiento*

Al recibir una sonda mediante la aparición de una operación-abstracta de transferencia-sonda (invocada desde un ATM vecino), se invoca el procedimiento de entrada-sonda. Este procedimiento simplemente pasa la sonda al módulo principal para determinar las acciones que debe emprender este ATM.

La responsabilidad de la sonda pasa al ATM receptor si la transferencia se realizó con éxito.

14.10.3 *Procedimiento de entrada-informe*

Este punto describe el comportamiento del ATM al recibir un informe en una puerta-transferencia mediante la aparición de una operación-abstracta de transferencia-informe invocada por otro ATM o al recibir una indicación para la generación de un informe procedente de una unidad de acceso tal como una UAEF.

14.10.3.1 *Argumentos*

Los argumentos de informe enumerados en el cuadro 31/X.411 y descritos en los puntos indicados en este cuadro.

14.10.3.2 *Resultados*

1) Se invoca el módulo informe y se pasa el informe transferido.

14.10.3.3 *Errores*

Ninguno.

14.10.3.4 *Descripción del procedimiento*

Al recibir una sonda mediante la aparición de una operación-abstracta de transferencia-sonda (invocada desde un ATM vecino), o al recibir una indicación para una generación de un informe procedente de una unidad de acceso tal como una UAEF, se invoca el procedimiento de entrada-informe. Este procedimiento simplemente transfiere el informe al módulo informe para determinar las acciones que debe emprender este ATM.

La responsabilidad de la sonda pasa al ATM receptor si la transferencia se realizó satisfactoriamente.

14.10.4 *Procedimiento de salida-mensaje*

Este punto describe los pasos dados por un ATM cuando éste se encarga de transferir un mensaje a otro ATM.

14.10.4.1 *Argumentos*

Un mensaje del procedimiento interno con instrucciones de encaminamiento para transferir a otro ATM. Los campos de este mensaje forman los argumentos de la operación-abstracta de transferencia-mensaje enumerados en el cuadro 29/X.411.

14.10.4.2 *Resultados*

Ninguno.

14.10.4.3 *Errores*

En el caso de un fallo de transferencia se invoca el módulo-principal y se pasa el mensaje con una instrucción por-mensaje que indica el motivo del fallo.

14.10.4.4 *Descripción del procedimiento*

El mensaje que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-mensaje. Debe observarse que el mensaje puede reflejar el proceso (por ejemplo, conversión de contenido, redireccionamiento, ampliación de la lista de distribución) llevado a cabo en este o en anteriores ATM.

1) Para garantizar que no se viola la política-seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohibe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.

2) En caso contrario, el ATM establece una asociación con el ATM-receptor (o utiliza uno existente) e invoca la operación-abstracta de transferencia-mensaje a través de esta asociación. La consecución de la salida-mensaje indica que la transferencia ha tenido éxito y que el ATM-receptor acepta ahora la responsabilidad del mensaje. Finaliza ahora el procedimiento de salida-mensaje.

   Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el ATM puede repetir el intento de establecimiento de asociación y/o transferencia, siendo el máximo número y/o la duración de las repeticiones un asunto local.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, se considera el mensaje como no transferible y se devuelve, con el motivo del fallo indicado, al módulo principal para un posible reencaminamiento o redireccionamiento. La responsabilidad del mensaje permanece en el ATM emisor. Termina entonces el procedimiento de salida-mensaje.

14.10.5 *Procedimiento de salida-sonda*

Este punto describe los pasos dados por un ATM cuando éste se encarga de transferir una sonda a otro ATM.

14.10.5.1 *Argumentos*

Una sonda del procedimiento interno con instrucciones de encaminamiento para transferir a otro ATM. Los campos de esta sonda forman los argumentos de la operación-abstracta de transferencia-sonda enumerados en el cuadro 30/X.411.

14.10.5.2 *Resultados*

Ninguno.

14.10.5.3 *Errores*

En el caso de un fallo de transferencia se invoca el módulo principal y se transfiere la sonda con una instrucción por-mensaje que indica el motivo del fallo.

14.10.5.4 *Descripción del procedimiento*

La sonda que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-sonda. Debe observarse que la sonda puede reflejar el proceso (por ejemplo, redireccionamiento) llevado a cabo en este o en anteriores ATM.

1) Para garantizar que no se viola la política de seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohibe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.

2) El ATM establece una asociación con el ATM receptor (o utiliza uno existente) e invoca la operación-abstracta de transferencia-sonda a través de esta asociación. La consecución de la salida-mensaje indica que la transferencia ha tenido éxito y que el ATM-receptor acepta ahora la responsabilidad de la sonda. Finaliza ahora el procedimiento de salida-sonda.

   Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el ATM puede repetir la tentativa de establecimiento de asociación y/o transferencia, siendo el máximo número y/o duración de las repeticiones un asunto local.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, se considera la sonda como no transferible y se devuelve, con el motivo del fallo indicado, al módulo principal para un posible reencaminamiento o redireccionamiento. La responsabilidad del mensaje permanece en el ATM emisor. Termina entonces el procedimiento de salida-sonda.

14.10.6 *Procedimiento de salida-informe*

Este punto describe los pasos dados por un ATM cuando se enfrenta con la transferencia de un informe a otro ATM.

14.10.6.1 *Argumentos*

Un informe del procedimiento interno con instrucciones de encaminamiento para transferir a otro ATM. Los campos de este informe forman los argumentos de la operación-abstracta de transferencia-informe enumerados en el cuadro 31/X.411.

14.10.5.2 *Resultados*

Ninguno.

14.10.6.3 *Errores*

El informe, junto con el motivo del fallo de transferencia se devuelven al módulo informe.

14.10.6.4 *Descripción del procedimiento*

El informe que hay que transferir proporciona los argumentos de la operación-abstracta de transferencia-informe. Debe observarse que el informe puede reflejar el proceso (por ejemplo, redireccionamiento) llevado a cabo en este o en anteriores ATM.

1) Para garantizar que no se viola la política de seguridad durante la transferencia, se compara la **etiqueta-seguridad-mensaje** con el **contexto-seguridad**. Si se prohibe la transferencia debido a la política-seguridad o a restricciones transitorias, el proceso continúa en el paso 3 siguiente.

2) El ATM establece una asociación con el ATM-receptor (o utiliza uno existente) e invoca la operación-abstracta de transferencia-informe a través de esta asociación. La consecución de la salida-informe indica que la transferencia ha tenido éxito y que el ATM-receptor acepta ahora la responsabilidad del informe. Finaliza ahora el procedimiento de salida-informe.

   Si no existe una asociación o no puede establecerse inicialmente, o existe un fallo de transferencia a través de la asociación, el ATM puede repetir la tentativa de establecimiento de asociación y/o transferencia, siendo el máximo número y/o la duración de las repeticiones un asunto local.

3) Si después de repetidos intentos no se ha logrado la transferencia, o se ha detectado en el paso 1 una violación de seguridad, se considera el informe como no transferible y se devuelve, con el motivo del fallo indicado, al módulo informe para un posible reencaminamiento o redireccionamiento. La responsabilidad del informe permanece en el ATM emisor. Termina entonces el procedimiento de salida-informe.

ANEXO A

(a la Recomendación X.411)

Definición de referencia de los identificadores de objetos del STRM

Este anexo define como referencia varios identificadores de objetos citados en los módulos NSA.1 en el texto de esta Recomendación. Los identificadores de objetos se asignan en la figura A-1/X.411.

Todos los identificadores de objetos que asigna esta Recomendación se indican en este anexo. El anexo es definitivo para todos, excepto para los módulos NSA.1 y el propio sistema de transferencia de mensajes. Las asignaciones definitivas para los primeros se producen en los propios módulos; en las cláusulas IMPORTAR aparecen otras referencias a ellas. Esas cláusulas están fijadas.

```
MTSObjectIdentifiers { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) object-identifiers(0) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

-- Prólogo
-- Exporta todo


IMPORTS -- nada --;


-- Sistema de transferencia de mensajes

id-mts OBJECT IDENTIFIER ::= { joint-iso-ccitt mhs-motis(6) mts(3) }      -- no definitivo


-- Categorías de identificadores de objeto

id-mod OBJECT IDENTIFIER ::= { id-mts 0 }          -- módulos
id-ot OBJECT IDENTIFIER ::= { id-mts 1 }           -- tipos de objeto
id-pt OBJECT IDENTIFIER ::= { id-mts 2 }           -- tipos de puerta
id-cont OBJECT IDENTIFIER ::= { id-mts 3 }         -- tipos de contenido
id-eit OBJECT IDENTIFIER ::= { id-mts 4 }          -- tipos de información codificada
id-att OBJECT IDENTIFIER ::= { id-mts 5 }          -- atributos
id-tok OBJECT IDENTIFIER ::= { id-mts 6 }          -- tipos de distintivo
id-sa OBJECT IDENTIFIER ::= { id-mts 7 }           -- tipos de agentes seguros


-- Módulos

id-mod-object-identifiers OBJECT IDENTIFIER ::= { id-mod 0 }          -- no definitivo
id-mod-mts-abstract-service OBJECT IDENTIFIER ::= { id-mod 1 }        -- no definitivo
id-mod-mta-abstract-service OBJECT IDENTIFIER ::= { id-mod 2 }        -- no definitivo
```

FIGURA A-1/X.411 (parte 1 de 3)

Definición de la sintaxis abstracta de los identificadores de objetos del STRM

```
id-mod-upper-bounds OBJECT IDENTIFIER ::= { id-mod 3 }          -- no definitivo

-- Tipos de objeto
id-ot-mts OBJECT IDENTIFIER ::= { id-ot 0 }
id-ot-mts-user OBJECT IDENTIFIER ::= { id-ot 1 }
id-ot-mta OBJECT IDENTIFIER ::= { id-ot 2 }

-- Tipos de puerto
id-pt-submission OBJECT IDENTIFIER ::= { id-pt 0 }
id-pt-delivery OBJECT IDENTIFIER ::= { id-pt 1 }
id-pt-administration OBJECT IDENTIFIER ::= { id-pt 2 }
id-pt-transfer OBJECT IDENTIFIER ::= { id-pt 3 }

-- Tipos de contenido
id-cont-undefined OBJECT IDENTIFIER ::= { id-cont 0 }
id-cont-inner-envelope OBJECT IDENTIFIER ::= { id-cont 1 }

-- Tipos de información codificada
id-eit-undefined OBJECT IDENTIFIER ::= { id-eit 0 }
id-eit-telex OBJECT IDENTIFIER ::= { id-eit 1 }
id-eit-ia5-text OBJECT IDENTIFIER ::= { id-eit 2 }
id-eit-g3-facsimile OBJECT IDENTIFIER ::= { id-eit 3 }
id-eit-g4-class-1 OBJECT IDENTIFIER ::= { id-eit 4 }
id-eit-teletex OBJECT IDENTIFIER ::= { id-eit 5 }
id-eit-videotex OBJECT IDENTIFIER ::= { id-eit 6 }
```

FIGURA A-1/X.411 (parte 2 de 3)

Definición de la sintaxis abstracta de los identificadores de objetos del STRM

```
id-eit-voice OBJECT IDENTIFIER ::= { id-eit 7 }

id-eit-sfd OBJECT IDENTIFIER ::= { id-eit 8 }

id-eit-mixed-mode OBJECT IDENTIFIER ::= { id-eit 9 }


-- Atributos

id-att-physicalRendition-basic OBJECT IDENTIFIER ::= { id-att 0 }


-- Tipos de testigos

id-tok-asymmetricToken OBJECT IDENTIFIER ::= { id-tok 0 }


-- Tipos de agentes seguros

id-sa-ua OBJECT IDENTIFIER ::= { id-sa 0 }

id-sa-ms OBJECT IDENTIFIER ::= { id-sa 1 }


END  -- of MTSObjectIdentifiers
```

FIGURA A-1/X.411 (parte 3 de 3)

Definición de la sintaxis abstracta de los identificadores de objetos del STRM

ANEXO B

(a la Recomendación X.411)

Definición de referencia de los límites superiores de los parámetros del STRM

Este anexo define como referencia los límites superiores de varios tipos de datos de longitud variable, cuyas sintaxis abstractas se definen en los módulos NSA.1 del texto de esta Recomendación. Los límites superiores se definen en la figura B-1/X.411.

```
MTSUpperBounds { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) upper-bounds(3) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


-- Prólogo
-- Exporta todo


IMPORTS -- nothing --;


-- Límites superiores

ub-integer-options INTEGER ::= 256

ub-queue-size INTEGER ::= 2147483647                    -- el mayor entero en 32 bits

ub-content-length INTEGER ::= 2147483647                -- el mayor entero en 32 bits

ub-password-length INTEGER ::= 62

ub-bit-options INTEGER ::= 16

ub-content-types INTEGER ::= 1024

ub-tsap-id-length INTEGER ::= 16

ub-recipients INTEGER ::= 32767

ub-content-id-length INTEGER ::= 16

ub-x121-address-length INTEGER ::= 15

ub-mts-user-types INTEGER ::= 256

ub-reason-codes INTEGER ::= 32767

ub-diagnostic-codes INTEGER ::= 32767

ub-supplementary-info-length INTEGER ::= 256

ub-extension-types INTEGER ::= 256
```

FIGURA B-1/X.411 (parte 1 de 3)

Definiciones de la sintaxis abstracta de los límites superiores del STRM

```
ub-recipient-number-for-advice-length INTEGER ::= 32

ub-content-correlator-length INTEGER ::= 512

ub-redirections INTEGER ::= 512

ub-dl-expansions INTEGER ::= 512

ub-built-in-content-type INTEGER ::= 32767

ub-local-id-length INTEGER ::= 32

ub-mta-name-length INTEGER ::= 32

ub-country-name-numeric-length INTEGER ::= 3

ub-country-name-alpha-length INTEGER ::= 2

ub-domain-name-length INTEGER ::= 16

ub-terminal-id-length INTEGER ::= 24

ub-organization-name-length INTEGER ::= 64

ub-numeric-user-id-length INTEGER ::= 32

ub-surname-length INTEGER ::= 40

ub-given-name-length INTEGER ::= 16

ub-initials-length INTEGER ::= 5

ub-generation-qualifier-length INTEGER ::= 3

ub-organizational-units INTEGER ::= 4

ub-organizational-unit-name-length INTEGER ::= 32

ub-domain-defined-attributes INTEGER ::= 4

ub-domain-defined-attribute-type-length INTEGER ::= 8

ub-domain-defined-attribute-value-length INTEGER ::= 128
```

FIGURA B-1/X.411 (parte 2 de 3)

Definiciones de la sintaxis abstracta de los límites superiores del STRM

```
ub-extension-attributes INTEGER ::= 256

ub-common-name-length INTEGER ::= 64

ub-pds-name-length INTEGER ::= 16

ub-postal-code-length INTEGER ::= 16

ub-pds-parameter-length INTEGER ::= 30

ub-physical-address-lines INTEGER ::= 6

ub-unformatted-address-length INTEGER ::= 180

ub-e163-4-number-length INTEGER ::= 15

ub-e163-4-sub-address-length INTEGER ::= 40

ub-built-in-encoded-information-types INTEGER ::= 32

ub-teletex-private-use-length INTEGER ::= 128

ub-encoded-information-types INTEGER ::= 1024

ub-security-labels INTEGER ::= 256

ub-labels-and-redirections INTEGER ::= 256

ub-security-problems INTEGER ::= 256

ub-privacy-mark-length INTEGER ::= 128

ub-security-categories INTEGER ::= 64

ub-transfers INTEGER ::= 512

ub-bilateral-info INTEGER ::= 1024

ub-additional-info INTEGER ::= 1024


END -- of MTSUpperBounds
```

FIGURA B-1/X.411 (parte 3 de 3)

Definiciones de la sintaxis abstracta de los límites superiores del STRM

ANEXO C

(a la Recomendación X.411)

Diferencias entre la Norma ISO/CEI y la Recomendación del CCITT

En este anexo se identifican las diferencias técnicas entre la Recomendación X.411 del CCITT y la Norma ISO/CEI 10021-4.

Estas diferencias son:

1) En la Recomendación X.411 los campos de ampliación se identifican mediante enteros. La publicación ISO/CEI 10021-4 permite además la utilización de identificadores de objeto para ampliaciones dentro de los DGPR y/o entre ellos.
2) En la Recomendación X.411 se establecen limitaciones de tamaño a un cierto número de campos de protocolo (véase el anexo B). En la publicación ISO/CEI 10021-4, los valores reales de las limitaciones no forman parte de la Norma.

Recomendación X.413

SISTEMAS DE TRATAMIENTO DE MENSAJES: DEFINICIÓN DEL SERVICIO ABSTRACTO DE ALMACENAMIENTO DE MENSAJES[1)]

(Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y de servicios de mensajes con almacenamiento y retransmisión basados en computador, y asociados a redes públicas de datos, ha creado la necesidad de elaborar normas para facilitar el intercambio de mensajes en el plano internacional entre los abonados a esos servicios.

El CCITT,

considerando

(a) la necesidad de servicios de tratamiento de mensajes;

(b) la necesidad de transferir y almacenar mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT;

(e) que las Recomendaciones de la serie X.500 especifican servicios y sistemas de guía;

(f) que los servicios y sistemas de tratamiento de mensajes se especifican en la serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419;

(g) que la mensajería interpersonal se especifica en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

(1) que la definición del servicio abstracto de almacenamiento de mensajes sea la especificada en la sección 2;

(2) que los tipos de atributos generales y los tipos de acciones automáticas generales sean las especificadas en la sección 3;

(3) que los procedimientos para el almacenamiento de mensajes y la realización de puertos sean los especificados en la sección 4.

ÍNDICE

SECCIÓN 1 – *Introducción*

0 Introducción

1 Campo de aplicación

2 Referencias

3 Definiciones

4 Abreviaturas

5 Convenios

[1)] La Recomendación X.413 y la Norma ISO 10021-5 [Information processing systems – Text Communication – MOTIS – Message Store: Abstract-service definition] fueron preparadas en estrecha colaboración y están técnicamente armonizadas, salvo en lo que respecta a las diferencias indicadas en el apéndice G.

SECCIÓN 2 – *Definición del servicio abstracto de almacenamiento de mensajes*

6 Modelo de almacenamiento de mensajes

7 Operaciones abstractas de vinculación y de desvinculación

8 Operaciones abstractas

9 Errores abstractos

SECCIÓN 3 – *Tipos de atributos generales y tipos de acciones automáticas generales*

10 Visión de conjunto

11 Tipos de atributos generales

12 Tipos de acciones automáticas generales

SECCIÓN 4 – *Procedimiento para almacenamiento de mensajes y realización de puertos*

13 Visión de conjunto

14 Consumo del servicio abstracto de sistema de transferencia de mensajes

15 Suministro del servicio abstracto de almacenamiento de mensajes

16 Realización de puertos

Anexo A – Asignación formal de identificadores de objeto

Anexo B – Definición formal del servicio abstracto de almacenamiento de mensajes

Anexo C – Definición formal de tipos de atributos generales

Anexo D – Definición formal de tipos de acciones automáticas generales

Anexo E – Definición formal de límites superiores de parámetros AM

Anexo F – Ejemplos de la operación abstracta resumir

Anexo G – Diferencias entre el texto de la Recomendación X.413 del CCITT y el texto de la Norma ISO/CEI 10021-5

SECCIÓN 1 – INTRODUCCIÓN

0 Introducción

Esta Recomendación forma parte de una serie de Recomendaciones que definen el tratamiento de mensajes (TM) en un entorno de sistemas abiertos distribuidos.

El tratamiento de mensajes proporciona el intercambio de mensajes entre usuarios en base al almacenamiento y retransmisión. El mensaje depositado por un usuario (el originador) es transferido a través del sistema de transferencia de mensajes (STRM) y entregado a uno o varios usuarios (los destinatarios).

Esta Recomendación define el servicio abstracto de almacenamiento de mensajes (servicio abstracto AM) que permite la extracción de mensajes de un dispositivo de almacenamiento de mensajes (AM) y el depósito indirecto de mensajes a través del AM en un sistema de tratamiento de mensajes (STM). El servicio abstracto AM proporciona también servicios de administración de mensajes, definidos por el servicio abstracto de sistema de transferencia de mensajes (STRM).

Esta Recomendación ha sido elaborada sobre la base de un acuerdo tomado conjuntamente entre el CCITT y la ISO. La correspondiente Norma Internacional es ISO 10021-5. El anexo G indica las diferencias entre los dos documentos.

1 Campo de aplicación

Esta Recomendación define el servicio abstracto de almacenamiento de mensajes. Este servicio abstracto se presta mediante el protocolo de acceso a la memoria de mensajes especificado en la Recomendación X.419 en combinación con el servicio abstracto STRM definido en la Recomendación X.411, junto con los servicios del elemento de servicio de operaciones a distancia (ESOD) definidos en la Recomendación X.219. La notación de sintaxis abstracta para los protocolos de la capa de aplicación utilizados en esta Recomendación se define en la Recomendación X.208.

Otras Recomendaciones definen otros aspectos del STM. La Recomendación X.400 define los servicios destinados a los usuarios, proporcionados por el STM. La Recomendación X.402 presenta una visión arquitectural del STM. La Recomendación X.407 da una descripción de los convenios de definición de servicio abstracto utilizados en STM. La Recomendación X.420 define el servicio abstracto para la mensajería interpersonal y define el formato de los mensajes interpersonales.

La sección 2 de esta Recomendación contiene la definición del servicio abstracto de almacenamiento de mensajes. El § 6 describe el modelo AN. El § 7 especifica la notación de sintaxis abstracta para las operaciones abstractas de vinculación y desvinculación. El § 8 especifica la notación de sintaxis abstracta para las operaciones del servicio abstracto. El § 9 especifica la notación de sintaxis abstracta para los errores del servicio abstracto.

La sección 3 de esta Recomendación define los tipos de atributos generales y los tipos de acciones automáticas generales relacionados con el AM. El § 10 presenta una visión de conjunto. El § 11 especifica la notación de sintaxis abstracta para los tipos de atributos generales. El § 12 especifica la notación de sintaxis abstracta para los tipos de acciones automáticas generales.

La sección 4 de esta Recomendación describe los procedimientos para el almacenamiento de mensajes y la realización de puertos. El § 13 presenta una visión de conjunto. El § 14 describe la manera de suministrar el servicio abstracto de almacenamiento de mensajes. El § 15 describe la manera de consumir el servicio abstracto de sistema de transferencia de mensajes. El § 16 describe la manera de realizar los puertos del AM.

No se establecen requisitos para la conformidad con esta Recomendación.

2 Referencias

Para la lista de referencias, véase la Recomendación X.402.

3 Definiciones

3.1 *Definiciones de términos usuales en STM*

En la Recomendación X.402 figura una lista de términos usuales en el STM, con sus definiciones.

3.2 *Definiciones de términos relativos al almacenamiento de mensajes*

Para los fines de esta Recomendación se aplican las siguientes definiciones:

3.2.1 **asociación abstracta:** Vinculación abstracta entre dos participantes en una comunicación, en esta Recomendación la vinculación entre un AU y un AM para la prestación del servicio abstracto AM, o entre un AM y un ATM para la prestación del servicio abstracto STRM.

3.2.2 **parámetros-vinculación-abstracta:** Parámetros definidos en este documento y que están contenidos en la operación abstracta de vinculación.

3.2.3 **parámetros-desvinculación-abstracta:** Parámetros definidos en este documento y que están contenidos en la operación abstracta de desvinculación.

3.2.4 **puerto de administración:** Puerto que ofrece el conjunto de servicios abstractos (para STRM) de administración dentro del servicio AM abstracto.

3.2.5 **operación abstracta de alerta:** Operación abstracta que permite al AM señalar, sobre la base de criterios de selección, el AU, que hay mensajes o informes en espera en el AM. Sólo puede tener lugar sobre una asociación abstracta existente.

3.2.6 **atributo:** Información de un tipo particular que aparece en una inscripción en una base de información.

3.2.7 **tipo de atributo:** Componente de un atributo que indica la clase de información dada por éste.

3.2.8 **valor de atributo:** Caso particular de la clase de información indicada por un tipo de atributo.

3.2.9 **aserción-valor-de atributo:** Proposición relativa a los valores de atributos en una inscripción que puede ser verdadera, falsa o indefinida.

3.2.10 **acción automática:** Acciones que pueden ser realizadas automáticamente por el AM y que se basan en una información previamente registrada, aportada por el propietario del AM a través del AU.

3.2.11 **tipo de acción automática:** Se utiliza un tipo de acción automática para indicar el tipo de acción automática, por ejemplo Alerta.

3.2.12 **alerta automática:** Acción automática dentro del AM que da lugar a una operación abstracta de alerta o a otra acción por el AM.

3.2.13 **retransmisión automática:** Acción automática dentro del AM que provoca la retransmisión automática de un mensaje a otro destinatario (o a otros destinatarios) por el AM.

3.2.14 **inscripción-vástago:** Inscripción que no es la inscripción principal en una base de información. La inscripción progenitora de una inscripción vástago puede ser la inscripción principal, u otra inscripción vástago, lo que dependerá del número de niveles de las inscripciones en cada caso.

3.2.15 **número secuencial de vástago:** Número secuencial en una inscripción progenitora que apunta a una inscripción vástago. Una inscripcón progenitora puede tener más de un valor del número secuencial de vástago, lo que depende del número de inscripciones vástago.

3.2.16 **componente condicional (C):** Elemento NSA.1 que estará presente en un caso de su clase como prescribe esta Recomendación. Véase **grado**.

3.2.17 **longitud del contenido:** Atributo que da la longitud del contenido de un mensaje entregado (o contenido devuelto).

3.2.18 **contenido devuelto:** Atributo que señala que un informe entregado (o un mensaje entregado) contenía un contenido devuelto.

3.2.19 **TIC convertidos:** Atributo que identifica los tipos de información codificada del contenido del mensaje después de la conversión.

3.2.20 **hora de creación:** Atributo que da la hora de creación (por la MM) de un asiento.

3.2.21 **operación abstracta de supresión:** Operación abstracta utilizada para suprimir inscripciones una o más inscripciones en una base de información.

3.2.22 **TIC entregados:** Atributo con múltiples valores que da información sobre los TIC en un mensaje entregado.

3.2.23 **inscripción de mensaje entregado:** Inscripción en la base de información de mensajes almacenados que se obtiene a partir de un mensaje entregado.

3.2.24 **inscripción por informe entregado:** Inscripción en la base de información de mensajes almacenados que se obtiene a partir de un mensaje entregado.

3.2.25 **inscripción:** Conjunto de informaciones en una base de información. Véase inscripción principal, inscripción progenitora e inscripción vástago para una ulterior clasificación de las inscripciones.

3.2.26 **información-asiento:** Parámetro, utilizado en operaciones abstractas, que transporta información seleccionada desde una inscripción.

3.2.27 **selección-información-inscripción:** Parámetro, utilizado en operaciones abstractas, que indica la información de un asiento que se está solicitando.

3.2.28 **estado-inscripción:** Atributo que da información sobre el estado de procesamiento de esa inscripción. Los valores posibles son: nuevo, listado o procesado.

3.2.29 **tipo-inscripción:** Atributo que señala si una inscripción está asociada con un mensaje entregado o con un informe entregado.

3.2.30 **operación-abstracta de captura:** Operación abstracta que permite recuperar una inscripción de la base de información de mensajes almacenados.

3.2.31 **restricciones a captura:** Restricciones impuestas por el AU a la clase de mensaje que él está preparado para recibir como resultado de la operación. Las restricciones posibles son la longitud del mensaje, los tipos de contenido y los TIC.

3.2.32 **filtro:** Parámetro utilizado en operaciones abstractas para probar una determinada inscripción en una base de información y que es satisfecho o no satisfecho por esa inscripción.

3.2.33 **elemento del filtro:** Aserción sobre la presencia de uno o más valores de un atributo de un determinado tipo en una inscripción sometida a prueba. Cada aserción es verdadera o falsa.

3.2.34 **petición de retransmisión:** Parámetro que puede estar presente en una operación abstracta de depósito de mensajes, invocada por el AU, para solicitar la retransmisión de un mensaje desde el AM.

3.2.35 **atributo general:** Conjunto de atributos del AM que son válidos para todos los tipos de mensajes e informes, independientemente del contenido. Sólo estos atributos del AM están explícitamente definidos en esta Recomendacón.

3.2.36 **acción automática general:** Acciones automáticas que son válidas para todos los tipos de mensajes e informes, independientemente del contenido. Sólo estas acciones automáticas están explícitamente definidas en esta Recomendación.

3.2.37 **Grado:** Definido en la Recomendación X.402.

3.2.38 **puerto de depósito indirecto:** Puerto que ofrece el servicio abstracto de depósito indirecto dentro del servicio abstracto AM. El servicio abstracto de depósito indirecto ofrece los mismos servicios que el servicio abstracto de depósito de mensajes (del servicio abstracto STRM) con la funcionalidad adicional de retransmitir mensajes residentes en el AM.

3.2.39 **base de información:** Objetos dentro del AM que almacenan información relativa al servicio abstracto AM, por ejemplo la base de información de mensajes almacenados, que almacéna los mensajes e informes que han sido entregados al AM.

3.2.40 **tipo de base de información:** Tipo de la base de la información, por ejemplo mensajes almacenados.

3.2.41 **límite:** Componente en el parámetro selector que define el número máximo de inscripciones seleccionadas que han de devolverse como resultado de una operación abstracta.

3.2.42 **operación abstracta de listar:** Operación abstracta que permite devolver, con relación a ciertas inscripciones, una selección de esas inscripciones, así como la información de atributo solicitada.

3.2.43 **listado:** Valor del estado de la inscripción.

3.2.44 **Macro:** Véase la Recomendación X.208.

3.2.45 **inscripción principal:** Para cada operación abstracta correcta que crea inscripción en una base de información hay siempre una inscripción principal. Una información ulterior, o más detallada, obtenida como resultado de la misma operación abstracta, puede almacenarse en inscripciones vástagos.

3.2.46 **componente obligatorio (O):** Elemento NSA.1 que debe estar siempre presente en un caso de su clase. Véase **grado.**

3.2.47 **concordancia:** Proceso de comparar el valor suministrado en una aserción de valor de atributo con el valor del tipo de atributo indicado, almacenado en el AM, o de decidir si el tipo de atributo indicado está o no presente.

3.2.48 **elemento de servicio de extracción de mensaje (ESRM):** Elemento del servicio de aplicación por medio del cual un AU efectúa la extracción de mensajes de un AM, o cualquiera de las diversas tareas conexas.

3.2.49 **MM:** Memoria de mensajes utilizado también como forma abreviada para «proveedor del servicio abstracto AM».

3.2.50 **servicio abstracto AM:** Conjunto de capacidades que ofrece el AM a sus usuarios por medio de sus puertos.

3.2.51 **usuario del servicio abstracto AM:** Consumidor del servicio abstracto AM. Este es el AU.

3.2.52 **proveedor del servicio abstracto AM:** AM que proporciona el servicio abstracto AM.

3.2.53 **usuario AM:** Forma abreviada para «usuario del servicio abstracto AM».

3.2.54 **operación abstracta de depósito de mensajes:** Operación abstracta que permite al AU depositar un mensaje en el STRM a través del AM y/o retransmitir un mensaje del AM al STRM.

3.2.55 **atributo de múltiples valores:** Atributo que puede tener asociados varios valores.

3.2.56 **nuevo:** Valor del estado de la inscripción.

3.2.57 **componente facultativo (F):** Elemento NSA.1 que debe estar presente en un caso de su clase a discreción del objeto (por ejemplo, el usuario) que suministra ese caso. Véase **grado.**

3.2.58 **TIC originales:** Atributo que identifica los tipos de información codificada originales del contenido del mensaje.

3.2.59 **contraorden:** Componente del parámetro selector que indica que las restricciones previamente registradas para esta operación abstracta no deben aplicarse a este caso de operación abstracta.

3.2.60 **inscripción progenitora:** Una inscripción progenitora tiene una o más inscripciones vástagos, que fueron creadas como resultado de la misma operación abstracta. Si una inscripción progenitora no es una inscripción vástago de ninguna otra inscripción progenitora, es una inscripción principal.

3.2.61 **número secuencial de progenitor:** Un número secuencial es una inscripción vástago que apunta a su inscripción progenitora. En una inscripción vástago sólo puede haber un número secuencial de progenitor.

3.2.62 **petición de atributo parcial:** Componente de la selección de información de asiento que permite que sean devueltos solamente los valores seleccionados de un atributo de múltiples valores.

3.2.63 **posición:** Las posiciones son parámetros utilizados para especificar una cota de una gama.

3.2.64 **procesado:** Valor del estado de la inscripción.

3.2.65 **gama:** Parámetro utilizado en operaciones abstractas, para seleccionar una secuencia contigua de inscripciones en una base de información.

3.2.66 **operación abstracta registro-AM:** Operación abstracta que permite al AU registrar en el AM cierta información relativa al interfuncionamiento AU-AM.

3.2.67 **registro:** Información que es registrada en el AM y almacenada (hasta que es cambiada por una operación abstracta de registro-AM entre asociaciones abstractas. (Véase registro-AM).

3.2.68 **identificador de registro:** Identificador de un conjunto particular de parámetros para un tipo de acción automática.

3.2.69 **puerto de recuperación:** Puerto que ofrece el conjunto de servicios abstractos de extracción dentro del servicio abstracto AM.

3.2.70 **inscripción de contenido devuelto:** Tipo de inscripción, en la base de información de mensajes almacenados, que contiene el contenido devuelto de un mensaje depositado anteriormente.

3.2.71 **selector:** Parámetro utilizado en operaciones abstractas, para seleccionar entradas a partir de una base de información.

3.2.72 **número secuencial:** Atributo que identifica de manera única una inscripción. Los números secuenciales son asignados en orden ascendente.

3.2.73 **atributo univaluado:** Atributo que sólo puede tener asociado un valor.

3.2.74 **intervalo:** Componente en el resultado de la operación abstracta resumir que contiene los números secuenciales más alto y más bajo de las inscripciones que concuerdan con los criterios de selección.

3.2.75 **mensajes almacenados:** La base de información más importante en esta Recomendación, utilizada para almacenar inscripciones que contienen mensajes e informes entregados por el STRM al AM.

3.2.76 **abono:** Acuerdo a largo plazo entre el suministrador o administrador del AM y los clientes del AM (propietarios del AM) sobre la disponibilidad y uso de prestaciones AM opcionales tales como servicios y atributos opcionales. Esta Recomendación presupone que se ha proporcionado tal mecanismo, pero no prescribe ni ofrece un método normalizado sobre la forma de proporcionarlo.

3.2.77 **subcadena:** Elemento de filtro utilizado para especificar una cadena de caracteres que aparece (en el mismo orden dado) en un valor de un atributo.

3.2.78 **operación abstracta de resumir:** Operación abstracta que permite obtener una rápida visión de conjunto de la clase y el número de las inscripciones que están almacenadas en ese momento en una base de información.

3.2.79 **sinopsis:** Atributo específico al contenido que puede utilizarse para describir la forma en que las inscripciones vástagos, que contienen partes del contenido, están relacionadas entre sí y con la inscripción principal. Este atributo tiene que estar especificado en la Recomendación que describe el tipo de contenido; por ejemplo, véase sinopsis de MIP, definida en la Recomendación X.420.

4 Abreviaturas

En la Recomendación X.402 figura una lista de abreviaturas.

5 Convenios

Esta Recomendación utiliza los convenios de descripción enumerados en los cuatro puntos siguientes.

5.1 *Convenios de descripción de los servicios abstractos*

Esta Recomendación utiliza los siguientes convenios de descripción, basados en la NSA.1, para los fines indicados:

1) La propia NSA.1, para especificar la sintaxis abstracta de bases de información y sus componentes, y los tipos de datos comunes.
2) La macro NSA.1 PORT y los convenios de definición de servicio abstracto asociados, de X.407, para especificar el puerto de extracción.
3) Las macros NSA.1, ABSTRACT-BIND, ABSTRACT-UNBIND, ABSTRACT-OPERATION, y ABSTRACT-ERROR y los convenios de definición de servicio abstracto asociados, de X.407, para especificar el servicio abstracto AM.

Cuando esta Recomendación describe una clase de estructura de datos que tiene componentes, cada componente se clasifica según uno de los siguientes **grados**:

1) **Obligatorio** (O) – Un componente obligatorio tiene que estar siempre presente en cada caso de la clase.
2) **Facultativo** (F) – Un componente facultativo estará presente en un caso de la clase a discreción del objeto (por ejemplo, el usuario) que suministra ese caso.
3) **Condicional** (C) – Un componente condicional estará presente en un caso de la clase como lo prescriba esta Recomendación.

5.2 *Convenios sobre los tipos de atributos utilizados en el cuadro 1/X.413 (§ 11)*

Esta Recomendación utiliza los convenios indicados a continuación para la definición de los tipos de atributo del servicio abstracto AM.

En la columna encabezada por *Uno/múltiples valores* pueden aparecer los siguientes valores:

S un solo valor

M múltiples valores

En la columna encabezada por *Nivel de soporte por el AM y la AU de acceso* pueden aparecer los siguientes valores:

O obligatorio

F facultativo

En las columnas que llevan por encabezamiento *Presencia en la inscripción de mensaje entregado, Presencia en la inscripción de informe entregado,* y *Presencia de mensaje devuelto,* la presencia de cada tipo de atributo se describe por uno de los siguientes valores:

P *siempre presente* en la inscripción porque:
- es obligatorio para generación por el AM; o
- es un parámetro obligatorio con valor por defecto en la operación abstracta correspondiente.

C *condicionalmente presente* en la inscripción. Estaría presente porque:
- el AM lo admite y el usuario está abonado al mismo; y
- estaba presente en un parámetro facultativo en la operación abstracta correspondiente.

– *siempre ausente,* en cualquier otro caso.

En las columnas encabezadas por *Disponible para listado alerta* y *Disponible para resumir* pueden aparecer los siguientes valores:

N no

Y sí

5.3 *Convenios de descripción para tipos de atributos utilizados en el cuadro 2/X.413 (§ 11)*

Esta Recomendación utiliza los convenios enumerados más adelante en su definición de los tipos de atributos para el servicio abstracto AM. El § 11 incluye el cuadro 2/X.413 que enumera los tipos de atributo.

En la columna encabezada por *Uno/múltiples valores* pueden aparecer los siguientes valores:

S un solo valor

M múltiples valores

En la columna encabezada por *Generado en la fuente por* pueden aparecer los siguientes valores:

EM Operación abstracta de entrega de mensaje

AM Almacenamiento de mensajes

EI Operación abstracta de entrega de informe.

5.4 *Convenios relativos al tipo de caracteres utilizados para texto en general*

En toda la exposición de esta Recomendación los términos se escriben en **negrita** cuando están definidos, y en todas las demás ocasiones no se destacan. En el texto inglés, los términos que son nombres propios se escriben comenzando por mayúscula, no escribiéndose así los términos genéricos. Los términos genéricos que se componen de múltiples palabras van unidos con guiones.

5.5 *Convenios relativos al tipo de caracteres utilizados para las definiciones NSA.1*

En toda la exposición de esta Recomendación, las definiciones se escriben en un tipo diferente (**negrita**) de caracteres que el resto del documento, a fin de resaltar la diferencia entre el texto normal y las definiciones NSA.1. El tipo de caracteres utilizado para las definiciones NSA.1 es también de menor tamaño, que el utilizado para el texto ordinario. Cuando en textos de acompañamiento se describen elementos de protocolo y valores de elementos de NSA.1, sus nombres se escriben en **negrita**.

5.6 *Reglas para las definiciones NSA.1*

Las definiciones NSA.1 aparecen tanto en el cuerpo del documento para facilitar la exposición como formalmente, en anexos para referencia. Si se encuentran diferencias entre la NSA.1 utilizada en la exposición y la definida formalmente en el anexo correspondiente, se indica un error de especificación.

6 Modelo de almacenamiento de mensajes

El almacenamiento de mensajes (AM) se modela como un objeto atómico, que actúa como un proveedor de servicios a un usuario del servicio abstracto AM (es decir, un agente de usuario), y como un usuario de servicios proporcionados por el sistema de transferencia de mensajes (STRM).

Un AM desempeña un papel intermedio entre el AU y el STRM. Su función primaria es aceptar la entrega de mensajes a nombre de un solo usuario final del STM, y mantenerlos para que sean posteriormente extraídos por el agente de usuario del usuario final. El AM proporciona también servicios de depósito de mensajes y de administración de mensajes al AU, en efecto, «atravesando» el STRM. Esto permite al AM proporcionar una funcionalidad adicional en comparación con el depósito directo en el ATM, como la retransmisión de mensajes residentes en el AM.

Al igual que el AU, el AM actúa en representación de un solo usuario final del STM, es decir, no proporciona un servicio AM común a, o compartido entre, múltiples usuarios.

El AM se describe utilizando un modelo abstracto para definir los servicios proporcionados por el AM; el servicio abstracto de almacenamiento de mensajes. La figura 1/X.413 muestra el servicio abstracto AM en relación con su usuario y el servicio abstracto de sistema de transferencia de mensajes. En esta figura, las casillas abiertas representan el consumo del servicio abstracto y las casillas cerradas representan el suministro del servicio abstracto.

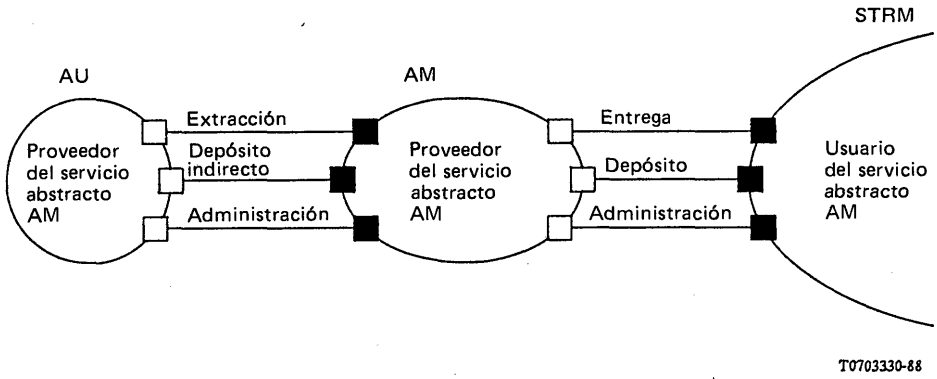


FIGURA 1/X.413

Servicio abstracto de almacenamiento de mensajes

Para una introducción y descripción del concepto del servicio abstracto y sus convenios de definición, véase la Recomendación X.407.

En la mensajería segura, el AM se trata como un objeto independiente con identidad única, y tiene una clave (o un conjunto de claves) independiente con el AU.

6.1 *Objeto almacenamiento de mensajes*

El AM se modela como un objeto atómico. Suministra los servicios abstractos de puerto de extracción AM al usuario del servicio abstracto AM. Actuando como un proveedor del servicio abstracto STRM «subrogado», el AM suministra también los servicios abstractos de depósito y administración del STRM al usuario del servicio abstracto AM (usuario AM), y actuando como un «subrogado» del AU, consume los servicios abstractos de puerto de entrega, puerto de depósito y puerto de administración del STRM en su papel de usuario del servicio abstracto STRM.

La definición formal del objeto almacenamiento de mensaje es la siguiente:

```
mS OBJECT
        PORTS { retrieval[S],
                indirectSubmission[S],
                administration[S],
                delivery[C],
                submission[C],
                administration[C] }
        ::= id-ot-ms
```

El usuario AM se modela también como un objeto. Consume los servicios abstractos de puerto de extracción y puerto de depósito indirecto del AM y los servicios abstractos de puerto de administración proporcionados transparentemente por el AM.

```
msUser OBJECT
        PORTS { retrieval[C],
                indirectSubmission[C],
                administration[C] }
        ::= id-ot-ms-user
```

6.2 *Puertos de almacenamiento de mensajes*

Un AM proporciona puertos de extracción, depósito indirecto y administración al usuario del servicio abstracto AM. El conjunto de capacidades proporcionadas por estos puertos suministra el servicio abstracto AM. Las capacidades de extracción son exclusivas del AM. Estas capacidades incluyen la obtención de información sobre la captura (total o parcial), y la supresión de mensajes residentes en el AM. Se proporcionan capacidades adicionales para registrar ciertas acciones automáticas proporcionadas por el AM (esto es, retransmisión automática y alerta).

Nota – La ISO proyecta de definir servicios adicionales de gestión de mensajes proporcionados por el AM en nombre del AU para el registro cronológico de mensajes entrantes y salientes y para correlacionar automáticamente las notificaciones entrantes con la información de registro cronológico sobre los mensajes salientes. Estos servicios están fuera del ámbito de esta Recomendación.

A fin de proporcionar los servicios descritos en el § 6.1 al usuario AM, el AM interactúa, a nombre del usuario AM, con el servicio abstracto STRM, y actúa como un consumidor de los puertos de entrega, depósito y administración del STRM. Los servicios abstractos proporcionados por los puertos STRM se definen en el § 8 de la Recomendación X.411.

Por medio de la operación abstracta de vinculación, el AM autentica a un usuario AM antes de proporcionarle cualquiera de las mencionadas capacidades de extracción. Análogamente, los servicios abstractos STRM tienen que autenticar al usuario del servicio abstracto STRM antes de extender sus servicios a dicho usuario del servicio abstracto STRM.

Con excepción del servicio de alerta proporcionado por el puerto de extracción y el servicio de control de depósito proporcionado por el puerto de depósito indirecto, todos los servicios proporcionados por el servicio abstracto AM son invocados por el usuario AM y efectuados por el AM.

Pueden asignarse etiquetas de seguridad al AM de acuerdo con la política de seguridad que se esté aplicando. La política de seguridad puede también definir cómo han de utilizarse las etiquetas de seguridad para poner en práctica dicha política de seguridad. Si se asignan etiquetas de seguridad al AM, el tratamiento de los mensajes almacenados y los informes que llevan esas etiquetas de seguridad pueden verse afectados por la política de seguridad en vigor. Si no se asignan etiquetas de seguridad al AM, el tratamiento de los mensajes almacenados y de los informes es discrecional.

Si se establecen contextos de seguridad entre el AU y el AM, y entre el AM y el ATM, la etiqueta de seguridad que se asigna a un mensaje o a una sonda está confinada al contexto de seguridad concordante con la política de seguridad en vigor. Si no se establecen contextos de seguridad, la asignación de una etiqueta de seguridad a un mensaje o a una sonda queda a la discreción del originador.

6.2.1 *Puerto de extracción*

El **puerto de extracción** se define como sigue:

```
retrieval PORT
        CONSUMER INVOKES {
            Summarize,
            List,
            Fetch,
            Delete,
            Register-MS }
        SUPPLIER INVOKES {
            Alert }
        ::= id-pt-retrieval
```

Los detalles de los servicios abstractos de **puerto de extracción** se describen en los § 7 a 9.

6.2.2 *Puerto de depósito indirecto*

El **puerto de depósito indirecto** se define como sigue:

```
indirectSubmission PORT ::= submission
```

El **puerto de depósito indirecto** utiliza los servicios abstractos de puerto de depósito definidos en el § 8.2 de la Recomendación X.411.

6.2.3 *Puerto de administración*

El **puerto de administración** se define en el § 8.4 de la Recomendación X.411.

No tendrá interacción con el servicio abstracto de cambio de credenciales. Si el usuario AM necesita que sus credenciales sean actualizadas, se utiliza la operación abstracta registro en el AM. Véase el § 8.6.

6.3 *Modelo de información*

Este punto describe el modelo de información utilizado por el AM. Este es un modelo de **bases de información**, constituido por **inscripciones**, que consisten en **atributos**.

6.3.1 *Bases de información*

El AM almacena y mantiene **bases de información**. Una **base de información** en el AM es una «base de datos» que contiene todas las **inscripciones** que representan objetos constituyentes de una o más categorías particulares.

Esta Recomendación define y describe la **base de información de mensajes almacenados**. Esta mantiene información derivada de entregas de mensaje y entregas de informe al AM a través del puerto de entrega STRM, y se describe en el § 6.4.

Nota – Un futuro addéndum a la parte correspondiente de la Norma ISO definirá bases de información adicionales para el registro, denominadas registro de entrada y registro de salida, que están fuera del alcance de la presente Recomendación del CCITT.

```
InformationBase ::= INTEGER {
        stored-messages         (0),
        inlog                   (1),
        outlog                  (2) } (0 .. ub-information-bases)
```

6.3.2 *Inscripciones*

Cada **base de información** está organizada como una secuencia de **inscripciones**. Una **inscripción** representa un objeto y sólo uno (por ejemplo un mensaje entregado) dentro de la **base de información**.

Cada inscripción se identifica por medio de su **número secuencial**, que es único dentro de una **base de información**, y es generado por el AM cuando se crean nuevas inscripciones. Dentro de una **base de información**, el AM genera los **números secuenciales** en orden ascendente, sin reciclar. Estos números no se reutilizan nunca.

```
SequenceNumber ::= INTEGER (0 .. ub-messages)
```

Nota – Por ejemplo, el AM puede decidir atribuir **números secuenciales** utilizando el tiempo con una granularidad suficiente para asegurar la unicidad.

6.3.3 *Atributos*

6.3.3.1 *Introducción*

Una **inscripción** consiste en un conjunto de **atributos**. Se representa en la figura 2/X.413.

Cada **atributo** proporciona un elemento de información sobre los datos, o derivado de los datos, a que corresponde la **inscripción**. Uno de estos elementos de información es el **número secuencial** de la **inscripción** propiamente dicho, y otro es la **hora de creación**.

Un **atributo** consiste en un **tipo de atributo**, que identifica la clase de información dada por un **atributo**, y el correspondiente (o los correspondientes) **valor o (valores) de atributo**, que son casos particulares de la clase que aparece en la **inscripción**.

```
Attribute ::= SEQUENCE {
        type            AttributeType,
        values          SEQUENCE (SIZE 1 .. ub-attribute-values) OF ANY -- DEFINED BY type }
```

Nota 1 – Así, por ejemplo, en una inscripción de mensaje entregado (descrita en el § 6.4), el **tipo de atributo** podría ser la **prioridad** del mensaje, y un **valor de atributo** correspondiente podría ser **urgente**.

Todos los **atributos** de una **inscripción** tienen que ser de **tipos de atributo** distintos.

Para algunos **tipos de atributo**, un **atributo** puede contener únicamente un solo **valor de atributo**. Se dice entonces que tal **tipo de atributo** es **de un solo valor** (o **univaluado**). Para otros, un **atributo** puede contener uno o más **valores de atributo**, todos del mismo tipo de datos NSA.1. Se dice de tal **tipo de atributo** que es de **múltiples valores** (o **multivaluado**). Al definirse el **tipo de atributo** se enuncia si éste es un tipo de atributo **de un solo valor** o de **múltiples valores** (véase el § 6.3.3.2).

Nota 2 – Así, por ejemplo, el **tipo de atributo** para el **atributo nombre de originador** (descrito en el § 11.2.28) es **de un solo valor**, en tanto que para **nombres de otros destinatarios** (descrito en el § 11.2.29) es de **múltiples valores**.

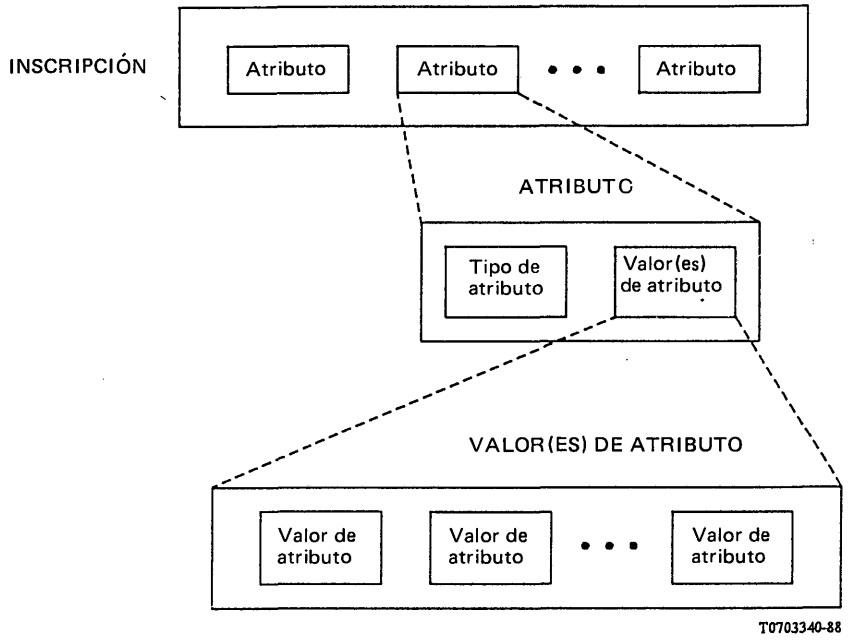


FIGURA 2/X.413

Componentes de una inscripción

6.3.3.2 *Tipo de atributo*

Algunos **tipos de atributo** se normalizarán internacionalmente. Otros **tipos de atributo** serán definidos por autoridades administrativas nacionales y organizaciones privadas. Esto implica que cierto número de autoridades distintas serán responsables de la asignación de tipos de una manera que asegure que cada uno será distinto de todos los demás tipos asignados. Esto se consigue identificando cada **tipo de atributo** con un identificador de objeto cuando se define el **tipo de atributo**.

Attribute Type ::= OBJECT IDENTIFIER

Ciertos **tipos de atributo** de carácter general para la base de información de mensajes almacenados se definen en el § 11 de esta Recomendación. Estos **tipos de atributo** se denominan **tipos de atributo generales** y los atributos de estos tipos son **atributos generales.**

6.3.3.3 *Valores de atributo*

La definición de un **tipo de atributo** implica también la especificación del tipo de datos NSA.1 con el cual tienen que ser conformes tales atributos. El tipo de datos de un **valor de atributo** para el **tipo de atributo** se define mediante el identificador de objeto para el **tipo de atributo.**

6.3.3.4 *Definición de tipo de atributo y la macro ATTRIBUTE*

La definición de **tipo de atributo** comprende:

a) la asignación de un identificador de objeto al **tipo de atributo**;

b) la indicación del tipo de datos NSA.1 de un **valor de atributo**;

c) la indicación de un **atributo** de este **tipo de atributo** puede tener más de un valor;

d) la indicación de si un **atributo** de este **tipo de atributo** puede utilizarse para filtrado basado en la igualdad, subcadena y/o relaciones de ordenamiento (véase el § 8.1.2).

Nota – Un filtro puede siempre detectar la presencia o ausencia, en una inscripción, de un **atributo** de un **tipo de atributo** determinado.

La siguiente macro NSA.1 se utiliza para definir un **tipo de atributo**. La definición formal de esta macro se da en la Recomendación X.501 y se reproduce aquí como ayuda al lector.

```
ATTRIBUTE MACRO ::=
BEGIN

    TYPE NOTATION   ::= AttributeSyntax Multivalued | empty
    VALUE NOTATION  ::= value (VALUE OBJECT IDENTIFIER)

    AttributeSyntax     ::= "WITH ATTRIBUTE-SYNTAX" SyntaxChoice
    SyntaxChoice        ::= value (ATTRIBUTE-SYNTAX) Constraint | type MatchTypes

    Constraint          ::= "(" ConstraintAlternative ")" | empty
    ConstraintAlternative ::= StringConstraint | IntegerConstraint
    StringConstraint    ::= "SIZE" "(" SizeConstraint ")" | empty
    SizeConstraint      ::= SingleValue | Range
    SingleValue         ::= value (INTEGER)
    Range               ::= value (INTEGER) ".." value (INTEGER)
    IntegerConstraint   ::= "(" Range ")"

    MatchTypes          ::= "MATCHES FOR" Matches | empty
    Matches             ::= Match Matches | Match
    Match               ::= "EQUALITY" | "SUBSTRINGS" | "ORDERING"
    Multivalued         ::= "SINGLE VALUE" | "MULTIVALUE" | empty

END
```

La correspondencia entre las partes de la definición, enumeradas anteriormente y los diversos elementos de la notación introducidos por la macro **ATTRIBUTE**, es la siguiente:

a) **Valor de MACRO**: El **identificador de objeto** que se utiliza para identificar un atributo.

b) **Sintaxis de atributo**: Señala qué elección de sintaxis se ha hecho.

c) **Elección de sintaxis**: Señala si el atributo está definido externa o internamente. La sintaxis de todos los atributos definidos en esta [Recomendación Parte de la Norma] se define internamente, lo que significa que se utiliza la elección de **tipo de concordancia-tipos.**

d) **Multivalorado**: indica si el atributo es de valor simple o múltiple.

e) **Concordancia-tipos**: Da el tipo de datos del contenido del atributo, y describe si el atributo puede o no hacerse concordar ("**MATCHES FOR**") para **igualdad** ("**EQUALITY**"), para **subcadenas** ("**SUBSTRINGS**"), y por una relación de **ordenamiento** ("**ORDERING**"). Si la producción es vacía no se definen reglas de concordancia.

La concordancia a los efectos de esta Recomendación está limitada a lo siguiente:

i) **EQUALITY** se aplica a cualquier sintaxis de atributo. El valor presentado debe ajustarse al tipo de datos de la sintaxis de atributo,

ii) **SUBSTRING** se aplica a cualquier sintaxis de atributo con un tipo de datos de cadena. El valor presentado debe ser una secuencia ("**SEQUENCE OF**"), en la que sus elementos se ajusten al tipo de datos, y

iii) **ORDERING** es aplicable a cualquier sintaxis de atributo para la que pueda definirse una regla que permita que un valor presentado sea descrito como menor o igual que, o mayor que un valor objetivo. El valor presentado debe ajustarse al tipo de datos de la sintaxis de atributo. El AM lo utiliza para los tipos de datos INTEGER y UTCTime. Para los UTCTime el orden es cronológico, no alfabético.

Las elecciones y parámetros restantes de la macro **ATTRIBUTE** no se utilizan en la presente Recomendación.

6.3.4 *Inscripciones principales, inscripciones progenitoras e inscripciones vástagos*

Aunque las inscripciones en una base de información generalmente son independientes unas de otras, el modelo de información AM permite relacionar tales **inscripciones** unas con otras. Una **inscripción**, una **inscripción vástago**, puede ser el vástago de otra, que es su **inscripción progenitora**, en una relación estructurada en forma de árbol. Una **inscripción** que no es una **inscripción vástago** se denomina **inscripción principal**.

Esta relación se registra por medio de dos **atributos generales** especiales:

a) **número secuencial de progenitor**: Este atributo de un solo valor da el número secuencial de una **inscripción progenitora** de la **inscripción vástago**. No existe en una **inscripción principal**. Su definición se da en el § 11.2.30.

b) **número secuencial de vástago**: Este atributo de múltiples valores da los números secuenciales de todas las **inscripciones vástagos** de una **inscripción progenitora**. No existe en una inscripción que no sea una **inscripción progenitora**. Su definición se da en el § 11.2.1.

Las operaciones abstractas de un servicio abstracto AM (véase el § 8) actúan por defecto solamente sobre **inscripciones principales**. Puede hacerse que algunas actúen sobre todas las inscripciones: las **inscripciones principales** y las **inscripciones vástagos**. En particular, el argumento de una operación abstracta de suprimir (véase el § 8.5) sólo puede seleccionar **inscripciones principales**, en cuyo caso la **inscripción principal** y todos sus vástagos, y los vástagos de sus vástagos, etc., serán suprimidos.

Nota – Este concepto permite, por ejemplo, que las partes de cuerpo de un mensaje interpersonal que contenga un mensaje retransmitido (para detalles véase el § 19.1 de la Recomendación X.420) se representen por **inscripciones vástagos** individuales. El **atributo general de contenido** de la **inscripción principal** comprenderá el **contenido** completo, por lo que los datos que representan esa **parte del cuerpo** de mensaje, están lógicamente presentes en más de una **inscripción**.

6.4 *Mensajes almacenados*

La **base de información de mensajes almacenados** actúa como un depositario de la información obtenida de las operaciones abstractas entrega de mensaje (MessageDelivery) y entrega de informe (ReportDelivery) del puerto de entrega contiene inscripciones para mensajes entregados (**inscripciones de mensaje entregado**) de un número abierto de tipos de contenido, y para informes (**inscripciones de informe entregado**). El AM crea una inscripción en la **base de información de mensajes almacenados** cuando se entrega un mensaje o informe al AM. Para más detalles sobre estos asientos y la manera de generarlos, véanse los § 11 y 15.

Para obtener información del contenido de un mensaje, el AM tiene que conocer la sintaxis y la semántica del contenido, señaladas mediante el tipo de contenido. En general, un caso concreto del AM tiene conocimiento de cero o más tipos de contenido. Cuando un AM encuentra un mensaje de cuyo tipo de contenido tiene un conocimiento insuficiente, está incapacitado para generar cualquier atributo específico al tipo de contenido en la inscripción del mensaje.

Un mensaje entregado o una notificación que llega pueden dar lugar a una inscripción principal y a uno o más niveles de inscripciones vástagos. El caso definido por esta Recomendación es aquél en que una notificación de no entrega tiene un contenido devuelto (la **inscripción de informe entregado** es la inscripción principal y el contenido devuelto es la inscripción vástago, denominada **inscripción de contenido devuelto**).

Las reglas para la división del contenido de un mensaje a través de varias inscripciones son específicas para cada tipo de contenido. Puede utilizarse un **atributo de sinopsis** específico al contenido para indicar cómo se relaciona la inscripción principal y las inscripciones vástagos correspondientes. Cuando tal atributo se define, aparece en la Recomendación que define el tipo de contenido propiamente dicho. El **atributo de sinopsis** es construido por el AM.

Nota – Para la mensajería interpersonal (Recomendación X.420), los mensajes IP anidados dentro de un mensaje IP se representan, cada uno de ellos, por una inscripción vástago. El tipo de atributo sinopsis-mip es un ejemplo de un **tipo de atributo de sinopsis** específico del contenido.

Una propiedad importante de una inscripción en los mensajes almacenados es su **estado de inscripción**. Este es creado y mantenido por el AM. Puede tomar los siguientes valores:

a) **Nuevo** – El mensaje no ha sido ni **listado** por un AU ni procesado automáticamente por el AM.

b) **Listado** – Se ha devuelto al AU información sobre el mensaje en una operación abstracta de listado o en una operación abstracta de captura, pero el mensaje no ha sido aún completamente **procesado**.

c) **Procesado** – O bien el AU ha «capturado completamente» el mensaje, o el AM ha efectuado alguna acción automática sobre el mismo. (Obsérvese que algunas acciones automáticas culminan en la supresión del mensaje). La definición exacta de «traído completamente» es específica del contexto y aparece en la correspondiente Recomendación específica del contenido.

   El **estado de la inscripción** de una notificación de (no)entrega pasa a ser **procesado** cuando se recupera el sobre de informe entregado.

La definición del **estado de inscripción** es la siguiente:

```
EntryStatus ::= INTEGER {
        new             (0),
        listed          (1),
        processed       (2) }
```

6.5 *Acciones automáticas*

6.5.1 *Introducción*

Este punto define un marco para las **acciones automáticas** que pueden registrarse en el AM.

Una **acción automática** es una acción que ocurrirá automáticamente cuando se satisfagan los criterios de registro asociados. El resultado de una acción que se está invocando resulta visible externamente al AM. Las **acciones automáticas** se registran en el AM utilizando la operación abstracta de registro en el AM (véase el § 8.6).

Cada clase de **acción automatica** se identifica por medio de un **tipo de acción automática**. Asociado con el registro de una **acción automática** hay un **parámetro registro de acción automática** correspondiente, que es el parámetro (o parámetros) que necesita el AM para efectuar automáticamente la **acción automática** registrada. El registro de una **acción automática** requiere el uso de un **identificador de registro de acción automática** para identificar ese registro.

```
AutoActionRegistration ::= SEQUENCE {
        type                        AutoActionType,
        registration-identifier     [0] INTEGER (1 .. ub-per-auto-action)DEFAULT1,
        registration-parameter      [1] ANY DEFINED BY type }
```

6.5.2 *Tipo de acción automática*

Algunos **tipos de acción automática** se normalizarán imternacionalmente. Otros **tipos de acción automática** serán definidos por autoridades administrativas nacionales y organizaciones privadas. Esto significa que diversas autoridades distintas serán responsables de asignar tipos de una forma que asegure que cada uno es distinto de todos los demás **tipos de acción automática** asignados. Esto se consigue identificando cada **tipo de acción automática** mediante un identificador de objeto cuando se define el **tipo de acción automática**.

```
AutoActionType ::= OBJECT IDENTIFIER
```

Ciertos **tipos de acción automática** de carácter general se definen en el § 12 de esta Recomendación. Tales **tipos de acción automática** se conocen como **tipos de acción automática generales** y las **acciones automáticas**.

6.5.3 *Parámetros de registro de acción automática*

La definición de un **tipo de acción automática** comprende también la especificación del tipo de datos NSA.1 al cual debe ajustarse el **parámetro registro de acción automática**. El tipo de datos de un **parámetro registro** se define mediante el identificador de objeto para el **tipo de acción automática**.

6.5.4 *Definición de tipo de acción automática y la macro AUTO-ACTION*

La definición de un **tipo de acción automática** comprende:

a) asignar un identificador de objeto al **tipo de acción automática**;

b) indicar el tipo de datos NSA.1 del **parámetro registro de acción automática**.

La siguiente macro NSA.1 puede (pero no tiene necesariamente que) utilizarse para definir un **tipo de acción automática**:

```
AUTO-ACTION MACRO ::=
BEGIN
        TYPE NOTATION    ::= Registration
        VALUE NOTATION   ::= value (VALUE OBJECT IDENTIFIER)

        Registration     ::= "REGISTRATION PARAMETER IS" type
END
```

La correspondencia entre las partes de la definición, tal como han sido enumeradas anteriormente, y los diversos elementos de la notación introducida por la macro **AUTO-ACTION** es la siguiente:

a) **Registro**: proporciona el tipo de datos de los parámetros de registro asociados con una acción automática.

b) **Valor**: el **identificador de objeto** que se utiliza para identificar la acción automática.

Nota – En la macro no se proporciona un soporte para definir la interacción (si la hubiere) entre registros deferentes de las mismas (o diferentes) **acciones automáticas**.

6.6 *Retransmisión de un mensaje*

El usuario AM utiliza la operación abstracta de depósito de mensaje y sus parámetros definidos en el § 8.2 de la Recomendación X.411 para solicitar que un mensaje almacenado en el AM sea retransmitido explícitamente a otros usuarios.

El **parámetro petición de retransmisión** se define utilizando la macro **EXTENSION** definida en el § 9 de la Recomendación X.411 de la forma siguiente:

```
forwarding-request EXTENSION
        SequenceNumber
        CRITICAL FOR SUBMISSION
        ::= 36
```

Si el **número secuencial** no corresponde al de una entrada en la **base de información** de **mensajes almacenados**, o corresponde a una entrada que es inapropiada para la retransmisión, se informa de ello utilizando el error abstracto **petición incoherente** del § 8.2.2.7 de la Recomendación X.411.

7 Operaciones abstractas de vinculación y de desvinculación

7.1 *Operaciones abstractas de vinculación*

La **operación abstracta de vinculación AM** vincula los puertos de depósito indirecto, extracción y administración del usuario AM (consumidor) al AM (suministrador). El iniciador (de vinculación AM) es el usuario AM, en tanto que el respondedor es el propio AM. Vinculación AM se define como sigue:

```
MSBind ::= ABSTRACT-BIND
        TO { IndirectSubmission[5], retrieval[5], administration[5] }
        BIND
            ARGUMENT  MSBindArgument
            RESULT    MSBindResult
            BIND-ERROR MSBindError
```

Puede existir una sola asociación abstracta en un instante dado entre el AM y el usuario AM.

7.1.1 *Argumento de vinculación-abstracta*

Los parámetros **argumento de vinculación-abstracta** se utilizan para identificar, autenticar y establecer el contexto de seguridad para un usuario del servicio abstracto AM. Contienen también un conjunto de restricciones a las inscripciones que han de devolverse como resultado de una operación abstracta de captura y, finalmente, una solicitud de ser informado sobre los tipos acción automática, tipos atributo y tipos contenido admitidos por el AM.

La definición de estos parámetros es la siguiente:

```
MSBindArgument ::= SET{
        initiator-name          ORAddressAndOrDirectoryName,
        initiator-credentials   [2] InitiatorCredentials,
        security-context        [3] IMPLICIT SecurityContext OPTIONAL,
        fetch-restrictions      [4] Restrictions OPTIONAL -- default is none --,
        ms-configuration-request [5] BOOLEAN DEFAULT FALSE,}
```

1) **Nombre del iniciador** (C): Este argumento contiene el nombre del iniciador de la asociación y es suministrado por el iniciador. Este argumento se define con más detalles en el § 8.1.1.1.1.1 de la Recomendación X.411.

2) **Credenciales del iniciador** (O): Este parámetro contiene las **credenciales** del iniciador de la asociación. Será generado por el iniciador de la asociación abstracta.

   Las **credenciales del iniciador** pueden ser utilizadas por el respondedor para autenticar la identidad del iniciador (véase la Recomendación X.509).

   Si sólo se utiliza la **autenticación simple**, las **credenciales del iniciador** comprenden una contraseña simple.

   Si se utilizan la **autenticación fuerte**, las **credenciales del iniciador** comprenden un **testigo vinculación iniciador**, y opcionalmente, un **certificado de iniciador**. El **testigo vinculación iniciador** y el **certificado de iniciador** se definen con más detalle en el § 8.1.1.1.1.2 de la Recomendación X.411. Las **credenciales de iniciador** del usuario AM pueden diferir de las **credenciales de iniciador** utilizadas en vinculación AM, como se define en el § 8.1.1.1.1.2 de la Recomendación X.411.

3) **Contexto de seguridad** (F): Este parámetro identifica el **contexto de seguridad** sobre el cual se propone operar el iniciador de la asociación abstracta. Es generado por el iniciador de la asociación abstracta. El **contexto de seguridad** se define con más detalles en el § 8.1.1.1.1.3 de la Recomendación X.411.

El **contexto de seguridad** comprende una o más **etiquetas de seguridad** que definen la sensibilidad de interacciones que pueden ocurrir entre el usuario del servicio abstracto AM y el servicio abstracto AM mientras dura la asociación abstracta, en consonancia con la **política de seguridad** en vigor. El **contexto de seguridad** será uno que esté permitido por las **etiquetas de seguridad de usuario** registradas, del usuario del servicio abstracto AM, y por las **etiquetas de seguridad** asociadas con el AM.

En ausencia de este parámetro, no se establecen **contextos de seguridad** entre el usuario del servicio abstracto AM y el servicio abstracto AM, y la sensibilidad de interacciones que pueden ocurrir entre el usuario del servicio abstracto AM y el servicio abstracto AM están a la discreción del invocador del servicio abstracto.

4) **Restricciones de captura** (F): Contiene las restricciones sobre las inscripciones que han de devolverse como resultado de una operación abstracta de captura. Las **restricciones de captura** siguen establecidas hasta que se ha emitido una operación abstracta de desvinculación.

En ausencia de este argumento, su valor por defecto es que no es necesario efectuar **restricciones de captura**.

Este argumento consiste en los siguientes componentes:

```
Restrictions ::= SET{
    allowed-content-types       [0] SET SIZE (1 .. ub-content-types) OF OBJECT IDENTIFIER
                                    OPTIONAL
        -- default is no restriction --,
    allowed-EITs                [1] MS-EITs OPTIONAL -- el valor por defecto es ausencia de
                                    restricciones --,
    maximum-content-length      [2] ContentLength OPTIONAL -- el valor por defecto es ausencia de
                                    restricciones -- }
```

a) **Tipos de contenido autorizados** (C): Los tipos de contenido que el usuario del servicio abstracto AM está dispuesto a aceptar como resultado de una operación abstracta de captura. Todo mensaje cuyo tipo de contenido sea diferente a los especificados no será retornado pero dará por resultado un error, a menos que la operación abstracta de captura haya contraordenado explícitamente la restricción.

En ausencia de este componente, el valor por defecto es que no es necesario efectuar restricciones a captura sobre tipos de contenido.

b) **TIC autorizados** (C): Los tipos de información codificada que el usuario del servicio abstracto AM está dispuesto a aceptar como resultado de una operación abstracta de captura. Si un mensaje contiene tipos de información codificada diferentes de los especificados se efectuará un filtrado a fin de que las partes TIC desautorizadas no se devuelvan junto con el texto del mensaje. Si el mensaje completo consiste en TIC desautorizados, se notificará un error. No se efectuará filtrado si la operación abstracta de captura ha contraordenado explícitamente la restricción.

MS-EITs ::= SET SIZE (1 .. ub-encoded-information-types) OF MS-EIT

MS-EIT ::= OBJECT IDENTIFIER

En ausencia de este componente, el valor por defecto es que no es necesario ejecutar **restricciones a captura** sobre tipos de información codificada.

c) **Máxima longitud de contenido** (C): Longitud máxima del contenido que el usuario del servicio abstracto AM está dispuesto a aceptar como resultado de una operación abstracta de captura. Todo mensaje cuya **longitud de contenido** sea superior a la especificada no se devolverá, sino que dará lugar a un error, a menos que la operación abstracta de captura haya contraordenado explícitamente la restricción.

En ausencia de este componente, el valor por defecto es que no es necesario efectuar **restricciones a captura** sobre la **longitud de contenido**.

5) **Petición de configuración AM** (C): Se solicita **petición de configuración AM** para obtener información sobre cuáles de las acciones automáticas y atributos opcionales son admitidos por el AM.

En ausencia de este componente, el valor por defecto es falso, que indica que no se está haciendo tal petición.

7.1.2 *Resultados vinculación abstracta*

Los parámetros **resultado de vinculación abstracta** son los siguientes:

```
MSBindResult ::= SET{
        responder-credentials       [2] ResponderCredentials,
        available-auto-actions      [3] SET SIZE (1 .. ub-auto-actions) OF AutoActionType OPTIONAL,
        available-attribute-types   [4] SET SIZE (1 .. ub-attributes-supported) OF Attribute Type
                                        OPTIONAL,
        alert-indication            [5] BOOLEAN DEFAULT FALSE,
        content-types-supported     [6] SET SIZE (1 .. ub-content-types) OF OBJECT IDENTIFIER
                                        OPTIONAL }
```

1) **Credenciales del respondedor** (M): Este parámetro contiene las credenciales del respondedor de la asociación abstracta. Será generado por el respondedor de la asociación abstracta.

   Las **credenciales del respondedor** pueden ser utilizadas por el iniciador para autenticar la identidad del respondedor (véase la Recomendación X.509).

   Si sólo se utiliza la **autenticación simple**, las **credenciales del respondedor** comprenden una **contraseña** simple asociada con el respondedor.

   Si se utiliza una **autenticación fuerte**, las **credenciales del respondedor** comprenden un **testigo de vinculación respondedor**, y, opcionalmente, un **certificado del respondedor**, generados ambos por el respondedor de la asociación abstracta. El **testigo de vinculación respondedor** y el **certificado del respondedor** se definen con más detalle en el § 8.1.1.1.2.2 de la Recomendación X.411.

2) **Acciones automáticas disponibles** (C): Especifica un conjunto de todas las posibles **acciones automáticas** admitidas por el AM (y no, sencillamente, las solicitadas por el usuario del servicio abstracto AM). Sólo está presente si se hace una **petición de configuración AM**.

3) **Tipos de atributo disponibles** (C): Especifica el conjunto de todos los atributos opcionales admitidos por el AM. Sólo está presente si se hace una **petición de configuración AM**.

4) **Indicación de alerta** (C): Si es verdadera ha ocurrido una condición de **alerta** con posterioridad a la última **indicación de alerta** correcta.

5) **Tipos de contenido admitidos** (C): Especifica un conjunto de identificadores de objetos que definen los **tipos de contenido** conocidos por el AM. Sólo está presente si se hace una **petición de configuración AM**

7.1.3 *Errores vinculación abstracta*

Hay dos posibles errores que son definidos por el **puerto de extracción**, a saber: **error de autenticación** y **contenido de seguridad inaceptable**.

La definición del error es:

```
MSBindError ::= ENUMERATED{
        authentication-error                (0),
        unacceptable-security-context       (1),
        unable-to-establish-association     (2) }
```

1) **Error de autenticación** (C): Este error da a conocer que una asociación abstracta no puede establecerse porque las **credenciales** del iniciador no son aceptables o están indebidamente especificadas.

   El **error de autenticación** no tiene parámetros.

2) **Contexto de seguridad inaceptable** (C): Este error informa que el **contexto de seguridad** propuesto por el iniciador de la asociación abstracta es inaceptable para el respondedor.

   El error de **contexto de seguridad inaceptable** no tiene parámetros.

3) **Incapacidad para establecer asociación** (C): Este error informa que el respondedor ha rechazado la tentativa del iniciador de establecer una asociación abstracta.

   El error **incapacidad para establecer asociación** no tiene parámetros.

7.2 *Operación desvinculación abstracta*

La **operación-desvinculación-abstracta, Devinculación AM** cierra la asociación abstracta. La emisión de **operación-desvinculación-abstracta** da por resultado la mitigación de cualesquiera **restricciones de captura** que se especificaron en el argumento **operación-desvinculación-abstracta**. La **operación-desvinculación-abstracta** no tiene asociados argumento, resultado ni error.

```
MSUnbind ::= ABSTRACT-UNBIND
        FROM { indirectSubmission[S], retrieval[S], administration[S] }
```

8 Operaciones abstractas

Este punto define las siguientes **operaciones abstractas** disponibles en el puerto de extracción:

a) resumir;
b) listado;
c) captura;
d) supresión;
e) registro en el AM;
f) alerta.

El AM es el proveedor del servicio abstracto AM de cada una de estas **operaciones abstractas**. Para la definición formal del puerto de extracción véase el § 6.2.

La operaciones abstractas pueden ser realizadas asíncronamente, con las siguientes condiciones. Las operaciones abstractas supresión y registro en el AM no se realizarán hasta que se hayan completado todas las operaciones abstractas pendientes. Además, estas operaciones abstractas se realizan en el orden en que son invocadas y hay que completarlas antes de que se realice cualquier otra operación abstracta. Como consecuencia de esto y del hecho de que las operaciones abstractas listado y captura cambian el estado de una inscripción de un mensaje, los resultados de las operaciones abstractas resumir, listar y captura pueden ser no determinísticos.

8.1 *Tipos de datos comunes utilizados en las operaciones abstractas*

Este punto define un número de tipos de datos comunes que se utilizan en algunas de las **operaciones abstractas** definidas en el resto del § 8. Muchas de las **operaciones abstractas** emplean inscripciones y atributos definidos en el § 6.3.

Los tipos de datos comunes definidos en esta Recomendación son:

a) gama;
b) filtro;
c) selector;
d) selección de información de inscripción;
e) información de inscripción.

8.1.1 *Gama*

El parámetro **gama** se utiliza para seleccionar una secuencia contigua de inscripciones a partir de una base de información.

```
Range ::= CHOICE {
        sequence-number-range    [0] NumberRange,
        creation-time-range      [1] TimeRange }

NumberRange ::= SEQUENCE {
        from    [0] SequenceNumber OPTIONAL -- omitido significa que no tiene cota inferior --,
        to      [1] SequenceNumber OPTIONAL -- omitido significa que no tiene cota superior -- }

TimeRange ::= SEQUENCE {
        from    [0] CreationTime OPTIONAL -- omitido significa que no tiene cota inferior --,
        to      [1] CreationTime OPTIONAL -- omitido significa que no tiene cota superior -- }

CreationTime ::= UTCTime
```

Los componentes de **gama** tienen los siguientes significados:

1) **Gama de números secuenciales** (C), y
2) **Gama de horas de creación** (C): Estos dos parámetros identifican la secuencia contigua de inscripciones a seleccionar. La **gama de números secuenciales** se da en términos de **números secuenciales**, y la **gama de horas de creación** se da en términos de **horas de creación**. La **hora de creación** de una inscripción es la hora (o fecha) en que el AM generó la inscripción. Los **números secuenciales** de inscripciones sucesivas están siempre en orden ascendente, pero varias inscripciones adyacentes pueden tener la misma **hora de creación**. Los parámetros de **gama de números** y de **gama de horas** tienen los siguientes significados:
   a) **Desde** (F): Es el límite inferior de la **gama**.

      En ausencia de este componente, el significado por defecto es **no hay límite inferior**, y la selección comienza con el mensaje más antiguo (**número secuencial** más bajo) en la base de información.
   b) **Hasta** (F): Es el límite superior de la **gama**.

      En ausencia de este componente el significado por defecto es **no hay límite superior**, y la selección termina con el último mensaje (**número secuencial** más alto) en la base de información.

8.1.2 *Filtros*

8.1.2.1 *Filtro*

Un parámetro **filtro** aplica una prueba para una inscripción dada, la cual satisface o no satisface dicha prueba. Un **filtro** se expresa en términos de aserciones sobre la presencia o el valor de ciertos atributos de la inscripción y es satisfecho únicamente si su evaluación es **verdadero (true)**.

```
Filter ::= CHOICE {
        item    [0] FilterItem,
        and     [1] SET SIZE (1 .. ub-nested-filters) OF Filter,
        or      [2] SET SIZE (1 .. ub-nested-filters) OF Filter,
        not     [3] Filter }
```

Un **filtro** es o bien un **elemento de filtro**, o una expresión que comprende **filtros** más sencillos reunidos por medio de operadores lógicos **y (and)**, **o (or)**, y **no (not)**.

Donde el **filtro** es:

a) un **elemento**, es **verdadero** únicamemte si el correspondiente **elemento de filtro** es **verdadero**;

b) un **y**, es **verdadero** a menos que cualquiera de los **filtros** del **conjunto (SET)** sea **falso**.

Nota – En consecuencia, si el **conjunto (SET)** no contiene **filtros**, el **y** da el valor **verdadero**.

c) un **o**, es **falso** a menos que cualquiera de los **filtros** del **conjunto (SET)** sea **verdadero**;

Nota – En consecuencia, si el **conjunto (SET)** no contiene **filtros** , el **o** da el valor **falso**.

d) un **no**, es **verdadero** si el **filtro** es **falso**.

8.1.2.2 *Elemento de filtro*

A **elemento de filtro** es una aserción sobre la presencia o valor(es) de un atributo de un tipo particular en la inscripción sometida a prueba. Cada una de estas aserciones es **verdadera (true)** o **falsa (false)**.

```
FilterItem ::= CHOICE {
        equality                [0] AttributeValueAssertion,
        substrings              [1] SEQUENCE {
            type                AttributeType,
            strings             SEQUENCE SIZE (1 .. ub-attribute-values) OF CHOICE {
              initital              [0] ANY -- DEFINED BY type --,
              any                   [1] ANY -- DEFINED BY type --,
              final                 [2] ANY -- DEFINED BY type -- } },
        greater-or-equal        [2] AttributeValueAssertion,
        less-or-equal           [3] AttributeValueAssertion,
        present                 [4] AttributeType,
        approximate-match       [5] AttributeValueAssertion }
```

Un elemento de filtro incluye un tipo de atributo que identifica el atributo particular en cuestión.

Una aserción sobre el valor de tal atributo sólo se evalúa si el tipo de atributo está definido, y el valor o valores del atributo contemplados son del tipo de datos definidos para valores de atributo de ese atributo.

Las aserciones sobre el valor de un atributo se evalúan determinando la concordancia del atributo para IGUALDAD (EQUALITY), SUBCADENAS (SUBSTRINGS), y ORDENAMIENTO (ORDERING), según se define en el § 6.3.3.4.

Cuando el **elemento de filtro** establece una aserción de:

a) **igualdad**, es **verdadero** si hay un valor del atributo que es igual establecido en la aserción;

b) **subcadenas**, es **verdadero** únicamente si hay un valor del atributo en el cual las **subcadenas** especificadas aparecen en el orden dado. Las **subcadenas** no deben superponerse y pueden (pero no necesariamente tienen que) estar separadas de los extremos del valor del atributo, y unas con respecto de otras, por cero o más elementos de la **cadena**.

De estar presente, el primer carácter contenido en **inicial**, concordará con el primer carácter del valor de atributo; de estar presente, el último carácter contenido en **final** concordará con el último carácter del valor de atributo. De estar presente, **cualquiera**, concordará con cualquier subcadena del valor de atributo;

c) **mayor o igual**, es **verdadero** únicamente si el orden relativo sitúa el valor suministrado *después de* cualquier valor del atributo;

d) **menor o igual**, es **verdadero** únicamente si el orden relativo sitúa el valor suministrado *antes que* cualquier valor del atributo;

e) **presente**, es **verdadero** únicamente si dicho atributo está presente en el asiento.

f) **concordancia aproximada**, es **verdadero** únicamente si hay un valor del atributo que concuerda con el que se ha hecho una aserción mediante algún algoritmo de concordancia aproximada definido localmente (por ejemplo, variaciones de deletreo, concordancia fonética, etc). En esta versión de la Recomendación no hay directrices específicas para la concordancia aproximada. De no soportarse la concordancia aproximada, debería tratarse este **elemento de filtro** como una concordancia para **igualdad.**

Nota – Si no se indican reglas de concordancia en la definición de atributo, esto significa que sólo se puede probar la presencia del atributo en un **elemento de filtro.**

8.1.2.3 *Aserción de valor de atributo*

Una **aserción de valor de atributo** es una proposición, que puede ser **verdadera, falsa,** o **indefinida,** sobre los valores de una inscripción. Comprende un tipo de atributo y un valor de atributo:

```
AttributeValueAssertion ::= SEQUENCE {
        type    AttributeType,
        value   ANY DEFINED BY type }
```

y es:

a) **indefinida**, si se da cualquiera de las siguientes situaciones:
   1) el tipo de atributo no está presente en la inscripción;
   2) la definición del tipo de atributo no puede hacerse concordar por igualdad o por ordenación;
   3) el valor de atributo no es conforme al tipo de datos de los valores de atributo;

b) **verdadera**, si la entrada contiene un atributo de ese tipo de atributo, uno de cuyos valores de atributo concuerda con ese valor de atributo;

c) **falsa**, en cualquier otro caso.

8.1.3 *Selector*

Un parámetro **selector** se utiliza para seleccionar asientos a partir de una base de información. La selección opera en tres etapas. En la primera, el conjunto total de inscripciones en la base de información puede limitarse a un conjunto contiguo particular especificando su gama. En segundo lugar, pueden seleccionarse las inscripciones dentro de este conjunto especificando un filtro que deba ser satisfecho por la inscripción seleccionada. En tercer lugar, se puede imponer un límite al número de inscripciones así seleccionadas; en este caso, se seleccionan las inscripciones con los números secuenciales más bajos.

```
Selector ::= SET {
        child-entries   [0] BOOLEAN DEFAULT FALSE,
        range           [1] Range OPTIONAL -- default is unbounded --,
        filter          [2] Filter OPTIONAL -- default is all entries within the specified range --,
        limit           [3] INTEGER (1 .. ub-messages) OPTIONAL,
        override        [4] OverrideRestrictions OPTIONAL -- default is that any fetch-restrictions in force
                            do apply -- }
```

Los componentes de **selector** tienen los siguientes significados:

1) **Inscripciones vástagos** (F): Si **falso**, sólo se consideran para la selección las inscripciones principales. Si **verdadero**, se consideran para la selección las inscripciones principales y las inscripciones vástagos.

   En la ausencia de este componente, el significado por defecto es *sólo se consideran las inscripciones principales.*

2) **Gama**(F): La notación de sintaxis abstracta de **gama** se indica en el § 8.1.1.

   En ausencia de este componente, el significado por defecto es *no limitado.*

3) **Filtro**(F): La notación de sintaxis abstracta de **filtro** se da en el § 8.1.2.

   En ausencia de este componente, el significado por defecto es *todas las inscripciones dentro de la gama especificada.*

4) **Límite** (F): Permite la especificación de un límite superior al número de inscripciones que deberán seleccionarse.

   En ausencia de este componente, se devolverán todas las inscripciones seleccionadas.

   Nota – La finalidad primaria del límite es impedir que, en una operación abstracta, como consecuencia de selecciones mal formuladas, se obtengan resultados enormes. Se puede utilizar también para presentar un número exacto de conjuntos de información de modo que sean adecuados para un determinado dispositivo de salida.

5) **Contraorden** (F): Si se requiere una contraorden de cualquiera de las **restricciones de captura**, tienen que estar presente los componentes correspondientes de **restricciones de contraorden**.

```
OverrideRestrictions ::= BIT STRING {
    overrideContentTypesRestriction    (0),
    overrideEITsRestriction            (1),
    overrideContentLengthRestriction   (2) } (SIZE (1 .. ub-information-bases))
```

Los bits de **restricciones a contraorden** tienen los significados siguientes:

a) **Restricción a tipos de contenido de contraorden** (O): Este bit debe ponerse a 1 si la **restricción a tipos de contenido** debe ser contraordenada.

Si este bit se pone a cero, se aplicarán las **restricciones a tipos de contenido** especificadas en la operación abstracta de vinculación.

b) **Restricción a contraordenar TIC** (O): Este bit tiene que ponerse a 1 si deberá contraordenarse **restricción a TIC**.

Si este bit se pone a cero, se aplicarán las **restricciones a TIC** especificadas en la operación abstracta de vinculación.

c) **Restricción a contraordenar longitud de contenido** (O): Este bit tiene que ponerse a 1 si la **restricción a longitud de contenido** ha de ser contraordenada.

Si este bit se pone a cero, se aplicarán las **restricciones a longitud de contenido** especificadas en la operación abstracta de vinculación.

En ausencia de **restricciones a contraordenar**, el significado por defecto es que se aplicarán todas las **restricciones de captura** especificadas en la operación abstracta de vinculación.

8.1.4 *Selección de información de inscripción*

Un parámetro de **selección de formación de inscripción** indica qué información de una inscripción se está solicitando.

```
EntryInformationSelection ::= SET SIZE (0 .. ub-per-entry) OF AttributeSelection
```

Un conjunto vacío indica que se solicita información sobre la propia inscripción, y no sobre los atributos de la inscripción.

```
AttributeSelection ::= SET {
        type    AttributeType,
        from    [0] INTEGER (1 .. ub-attribute-values) OPTIONAL -- used if type is multi valued --,
        count   [1] INTEGER (1 .. ub-attribute-values) OPTIONAL -- used if type is multi valued -- }
```

Los componentes de **selección de información de inscripción** tienen los siguientes significados:

1) **Tipo** (O): Indica el tipo-de-atributo del atributo.

2) **Desde** (F): Cuando el atributo tiene múltiples valores, este entero da la posición relativa del primer valor que ha de devolverse. Si especifica un valor más allá de los presentes en el atributo, no se devuelve ningún valor. Este componente sólo está presente si el tipo de atributo tiene múltiples valores. Si se omite, se devuelven los valores a partir del primer valor.

3) **Cómputo** (F): Cuando un atributo tiene múltiples valores, este entero da el número de valores a devolver. Si hay presentes en el atributo menos que cómputo, se devuelven todos los valores. Este atributo sólo está presente si el tipo de atributo es de múltiples valores. Si se omite, no hay límite para el número de valores que se devuelven.

8.1.5 *Información de inscripción*

Un parámetro **información de inscripción** lleva información seleccionada tomada de una inscripción.

```
EntryInformation ::= SEQUENCE {
        sequence-number         SequenceNumber,
        attributes              SET SIZE (1 .. ub-per-entry) OF Attribute OPTIONAL }
```

Los componentes de **información de inscripción** tienen los siguientes significados:

1) **Número secuencial** (O): Número secuencial que identifica la inscripción. Véase el § 6.3.2.2.

2) **Atributos** (F): Conjunto de atributos seleccionados tomados de la inscripción. Cuando se solicita expresamente por una petición de atributo parcial, un atributo seleccionado que está definido como multivaluado puede contener un subconjunto de todos los valores de atributo, en ese atributo, almacenados en la inscripción. Este parámetro está ausente si no se ha solicitado información procedente de los mensajes seleccionados, por ejemplo, cuando el usuario del servicio abstracto AM sólo desea los números secuenciales de los mensajes seleccionados.

8.2 *Operación abstracta de resumir*

La **operación abstracta de resumir** devuelve cómputos resumen de inscripciones seleccionadas en una base de información. Además de estos resúmenes, se devuelve también un cómputo de las inscripciones seleccionadas, y sus números secuenciales más bajos y más alto. Pueden solicitarse cero o más resúmenes individuales.

La **operación abstracta de resumir** sólo será correcta cuando la base de información permite el acceso de acuerdo con el contexto de seguridad y la política de seguridad en vigor.

Los atributos que pueden utilizarse para los resúmenes están restringidos. Para los atributos generales en la base de información de mensajes almacenados, las restricciones se indican en el cuadro 1/X.413.

```
Summarize ::= ABSTRACT-OPERATION
        ARGUMENT        SummarizeArgument
        RESULT          SummarizeResult
        ERRORS {
            AttributeError,
            InvalidParametersError,
            RangeError,
            SecurityError,
            SequenceNumberError,
            ServiceError }
```

Nota – En el anexo F se presenta un ejemplo de la operación abstracta.

8.2.1 *Argumento de resumir*

```
SummarizeArgument ::= SET {
        information-base-type [0] InformationBase DEFAULT stored-messages,
        selector              [1] Selector,
        summary-requests      [2] SEQUENCE SIZE (1 .. ub-summaries) OF AttributeType OPTIONAL
            -- ausente si no se solicitan resúmenes -- }
```

Los componentes de **argumento de resumir** tienen los siguientes significados:

1) **Tipo de base de información** (F): Especifica qué **base de información** es direccionada por la operación abstracta. Véase el § 6.3.1.

   En ausencia del componente **tipo de base de información,** el significado por defecto es mensajes almacenados.

2) **Selector** (F): Es un conjunto de criterios de selección para determinar que inscripciones han de resumirse. Véase el § 8.1.3.

3) **Peticiones de resúmenes** (F): Es la secuencia de tipos de atributo para la cual se solicitan resúmenes. Este parámetro sólo está presente si se solicita un resumen.

8.2.2 *Resultado de resumir*

En caso de éxito de la petición, se retornará el **resultado de resumir**.

```
SummarizeResult ::= SET {
        next        [0] SequenceNumber OPTIONAL,
        count       [1] INTEGER (0 .. ub-messages) } -- de las inscriciones seleccionadas --,
        span        [2] Span OPTIONAL -- de las inscripciones seleccionadas, omitidas si
                        cuenta es cero --,
        summaries   [3] Sequence SIZE (1 .. ub-summaries) OF Summary OPTIONAL)
```

Los componentes de **resultado de resumir** tienen los siguientes significados:

1) **Siguiente** (C): Se devuelve cuando el número de inscripciones seleccionadas sería mayor si no fuera por el límite especificado en el selector. El componente contiene el número secuencial para la inscripción siguiente que habrá sido seleccionada.

2) **Cómputo** (O): Es un entero que da el cómputo de las inscripciones que concordaron con los criterios de selección.

3) **Intervalo** (C): Contiene los números secuenciales más bajo y más alto de las inscripciones que concordaron con los criterios de selección. Si está ausente no hay tales inscripciones.

```
Span ::= SEQUENCE {
    lowest   [0] SequenceNumber,
    highest  [1] SequenceNumber }
```

Los componentes de **intervalo** tienen los siguientes significados:

a) **Más bajo** (O): Es el punto inicial de **intervalo**, dado como un número secuencial (véase el § 6.3.2.2).

b) **Más alto** (O): Es el punto final de **intervalo**, dado como un número secuencial (véase el § 6.3.2.2).

4) **Resúmenes** (C): Se devuelve un **resumen** para cada **petición de resumen**. Los **resúmenes** se devuelven en el orden en que fueron solicitados.

```
Summary ::= SET{
    absent   [0] INTEGER (1 .. ub-messages) OPTIONAL -- count of entries where the attribute is
                 absent --,
    present  [1] SET SIZE (1 .. ub-attribute-values) OF -- one for each attribute value present --
                     SEQUENCE{
                         type     AttributeType,
                         value    ANY DEFINED BY type,
                         count    INTEGER (1 .. ub-messages)} OPTIONAL}
```

Los componentes de **resumen** tienen los siguientes significados:

a) **Ausente** (C): Cómputo de las inscripciones que no contienen ningún atributo o tipo de atributo especificado en la petición. Se omite si no hay tales inscripciones.

b) **Presente** (C): Resumen de las inscripciones que contienen algún atributo del tipo de atributo especificado, descompuesto por los valores de atributo presentes efectivamente. Se omite si no hay tales inscripciones.

Los componentes de **presente** tienen los siguientes significados:

i) **Tipo** (O): Tipo del atributo.

ii) **Valor** (O): Valor del atributo para el que se da el cómputo.

iii) **Cómputo** (O): Cómputo de inscripciones con su valor de atributo.

8.2.3 *Errores abstractos de resumir*

En caso de fracaso de la petición, se informa uno de los errores abstractos listados. Las circunstancias en que se notificarán los errores abstractos particulares se definen en el § 9.

8.3 *Operación abstracta-listado*

La **operación abstracta-listado** se utiliza para explorar una base de información seleccionada a fin de buscar inscripciones de interés y devolver la información seleccionada a dichas inscripciones.

La **operación abstracta-listado** sólo tendrá éxito cuando la base de la información permita el acceso conforme al contexto de seguridad y a la política de seguridad en vigor.

La información que puede seleccionarse para las inscripciones en una base de información puede estar restringida. Para los atributos generales en la base de información de mensajes almacenados, las restricciones se indican en el cuadro 1/X.413.

```
List ::= ABSTRACT-OPERATION
         ARGUMENT      ListArgument
         RESULT        ListResult
         ERRORS{
             AttributeError,
             InvalidParametersError,
             RangeError,
             SecurityError,
             SequenceNumberError,
             ServiceError}
```

8.3.1 *Argumento de listado*

```
ListArgument ::= SET{
         information-base-type    [0] InformationBase DEFAULT stored-messages,
         selector                 [1] Selector,
         requested-attributes     [3] EntryInformationSelection OPTIONAL}
```

Los componentes de **argumento de listado** tienen los siguientes significados:

1) **Tipo de base de información** (F): Especifica qué base de información es seleccionada por la operación abstracta. Véase el § 6.3.1.

   En ausencia del componente **tipo base de información**, el significado por defecto es mensajes almacenados.

2) **Selector** (O): Conjunto de criterios de selección para determinar que inscripciones han de devolverse. Véase el § 8.2.3.

3) **Atributos solicitados** (F): Indica qué información, de las inscripciones seleccionadas, debe devolverse en el resultado. Véase el § 8.1.4.

   Si este parámetro está ausente, se utiliza el conjunto registrado de los **significados por defecto atributo de listado**. Para más información sobre los significados por defecto, véase el § 8.6.1.

8.3.2 *Resultado de listado*

Si tiene éxito la petición, se devolverá **resultado de listado.**

```
ListResult ::= SET{
        next        [0] SequenceNumber OPTIONAL,
        requested   [1] SEQUENCE SIZE (1..ub-messages) OF EntryInformation OPTIONAL -- omitted
                        if none found -- }
```

Los componentes de **resultado de listado** tienen los siguientes significados:

1) **Siguiente** (C): Se devolverá en el caso en que el número de inscripciones seleccionadas sería mayor si no fuese por el límite especificado en el selector. El componente contiene el número secuencial para la siguiente inscripción que se habría seleccionado.

2) **Seleccionado** (C): Transporta la información de inscripción solicitada (véase el § 8.1.5) a partir de cada inscripción seleccionada (una o más), en orden ascendente del número secuencial. No está presente en el caso en que se efectuó una búsqueda y no se seleccionó ninguna inscripción.

8.3.3 *Errores abstractos de listado*

En caso de fracaso de la petición, se notificará uno de los errores abstractos de listado. Las circunstancias en las cuales se notifican los distintos errores abstractos se definen en el § 9.

8.4 *Operación abstracta de captura*

La **operación abstracta de captura** se utiliza para devolver información seleccionada a partir de una inscripción específica en una base de información. Alternativamente, se utiliza para devolver información seleccionada a partir de la primera inscripción entre varias inscripciones de interés; en este caso se devuelven también los números secuenciales de las otras inscripciones seleccionadas. La **operación abstracta de captura** sólo tendrá éxito cuando se soliciten bases de información permitidas por el contexto de seguridad y la política de seguridad en vigor.

Una información de una inscripción puede ser capturada varias veces, hasta que la inscripción sea suprimida explícitamente por una operación abstracta de supresión.

```
Fetch ::= ABSTRACT-OPERATION
        ARGUMENT        FetchArgument
        RESULT          FetchResult
        ERRORS{
            AttributeError,
            FetchRestrictionError,
            InvalidParametersError,
            RangeError,
            SecurityError,
            SequenceNumberError,
            ServiceError }
```

8.4.1 *Argumento de captura*

```
FetchArgument ::= SET{
        information-base-type   [0] InformationBase DEFAULT stored-messages,
        item                        CHOICE{
            search                      [1] Selector,
            precise                     [2] SequenceNumber },
        requested-attributes    [3] EntryInformationSelection OPTIONAL }
```

Los componentes de **argumento de captura** tienen los siguientes significados:

1) **Tipo de base de información** (F): Especifica qué base de información es direccionada por la operación abstracta. Véase el § 6.3.1.

   En ausencia del tipo de base de información, el significado por defecto es mensajes almacenados.

2) **Elemento** (O): Debe especificarse uno de los componentes descritos más abajo para determinar qué inscripción ha de capturarse:

   a) **Búsqueda** (C): Es un selector que especifica un conjunto de inscripciones de las cuales la que tiene el número secuencial más bajo es la inscripción que debe capturarse. Véase el § 8.1.3.

   b) **Precisión** (C): Es el número secuencial de la inscripción que debe capturarse. Véase el § 6.3.2.2.

3) **Atributos solicitados** (F): Indica qué información de la inscripción seleccionada ha de devolverse en el resultado. Véase el § 8.1.4.

   Si este parámetro está ausente, se utiliza el conjunto registrado de los significados por **defecto del atributo de captura**. Para más información sobre los significados por defecto, véase el § 8.6.1.

8.4.2 *Resultado de captura*

Si la petición tiene éxito, se retornará el **resultado de captura**.

```
FetchResult ::= SET{
        entry-information   [0] EntryInformation OPTIONAL -- if an entry was selected --,
        list                [1] SEQUENCE SIZE (1 .. ub-messages) OF SequenceNumber
                                OPTIONAL,
        next                [2] SequenceNumber OPTIONAL }
```

Los componentes de **resultado de captura** tienen los siguientes significados:

1) **Información de inscripción** (C): Es un conjunto de atributos, de la inscripción, tal como fueron solicitados en el argumento. Véase el § 8.1.5. No está presente en el caso que se efectúa una búsqueda y no se selecciona ninguna inscripción.

2) **Lista** (C): Se devuelve cuando se efectuó una búsqueda y se encontraron más de una inscripción que concordaba con el selector de la búsqueda. La lista de los números secuenciales, en orden ascendente, de estas inscripciones ulteriores.

3) **Siguiente** (C): Se devuelve en el caso en que el número de inscripciones seleccionadas sería mayor si no fuese por el límite especificado en el selector. El componente contiene el número secuencial para la siguiente inscripción que se habría seleccionado.

8.4.3 *Errores abstractos de captura*

En caso de fracaso de la petición, se notificará uno de los errores abstractos listados. Las circunstancias en las cuales se notifican los distintos errores abstractos se definen en el § 9.

8.5 *Operación abstracta de supresión*

La **operación abstracta de supresión** se utiliza para suprimir inscripciones seleccionadas en una base de datos. Una inscripción principal y todas las inscripciones vástagos que dependen de la misma sólo pueden ser suprimidas conjuntamente. Esto se efectúa especificando simplemente la inscripción principal como argumento. La operación abstracta de supresión sólo tendrá éxito cuando opere sobre las bases de información permitidas por el contexto de seguridad y la política de seguridad en vigor.

Para bases de información específicas, puede haber restricciones a las inscripciones que podrían suprimirse. Además, pueden efectuarse acciones específicas del contenido, definidas en la Recomendación correspondiente que define el tipo contenido. En lo que respecta a los mensajes almacenados, no puede suprimirse ninguna inscripción, si el estado de esa inscripción (véase el § 6.4) es «nuevo».

```
Delete ::= ABSTRACT-OPERATION
        ARGUMENT            DeleteArgument
        RESULT              DeleteResult
        ERRORS{
            DeleteError,
            InvalidParametersError,
            RangeError,
            SecurityError,
            SequenceNumberError,
            ServiceError }
```

8.5.1 *Supresión argumento*

```
DeleteArgument ::= SET{
        information-base-type    [0] InformationBase DEFAULT stored-messages,
        items                        CHOICE{
            selector                     [1] Selector
            sequence-numbers             [2] SET SIZE (1 .. ub-messages) OF SequenceNumber}}
```

Los componentes de **supresión argumento** tienen los siguientes significados:

1) **Tipo de base de información** (O): Especifica qué base de información es direccionada por la operación abstracta. Véase el § 6.3.1.

   En la ausencia del componente **tipo de base de información**, el significado por defecto es mensajes almacenados.

2) **Elementos** (O): Para determinar las inscripciones que han de suprimirse hay que especificar uno de los componentes descritos a continuación:

   a) **Selector** (C): Véase el § 8.1.3.

   b) **Números secuenciales** (C): Una lista no ordenada de **números secuenciales**. Véase el § 6.3.2.2.

8.5.2 *Resultado de supresión*

Si la petición tiene éxito, se retornará el **resultado de supresión**. No existen parámetros.

```
DeleteResult ::= NULL
```

8.5.3 *Errores abstractos de supresión*

En caso de fracaso de la petición, se notificará uno de los errores abstractos listados. Las circunstancias en las cuales se informan los distintos errores abstractos se definen en el § 9.

8.6 *Operación abstracta de registro en AM*

La operación abstracta de registro en AM se utiliza para registrar o eliminar diversas informaciones en el AM:

a) acciones automáticas;

b) lista por defecto de tipos de atributo;

c) nuevas credenciales;

d) nuevo conjunto de etiquetas de seguridad de usuario.

```
Register-MS ::= ABSTRACT-OPERATION
    ARGUMENT Register-MSArgument
    RESULT   Register-MSResult
    ERRORS{
        AtrributeError,
        AutoActionRequestsError,
        InvalidParametersError,
        SecurityError,
        ServiceError}
```

8.6.1 *Argumento de registro en AM*

```
Register-MS Arguments := SET{
        auto-action-registrations       [0] SET SIZE (1 .. ub-auto-registrations) OF AutoActionRegistra-
                                            tion OPTIONAL,
        auto-action-deregistrations     [1] SET SIZE (1 .. ub-auto-registrations) OF AutoActionDere-
                                            gistration OPTIONAL,
        list-attribute-defaults         [2] SET SIZE (1 .. ub-default-registrations) OF Attribute Type
                                            OPTIONAL,
        fetch-attribute-defaults        [3] SET SIZE (1 .. ub-default-registrations) OF Attribute Type
                                            OPTIONAL,
        change-credentials              [4] SEQUENCE{
            old-credentials                 [0] IMPLICIT Credentials,
            new-credentials                 [1] IMPLICIT Credentials} OPTIONAL
              -- misma selección que para las credenciales viejas --,
        user-security-labels            [5] SET SIZE (1 .. ub-labels-and-redirections) OF SecurityLabel
                                            OPTIONAL}
```

Los componentes de argumento de registro en AM tienen los siguientes significados:

1) **Registro de acciones automáticas** (F): Es un conjunto de **registros de acción automática** (véase el § 6.5.1), uno para cada acción automática a registrar. El **parámetro registro de acción automática** nuevo prevalece sobre cualquier acción automática registrada anteriormente (si la hubiere) con ese **identificador de registro** y **tipo de acción automática.**

   En ausencia el valor por defecto de **registros de acciones automáticas**, es que no se registra ninguna nueva acción automática.

2) **Eliminaciones de acciones automáticas** (F): Es un conjunto de **eliminación de acción automática**, una para cada acción automática a eliminar. Es eliminada toda acción automática cuyo **identificador de registro** y **tipo de acción automática** concuerdan con los que figuran en una **eliminación de acción automática.**

   AutoActionDeregistration ::= AutoActionRegistration
   (WITH COMPONENTS { ..., registration-parameter ABSENT })

   En ausencia de **eliminaciones de acciones automáticas**, el significado por defecto es que ninguna acción automática registrada sea eliminada.

3) **Valores por defecto de atributos de listado** (F): Especifica un conjunto por defecto de tipos de atributos para indicar qué atributos deben devolverse para cualquier ulterior operación abstracta de listado o alerta si el argumento selección de información de inscripción está ausente.

   En ausencia de **valores por defecto de atributos de listado**, el significado por defecto es que no hay cambios en el valor por defecto registrado (si lo hubiere). **Valores por defecto de atributos de listado** es un conjunto vacío hasta que el usuario AM lo cambie explícitamente por medio de la operación abstracta de registro en el AM.

4) **Valores por defecto de atributos de captura** (F): Especifica un conjunto por defecto de tipos de atributo para indicar qué atributos deben devolverse para cualquier ulterior operación abstracta de captura si está ausente el argumento selección de información de asiento.

   En ausencia de **valores por defecto de atributos de captura**, el significado por defecto es que no se cambia el valor por defecto registrado (si no hubiere). **Valores por defecto de atributos de captura** es un conjunto vacío hasta que el usuario AM lo cambie explícitamente por medio de la operación abstracta de registro en el AM.

5) **Cambio de credenciales** (F): Las credenciales viejas y las nuevas, si se solicita **cambio de credenciales.**

   Las **credenciales viejas** son las credenciales que tiene actualmente un usuario, y las **credenciales nuevas** son las credenciales que el usuario querría tener.

   En ausencia de este argumento, el significado por defecto es que las credenciales registradas anteriormente se mantienen sin modificación.

   Las credenciales del usuario AM pueden diferir de las **credenciales del iniciador** detalladas en el § 8.1.1.1.1.2 de la Recomendación X.411.

6) **Etiquetas de seguridad de usuario** (F): Contiene las **etiquetas de seguridad** del usuario del servicio abstracto AM, si han de cambiarse. Puede ser generado por el usuario del servicio abstracto AM.

   En ausencia de este argumento, las **etiquetas de seguridad de usuario** se mantienen sin modificación.

   Obsérvese que algunas **políticas de seguridad** sólo permiten que las **etiquetas de seguridad de usuario** se cambien de esta manera si se emplea un enlace seguro. Pueden preverse otros medios locales de cambiar las **etiquetas de seguridad de usuario** de una manera segura. Las **etiquetas de seguridad de usuario** se definen en el § 8.4.1.1.1.7 de la Recomendación X.411.

   La **etiqueta de seguridad** se define en el § 9 de la Recomendación X.411.

8.6.2 *Resultado de registro en el AM*

Si la petición tiene éxito, se devolverá el resultado de registro en el AM. No hay parámetros.

Register-MSResult ::= NULL

8.6.3 *Errores abstractos de registrar en el AM*

Si la petición fracasa, se notificará uno de los errores abstractos listados. Las circunstancias en las que se notificarán los distintos errores abstractos se definen en el § 9.

8.7 *Operación abstracta de alerta*

La **operación abstracta de alerta** habilita al proveedor del servicio abstracto AM para informar inmediatamente al usuario del servicio abstracto AM sobre una nueva inscripción que ha sido introducida en el AM, cuyos atributos concuerdan con los criterios de selección de uno de los **registros de alerta automática** (véase el § 12.2) suministrados anteriormente utilizando la operación abstracta de registro en el AM (véase el § 8.6).

La **operación abstracta de alerta** puede ser invocada durante una asociación abstracta existente iniciada por el AU, y solamente como un resultado de inscripciones nuevas que han sido creadas después del establecimiento de la asociación abstracta.

Las inscripciones que concuerden con los criterios de selección que han sido creados entre asociaciones abstractas se indicarán en el resultado de la siguiente operación abstracta de vinculación para la asociación abstracta. Para estas inscripciones no se invocará ninguna **operación abstracta de alerta**. Véase el § 7.

La **operación abstracta de alerta** sólo tendrá éxito cuando la base de información permita el acceso de acuerdo con el contexto de seguridad y la política de seguridad en vigor.

```
Alert ::= ABSTRACT-OPERATION
          ARGUMENT        AlertArgument
          RESULT          AlertResult
          ERRORS {
              SecurityError }
```

8.7.1 *Argumento de alerta*

```
AlertArgument ::= SET {
          alert-registration-identifier    [0] INTEGER (1 .. ub-auto-actions),
          new-entry                        [2] EntryInformation OPTIONAL }
```

Los componentes del **argumento de alerta** tienen los siguientes significados:

1) **Identificador de registro de alerta** (O): Identifica cuál de los **registros de alertas automáticas** produjeron la alerta (véanse los § 6.4 y 12.2).
2) **Inscripción nueva** (F): Contiene la información de la inscripción nueva que fue solicitada en el **parámetro registro de alerta automática** (véase el § 12.2). Está ausente cuando el usuario del servicio abstracto AM nó especificó un **registro de alerta automática**.

8.7.2 *Resultado de alerta*

Si la petición tiene éxito, se devolverá el resultado de alerta.

```
AlertResult ::= NULL
```

8.7.3 *Errores abstractos de alerta*

Si la petición fracasa, se notificará uno de los errores abstractos listados. Las circunstancias en las cuales se notifican los distintos errores abstractos se definen en el § 9.

9 Errores abstractos

Este punto define los siguientes errores abstractos asociados con el uso de operaciones abstractas en el puerto de extracción:

a) ErrorDeAtributo;
b) ErrorDePeticiónDeAcciónAutomática;
c) ErrorDeSupresión;
d) ErrorDeRestricciónACaptura;
e) ErrorDeParámetrosInválidos;
f) ErrorDeGama;
g) ErrorDeSeguridad;
h) ErrorDeServicio;
i) ErrorDeNúmeroSecuencial.

9.1 *Precedencia de los errores*

El realizador de una operación abstracta no está obligado a continuar el procesamiento del mensaje más allá del punto en que se detectó un error. Esto permite a una realización la elección de si va o no a continuar el procesamiento de errores.

Nota – Una implicación de esta regla es que el primer error encontrado puede ser diferente en casos repetidos de la misma operación abstracta, pues no tiene necesariamente que existir un orden lógico específico en el cual procesar los distintos casos de la operación abstracta.

9.2 *Error de atributo*

Un **error de atributo** notifica un problema relacionado con un atributo.

```
AttributeError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problems [0] SET SIZE (1 .. ub-per-entry) OF SET{
                problem     [0] AttributeProblem,
                type        [1] AttributeType,
                value       [2] ANY DEFINED BY type OPTIONAL}}

AttributeProblem ::= INTEGER{
        invalid-attribute-value             (0),
        unavailable-attribute-type          (1),
        inappropriate-matching              (2),
        attribute-type-not-subscribed       (3),
        inappropriate-for-operation         (4)} (0 .. ub-error-reasons)
```

El parámetro tiene el siguiente significado:

1) **Problemas** (O): Los problemas concretos encontrados. Puede indicarse un número cualquiera de problemas individuales, cada uno de los cuales irá acompañado de una indicación del tipo de atributo, y, si fuese necesario para evitar la ambigüedad, del valor que causó el problema:
   a) **Valor de atributo no válido** (C): Un valor de atributo contemplado especificado como argumento de la operación abstracta no se ajusta al tipo de datos definido para el tipo de atributo en cuestión.
   b) **Tipo de atributo no disponible** (C): Un tipo de atributo contemplado utilizado como un argumento de la operación abstracta no es uno de los admitidos por el proveedor del servicio abstracto AM. Si el proveedor del servicio abstracto AM puede, de todas formas, realizar la operación, no está prohibido que lo haga.
   c) **Concordancia inapropiada** (C): El filtro contiene un elemento de filtro en el cual un atributo se hace concordar utilizando una operación (igualdad, ordenamiento, o subcadenas) que no está definida para ese atributo.
   d) **Tipo de atributo no abonado** (C): Un tipo de atributo utilizado como un argumento de la operación abstracta no es uno de los tipos a que está abonado el usuario del servicio abstracto AM.

      Nota – Un cambio en el abono no se refleja necesariamente en los atributos presentes en una inscripción creada antes del cambio.
   e) **Inapropiado para operación** (C): Un tipo de atributo utilizado como un argumento de la operación abstracta es inadecuado para el uso requerido.

9.3 *Error de petición de acción automática*

Un **error de petición de acción automática** notifica un problema relacionado con el registro de una acción automática.

```
AutoActionRequestError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problems [0]        SET SIZE (1 .. ub-auto-registrations) OF SET{
                problem         [0] Auto-ActionRequestProblem,
                type            [1] AutoActionType}}

AutoActionRequestProblem ::= INTEGER{
        unavailable-auto-action-type        (0),
        auto-action-type-not-subscribed     (1)} (0 .. ub-error-reasons)
```

El parámetro tiene el siguiente significado:

1) **Problemas** (O): Los problemas concretos encontrados. Puede indicarse cualquier número de problemas individuales, cada uno de los cuales va acompañado de una indicación del **tipo de acción automática** que causó el problema:
   a) **Tipo de acción automática no disponible** – Un tipo de acción automática utilizado como un argumento de la operación abstracta no es uno de los admitidos por el proveedor del servicio abstracto AM.

b) **Tipo de acción no abonado** – Un tipo de acción utilizado como un argumento de la operación abstracta no es uno de los tipos a que está abonado el usuario del servicio abstracto AM.

9.4 *Error de supresión*

Un **error de supresión** notifica un problema que se presenta al tratar de suprimir una o más inscripciones en una base de información.

```
DeleteError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problems [0] SET SIZE (1 .. ub-messages) OF SET{
                problem          [0] DeleteProblem,
                sequence-number  [1] SequenceNumber}}

DeleteProblem ::= INTEGER{
        child-entry-specified           (0),
        delete-restriction-problem      (1)} (0 .. ub-error-reasons)
```

El parámetro tiene el siguiente significado:

1) **Problema** (O): Los problemas concretos encontrados. Puede indicarse cualquier número de problemas individuales, cada uno de los cuales va acompañado de una indicación del número secuencial de la inscripción que causó el problema:

   a) **Inscripción vástago especificada**: Se ha tratado de suprimir una inscripción vástago.

   b) **Problema de restricción a supresión**: Se ha tratado de violar una restricción especificada para la operación abstracta de supresión (véase el § 8.5).

9.5 *Error de restricción a captura*

Un **error de restricción a captura** informa sobre una tentativa de violar una restricción asociada con la operación abstracta de captura.

```
FetchRestrictionError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problems [0] SET SIZE (1 .. ub-default-registrations) OF SET{
                problem          [3] FetchRestrictionProblem,
                restriction      CHOICE{
                  content-type       [0] ContentType,
                  eit                [1] MS-EITs,
                  content-length     [2] ContentLength}}}

FetchRestrictionProblem ::= INTEGER{
        content-type-problem            (1),
        eit-problem                     (2),
        content-length-problem          (3)} (0 .. ub-error-reasons)
```

El parámetro tiene el siguiente significado:

1) **Problemas** (O): Los problemas concretos encontrados. Puede indicarse cualquier número de problemas individuales, cada uno de los cuales va acompañado de una indicación del tipo de contenido infractor, del tipo de información codificada o de la longitud del contenido que causó el problema:

   a) **Problema de tipo de contenido** (C): El tipo de contenido del mensaje que se está capturando no está permitido por las restricciones a captura actualmente en vigor.

   b) **Problema de TIC** (C): Los tipos de información codificada solicitados en la operación abstracta de captura no están permitidos por las restricciones a captura actualmente en vigor.

   c) **Problema de longitud de contenido** (C): La longitud de contenido del mensaje que se está capturando es mayor que la autorizada por las restricciones a captura actualmente en vigor.

9.6 *Error de parámetro no válido*

Un **error de parámetro no válido** notifica un problema de semántica en el conjunto de parámetros recibidos. Este error se utilizaría, por ejemplo, para notificar que un parámetro opcional estaba presente en un contexto incorrecto, o para notificar que uno de los parámetros tiene un valor inadecuado.

```
InvalidParametersError ::= ABSTRACT-ERROR
        PARAMETER  NULL
```

Este error no tiene parámetros.

9.7 *Error de gama*

Un **error de gama** notifica un problema relacionado con el límite especificado en un selector como un argumento a una operación abstracta.

```
RangeError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problem         [0] RangeProblem }

RangeProblem ::= INTEGER{
        reversed                (0)} (0)..ub-error-reasons}
```

El parámetro tiene el significado siguiente:

1) **Problemas** (O): Los problemas concretos encontrados:
   a) **Invertido** (C): El límite superior indicaba un número secuencial o una hora de creación anterior al indicado por el límite inferior.

9.8 *Error de seguridad*

Un **error de seguridad** notifica que la operación abstracta solicitada no puede proporcionarse porque violaría la política de seguridad en vigor. Este error se define en la Recomendación X.411.

9.9 *Error de número secuencial*

Un **error de número secuencial** notifica un problema relacionado con el número secuencial especificado en un argumento de una operación abstracta.

```
SequenceNumberError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problems [1] SET SIZE (1..ub-messages) OF SET{
                problem         [0] SequenceNumberProblem,
                sequence-number [1] SequenceNumber}}

SequenceNumberProblem ::= INTEGER{
        no-such-entry           (0)} (0..ub-error-reasons)
```

El parámetro tiene el siguiente significado:

1) **Problemas** (O): Los problemas concretos encontrados. Puede indicarse un número cualquiera de problemas individuales, cada uno de los cuales va acompañado de una indicación de los números secuenciales que causaron el problema:
   a) **No hay tal inscripción**: El número secuencial suministrado no concuerda con el de ninguna inscripción en la base de información.

9.10 *Error de servicio*

Un **error de servicio** notifica un error relacionado con la prestación del servicio.

```
ServiceError ::= ABSTRACT-ERROR
        PARAMETER SET{
            problem             [0] ServiceProblem }

ServiceProblem ::= INTEGER{
        busy                    (0),
        unavailable             (1),
        unwilling-to-perform    (2)}(0..ub-error-reasons)
```

Este parámetro tiene el siguiente significado:

1) **Problema** (O): El problema concreto encontrado:
   a) **Ocupado** (C): El AM, o una parte de éste, está en este momento demasiado ocupado para realizar la operación abstracta solicitada, pero puede no estarlo en breve.
   b) **No disponible** (C): El AM, o alguna parte del mismo, está indisponible en este momento.
   c) **No dispuesto a funcionar** (C): El AM no está preparado para ejecutar esta petición porque conduciría a un consumo excesivo de recursos.

SECCIÓN 3 – TIPOS DE ATRIBUTOS GENERALES Y TIPOS DE ACCIONES AUTOMÁTICAS GENERALES

10 Visión de conjunto

El modelo de información AM y los conceptos de **atributo** y de **acción automática** ya fueron presentados en los § 6.3.3 y 6.5. El § 11 define los **tipos de atributo generales** que se especifican para AM. El § 12 define los **tipos de acción automática generales** especificados para AM.

11 Tipos de atributos generales

Los **tipos de atributos generales** son válidos para todos los tipos de contenido mensaje. Otros tipos de atributo, que son específicos al contenido, se definen en sus respectivas Recomendaciones, por ejemplo los tipos de atributo específicos al SMIP para AM se definen en el anexo C de la Recomendación X.420.

11.1 *Visión de conjunto de los tipos de atributos generales*

Los **atributos generales** que pueden presentarse en una inscripción de base de información de mensajes almacenados se enumeran en el cuadro 1/X.413. Están constituidos principalmente a partir de la información de los parámetros de las operaciones abstractas entrega de mensajes (MessageDelivery) y entrega de informe (ReportDelivery) del servicio abstracto STRM definido en el § 8 de la Recomendación X.411 y esos atributos son denominados correspondientemente. Algunos **atributos generales** son generados y otros son simplemente conservados por el AM.

El cuadro 1/X.413 define los diversos **atributos generales** y para cada tipo de atributo define lo siguiente:

- si el tipo de atributo tiene un solo valor o tiene valores múltiples;
- si es admitido o no por el AM y si el acceso al AU es obligatorio o facultativo;
- si el tipo de atributo siempre está presente, está presente de forma condicional, o está ausente en una inscripción de mensaje entregado, en una inscripción de informe entregado, o en una inscripción de contenido devuelto;
- si el tipo de atributo puede ser devuelto o no en una operación abstracta de listado o alerta;
- si el tipo de atributo puede o no ser utilizado en una operación abstracta de resumir.

  Nota – Únicamente para los tipos de datos NSA.1 simples.

Para una descripción detallada de la clasificación del cuadro 1/X.413, véanse los convenios del § 5.2.

Un AM admite un tipo de atributo facultativo únicamente si hay un abono correcto al soporte de ese atributo (lo que implica que el AM y el AU que accede admiten dicho atributo). El abono a tipos de atributos facultativos puede hacerse para cada tipo de atributo, para cada AU.

11.2 *Descripción de los tipos de atributos generales*

Los siguientes puntos contienen una breve descripción de cada **tipo de atributo general** junto con su sintaxis abstracta utilizando la macro ATRIBUTE descrita en el § 6.3.

Debe señalarse que algunos **atributos generales** se utilizan básicamente para filtrar y listar, mientras que otros pueden contener información más compleja (tipos de datos NSA.1 más estructurados) y potencialmente voluminosa. Sólo pocos **atributos generales** resultan adecuados para los resúmenes.

11.2.1 *Números secuenciales de vástago*

Este atributo general, que tiene valores múltiples, contiene uno o más «punteros» hacia el nivel siguiente de inscripciones vástagos, si los hay. Es generado por el AM. Está presente en una progenitora que tiene una o más inscripciones vástagos asociadas. Está ausente en una inscripción que no tiene inscripciones vástagos.

```
ms-child-sequence-numbers ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MULTI VALUE
        ::= id-att-child-sequence-numbers
```

CUADRO 1/X.413

Tipos de atributos generales para mensajes almacenados

Nombre del tipo de atributo	Valor único o múltiples valores	Nivel de apoyo por AM y acceso al AU	Presencia en inscripción de mensaje entregado	Presencia en inscripción de informe entregado	Presencia en inscripción de contenido devuelto	Disponible para listado alerta	Disponible para resumir
Números secuenciales de vástago	M	O	C	C	C	Y	N
Contenido	S	O	P	–	P	N	N
Identificador del algoritmo de confidencialidad de contenido	S	F	C	–	–	Y	N
Correlacionador de contenido	S	F	–	C	–	Y	N
Identificador de contenido	S	F	C	C	–	Y	N
Verificación de integridad del contenido	S	F	C	–	–	Y	N
Longitud del contenido	S	F	P	–	P	Y	N
Devolución del contenido	S	F	–	P	–	Y	Y
Tipo de contenido	S	O	P	C	C	Y	Y
Prohibición de conversión con pérdida	S	F	C	–	–	Y	N
TIC convertidos	M	F	C	–	–	Y	N
Hora de creación	S	O	P	P	P	Y	N
TIC entregados	M	F	P	–		Y	N
Banderas de entrega	S	F	P	–	–	Y	N
Historia de la ampliación de la LD	M	F	C	C	–	Y	N
Estado de la inscripción	S	O	P	P	P	Y	Y
Tipo de inscripción	S	O	P	P	P	Y	Y
Nombre de destinatario deseado	S	F	C	–	–	Y	N
Sobre de entrega de mensaje	S	O	P	–	–	N	N
Identificador de entrega de mensaje	S	F	P	–	–	Y	N
Hora de entrega de mensaje	S	F	P	–	–	Y	N
Verificación de autenticación de origen del mensaje	S	F	C	–	–	Y	N
Etiqueta de seguridad del mensaje	S	F	C	C	–	Y	N
Hora de depósito del mensaje	S	F	P	–	–	Y	N
Testigo de mensaje	S	F	C	–	–	Y	N
TIC originales	M	F	C	C	–	Y	N
Certificado de originador	S	F	C	–	–	Y	N
Nombre de originador	S	F	P	–	–	Y	N
Nombres de otros destinatarios	M	F	C	–	–	Y	N
Número secuencial de progenitor	S	O	C	–	P	Y	N
Campos de entrega del informe por cada destinatario	M	O	–	P	–	Y	N
Prioridad	S	F	P	–	–	Y	Y
Petición de prueba de entrega	S	F	C	–	–	Y	N
Historia del redireccionamiento	M	F	C	–	–	Y	N
Sobre de la entrega de informe	S	O	–	P	–	N	N
Nombre de la LD informante	S	F	–	C	–	Y	N
Certificado del ATM informante	S	F	–	C	–	Y	N
Verificación de autenticación del origen del informe	S	F	C	C	–	Y	Y
Clasificación de seguridad	S	F	C	C	–	Y	Y
Número secuencial	S	O	P	P	P	Y	N
Identificador de depósito de asunto	S	O	–	P	–	Y	N
Nombre de este receptor	S	F	P	–	–	Y	N

11.2.2 *Contenido*

Este atributo general contiene el contenido completo de un mensaje tal como lo entrega la operación abstracta entrega de mensaje o bien se presenta como un contenido devuelto por la operación abstracta entrega de informe. Para mayores detalles véanse los § 8.2.1.1.1.37 y 8.3.1.2.1.14 de la Recomendación X.411.

ms-content ATTRIBUTE
WITH ATTRIBUTE-SYNTAX Content
SINGLE VALUE
::= id-att-content

11.2.3 *Identificador de algoritmo de confidencialidad del contenido*

Este atributo general contiene el **identificador de algoritmo** utilizado por el originador del mensaje para cifrar el contenido del mensaje. Puede ser generado por el originador del mensaje. Para detalles adicionales véase el § 8.5.10 de la Recomendación X.411.

mt-content-confidentiality-algorithm-identifier ATTRIBUTE
WITH ATTRIBUTE-SYNTAX AlgorithmIdentifier
SINGLE VALUE
::= id-att-content-confidentiality-algorithm-identifier

11.2.4 *Correlación de contenido*

Este atributo general contiene información que permite la correlación del contenido del mensaje. Puede ser generado por el AU de origen. Para detalles adicionales véase el § 8.2.1.1.1.36 de la Recomendación X.411.

mt-content-correlator ATTRIBUTE
WITH ATTRIBUTE-SYNTAX ContentCorrelator
MATCHES FOR EQUALITY
SINGLE VALUE
::= id-att-content-correlator

11.2.5 *Identificador de contenido*

Este atributo general contiene un identificador para el contenido del mensaje. Puede ser generado por un AU de origen. Para detalles adicionales véase el § 8.2.1.1.1.35 de la Recomendación X.411.

mt-content-identifier ATTRIBUTE
WITH ATTRIBUTE-SYNTAX ContentIdentifier
MATCHES FOR EQUALITY
SINGLE VALUE
::= id-att-content-identifier

11.2.6 *Verificación de integridad del contenido*

Este atributo general proporciona a los destinatarios del mensaje una forma de validar que el contenido del mensaje no ha sido modificado. Puede ser generado por el originador del mensaje y puede especificar un valor diferente para cada destinatario del mensaje. Para detalles adicionales véase el § 8.2.1.1.28 de la Recomendación X.411.

mt-content-integrity-check ATTRIBUTE
WITH ATTRIBUTE-SYNTAX ContentIntegrityCheck
SINGLE VALUE
::= id-att-content-integrity-check

11.2.7 *Longitud del contenido*

Este atributo general proporciona la longitud en octetos del contenido de un mensaje como fue entregado por la operación abstracta entrega de mensaje o de un contenido devuelto (si lo hay) notificado por la operación abstracta entrega de informe. Cuando no hay tal contenido devuelto, el atributo está ausente. Es generado por el AM.

ms-content-length ATTRIBUTE
WITH ATTRIBUTE-SYNTAX ContentLength
MATCHES FOR ORDERING
SINGLE VALUE
::= id-att-content-length

11.2.8 *Contenido devuelto*

Este atributo general indica si el contenido ha sido devuelto en la operación abstracta entrega de informe. Es generado por el AM.

ms-content-returned ATTRIBUTE
WITH ATTRIBUTE-SYNTAX BOOLEAN
MATCHES FOR EQUALITY
SINGLE VALUE
::= id-att-content-returned

11.2.9 *Tipo de contenido*

Este atributo general es generado a partir del tipo de contenido en la operación abstracta entrega de mensaje o entrega de informe. Véase también el § 8.2.1.1.1.34 de la Recomendación X.411.

mt-content-type ATTRIBUTE
WITH ATTRIBUTE-SYNTAX OBJECT IDENTIFIER
MATCHES FOR EQUALITY
SINGLE VALUE
::= id-att-content-type

11.2.10 *Prohibición de conversión con pérdida*

Este atributo general contiene información sobre si está permitida o prohibida la conversión con pérdida de información. Para detalles adicionales véase el § 8.2.1.1.1.10 de la Recomendación X.411.

mt-conversion-with-loss-prohibited ATTRIBUTE
WITH ATTRIBUTE-SYNTAX ConversionWithLossProhibited
MATCHES FOR EQUALITY
SINGLE VALUE
::= id-att-conversion-with-loss-prohibited

11.2.11 *TIC convertidos*

Este atributo general, que tiene valores múltiples, identifica los tipos de información codificada del contenido después de la conversión, tal como lo indica la operación abstracta de entrega de mensaje o entrega de informe. Es generado por el AM. Está ausente si no se realizó ninguna conversión. Para detalles adicionales véanse los § 8.3.1.1.1.8 y 8.3.1.2.1.5 de la Recomendación X.411.

ms-converted-EITs ATTRIBUTE
WITH ATTRIBUTE-SYNTAX MS-EIT
MATCHES FOR EQUALITY
MULTI VALUE
::= id-att-converted-EITs

11.2.12 *Hora de creación*

Este atributo general proporciona la hora (o fecha) en que se creó el asiento en el AM. Es generado por el AM. Para detalles adicionales véase el § 6.3.2.

Nota – Dos o más inscripciones consecutivas pueden tener la misma hora de creación.

ms-creation-time ATTRIBUTE
WITH ATTRIBUTE-SYNTAX CreationTime
MATCHES FOR EQUALITY ORDERING
SINGLE VALUE
::= id-att-creation-time

11.2.13 *TIC entregados*

Este atributo general, que tiene valores múltiples, identifica los tipos de información codificada en el contenido del mensaje tal como se entregó. Es generado por el AM basándose en la información sobre los TIC originales y los TIC convertidos en la operación abstracta entrega de mensaje.

ms-delivered-EITs ATTRIBUTE
WITH ATTRIBUTE-SYNTAX MS-EIT
MATCHES FOR EQUALITY
MULTI VALUE
::= id-att-delivered-EITs

11.2.14 *Banderas de entrega*

Este atributo general contiene información de entrega. Actualmente se utiliza únicamente para indicar la conversión implícita del contenido. Para mayores detalles véase el § 8.2.1.1.1.9 de la Recomendación X.411.

```
mt-delivery-flags ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DeliveryFlags
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-delivery-flags
```

11.2.15 *Historia de la ampliación de la LD*

Este atributo general, de múltiples valores, se utiliza para mostrar la historia de la ampliación de la lista de distribución. Contiene uno o más nombres de listas de distribución utilizados durante el proceso de ampliación. Está ausente si la entrega a dicho destinatario no implica ninguna ampliación de una lista de distribución. Para mayores detalles véase el § 8.3.1.1.1.7 de la Recomendación X.411.

```
mt-dl-expansion-history ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DLExpansionHistory
        MULTI VALUE
        ::= id-att-dl-expansion-history
```

11.2.16 *Estado de la inscripción*

Este atributo general contiene el estado actual de cualquier inscripción en la base de información de mensajes almacenados. Es creado y mantenido por el AM. Para mayores detalles véase el § 6.4.

```
ms-entry-status ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EntryStatus
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-entry-status
```

11.2.17 *Tipo de inscripción*

Este atributo general contiene información que indica si una inscripción se refiere a un mensaje entregado o a un informe entregado. Es generado por el AM.

```
ms-entry-type ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EntryType
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-entry-type

EntryType ::= INTEGER {
        delivered-message       (0),
        delivered-report        (1),
        returned-content        (2) (0 .. ub-entry-types) }
```

11.2.18 *Nombre del destinatario deseado*

Este atributo general contiene el nombre O/D del destinatario previsto inicialmente si el mensaje ha sido redireccionado, y en donde cada valor representa un redireccionamiento. Para mayores detalles véase el § 8.3.1.1.1.4 de la Recomendación X.411.

```
mt-intended-recipient-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-intended-recipient-name
```

11.2.19 *Sobre de entrega de mensaje*

Este atributo general contiene el **sobre de entrega de mensaje** completo de un mensaje tal como es entregado por la operación abstracta. Para mayores detalles véase el § 9 de la Recomendación X.411.

```
mt-message-delivery-envelope ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryEnvelope
        SINGLE VALUE
        ::= id-att-message-delivery-envelope
```

11.2.20 *Identificador de entrega de mensajes*

Este atributo general contiene el **identificador de entrega de mensaje** proveniente de la operación abstracta entrega de mensaje. Para mayores detalles véase el § 8.3.1.1.1.1 de la Recomendación X.411.

```
mt-message-delivery-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryIdentifier
        SINGLE VALUE
        ::= id-att-message-delivery-identifier
```

11.2.21 *Hora de entrega del mensaje*

Este atributo general contiene la **hora de entrega de mensaje** procedente de la operación abstracta entrega de mensaje. Para mayores detalles véase el § 8.3.1.1.1.2 de la Recomendación X.411.

Nota – No existe ningún atributo general correspondiente al parámetro hora de entrega de la operación abstracta entrega de informe, ya que para ser útil este tiempo de entrega debe estar correlacionado con el nombre del destinatario al que fue entregado el mensaje. Esta información se incluye en el atributo general información de informe.

```
mt-message-delivery-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryTime
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-message-delivery-time
```

11.2.22 *Verificación de la autenticación del origen del mensaje*

Este atributo general se calcula utilizando el algoritmo identificado por el identificador de autenticación del origen del mensaje. Proporciona al destinatario del mensaje una forma de autenticar el origen del mensaje y puede ser generado por el originador del mensaje. Para detalles adicionales véase el § 8.2.1.1.1.29 de la Recomendación X.411.

```
mt-message-origin-authentication-check ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageOriginAuthenticationCheck
        SINGLE VALUE
        ::= id-att-message-origin-authentication-check
```

11.2.23 *Etiqueta de seguridad del mensaje*

Este atributo general consta de un conjunto de atributos de seguridad que pueden incluir un identificador de política de seguridad, una clasificación de seguridad, una marca de confidencialidad, y un conjunto de categorías de seguridad. Para mayores detalles, véase el § 8.2.1.1.1.30 de la Recomendación X.411.

```
mt-message-security-label ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageSecurityLabel
        SINGLE VALUE
        ::= id-att-message-security-label
```

11.2.24 *Hora de depósito del mensaje*

Este atributo general contiene la **hora de depósito del mensaje** proveniente de una operación abstracta de entrega de mensaje. Para mayores detalles véase el § 8.2.1.1.2.2 de la Recomendación X.411.

```
mt-message-submission-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageSubmissionTime
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-message-submission-time
```

11.2.25 *Testigo de mensaje*

Este atributo general contiene el testigo asociado al mensaje. Es generado por el originador del mensaje y puede contener un valor diferente para cada destinatario del mensaje. Para detalles adicionales véase el § 8.2.1.1.1.26 de la Recomendación X.411.

```
mt-message-token ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageToken
        SINGLE VALUE
        ::= id-att-message-token
```

11.2.26 *TIC originales*

Este atributo general, de múltiples valores, contiene los **tipos de información codificada originales** provenientes de la operación abstracta entrega de mensaje. Es generado por el AM. Para detalles adicionales véase el § 8.2.1.1.1.33 de la Recomendación X.411.

```
ms-original-EITs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EIT
        MATCHES FOR EQUALITY
        MULTI VALUE
    ::= id-att-original-EITs
```

11.2.27 *Certificado de originador*

Este atributo general contiene el certificado del originador del mensaje. Es generado por una fuente de confianza (por ejemplo una autoridad de certificación) y puede ser suministrado por el originador del mensaje. Para detalles adicionales véase el § 8.2.1.1.1.25 de la Recomendación X.411.

```
mt-originator-certificate ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Originator-Certificate
        SINGLE VALUE
        ::= id-att-originator-certificate
```

11.2.28 *Nombre del originador*

Este atributo general contiene el nombre O/D del originador de la operación abstracta entrega de mensaje. Para detalles adicionales véase el § 8.2.1.1.1.1 de la Recomendación X.411.

```
mt-originator-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-originator-name
```

11.2.29 *Otros nombres de destinatarios*

Este atributo general, de múltiples valores, contiene los nombres O/D de todos los demás destinatarios especificados, si los hubiere, de un mensaje provenientes de la operación abstracta entrega de mensaje. Para mayores detalles véase el § 8.3.1.1.1.6 de la Recomendación X.411.

```
mt-other-recipient-names ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-att-other-recipient-names
```

11.2.30 *Número secuencial de progenitor*

Este atributo general apunta a una inscripción progenitora. Es generado por el AM. Siempre está presente en una inscripción vástago y está ausente en una inscripción principal.

```
ms-parent-sequence-number ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-parent-sequence-number
```

11.2.31 *Campos de entrega de informes por destinatario*

Este atributo general, de múltiples valores, contiene información destinatario por destinatario de la operación abstracta entrega de informe. Para detalles adicionales véase el § 8.3.1.2 de la Recomendación X.411.

```
mt-per-recipient-report-delivery-fields ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX PerRecipientReportDeliveryFields
        MUTLI VALUE
        ::= id-att-per-recipient-report-delivery-fields
```

11.2.32 *Prioridad*

Este atributo general contiene la **prioridad** relativa del mensaje proveniente de la operación abstracta entrega de mensaje. Si en el parámetro de la operación abstracta entrega de mensaje no se proporciona ningún valor al generar dicho atributo, el AM utiliza el valor por defecto. Para detalles adicionales véase el § 8.2.1.1.1.8 de la Recomendación X.411.

```
mt-priority ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Priority
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-priority
```

11.2.33 *Petición de prueba de entrega*

Este atributo general indica si el originador del mensaje necesita o no **prueba de entrega** del mensaje al destinatario. Puede ser generada por el originador del mensaje y puede especificar un valor diferente para cada destinatario del mensaje. Para detalles adicionales véase el § 8.2.1.1.1.32 de la Recomendación X.411.

```
mt-proof-of-delivery-request ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ProofOfDeliveryRequest
        SINGLE VALUE
        ::= id-att-proof-of-delivery-request
```

11.2.34 *Historia del redireccionamiento*

Este atributo general, de múltiples valores, contiene la historia de los redireccionamientos al destinatario con el (los) motivo(s) proporcionados por la operación abstracta entrega de mensaje o entrega de informe. Para detalles adicionales véase el § 8.3.1.1.1.5 de la Recomendación X.411.

```
mt-redirection-history ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RedirectionHistory
        MULTI VALUE
        ::= id-att-redirection-history.
```

11.2.35 *Sobre de entrega de informe*

Este atributo general contiene todos los parámetros de la operación abstracta entrega de informe, excepto el contenido devuelto (si lo hay). Para detalles adicionales véase el § 8.3.1.2 de la Recomendación X.411.

```
mt-report-delivery-envelope ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportDeliveryEnvelope
        SINGLE VALUE
        ::= id-att-report-delivery-envelope
```

11.2.36 *Nombre de la LD informante*

Este atributo general contiene el nombre O/D de la lista de distribución que envió el informe al propietario de la lista de distribución. Para detalles adicionales véase el § 8.3.1.2.1.4 de la Recomendación X.411.

```
mt-reporting-DL-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportingDLName
        SINGLE VALUE
        ::= id-att-reporting-DL-name
```

11.2.37 *Certificado del ATM informante*

Este atributo general contiene el certificado del ATM que generó el informe. Para detalles adicionales véase el § 8.3.1.2.1.12 de la Recomendación X.411.

```
mt-reporting-MTA-certificate-ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportingMTACertificate
        SINGLE VALUE
        ::= id-att-reporting-MTA-certificate
```

11.2.38 *Verificación de la autenticación del origen del informe*

Este atributo general proporciona una forma de autenticar el origen del informe. Para detalles adicionales véase el § 8.3.1.2.1.13 de la Recomendación X.411.

```
mt-report-origin-authentication-check ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportOriginAuthenticationCheck
        SINGLE VALUE
        ::= id-att-report-origin-authentication-check
```

11.2.39 *Clasificación de seguridad*

Este atributo general comprende el parámetro clasificación de seguridad procedente de la etiqueta de seguridad del mensaje. Se define como un atributo separado para permitir su uso de la operación abstracta resumir. Para detalles adicionales véase el § 8.5.9 de la Recomendación X.411.

```
mt-security-classification ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SecurityClassification
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-security-classification
```

11.2.40 *Número secuencial*

Este atributo general se utiliza para identificar la propia inscripción. Es atribuido por el AM al crear la inscripción. Para mayores detalles véase el § 6.3.2.

```
mt-sequence-number ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-sequence-number
```

11.2.41 *Identificador de depósito asunto*

Este atributo general contiene el identificador de depósito de mensaje o identificador de depósito de sonda del asunto del informe. Para mayores detalles véase el § 8.3.1.2.1.1 de la Recomendación X.411.

```
mt-subject-submission-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectSubmissionIdentifier
        SINGLE VALUE
        ::= id-att-subject-submission-identifier
```

11.2.42 *Nombre de este destinatario*

Este atributo general contiene el nombre O/D de este destinatario (AM) procedente de la operación abstracta entrega de mensaje para mayores detalles véase el § 8.3.1.1.1.3 de la Recomendación X.411.

```
mt-this-recipient-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-this-recipient-name
```

11.3 *Generación de los atributos generales*

Este punto describe la forma en que se generan los atributos generales. La información se presenta en el cuadro 2/X.413. Para la descripción de las clasificaciones utilizadas véase el § 5.3.

CUADRO 2/X.413

Generación de los tipos de atributos generales

Nombre de tipo de atributo	Uno/ múltiples valores	Parámetro fuente	Generado en la fuente por	Reglas de generación
Números secuenciales de vástago	M	–	AM	Se genera un valor para cada inscripción vástago correspondiente que tenga la inscripción progenitora
Contenido	S	**contenido** **contenido devuelto**	EM EI	El valor del parámetro es el valor del atributo
Identificador de algoritmo de confidencialidad del contenido	S	**identificador de algoritmo de confidencialidad del contenido**	EM	El valor del parámetro es el valor del atributo
Correlacionador de contenido	S	**correlacionador de contenido**	EI	El valor del parámetro es el valor del atributo
Identificador de contenido	S	**identificador de contenido**	EM EI	El valor del parámetro es el valor del atributo
Verificación de integridad de contenido	S	**verificación de integridad de contenido**	EM	El valor del parámetro es el valor del atributo
Longitud del contenido	S	–	AM	El tamaño (aproximado) del contenido almacenado, en octetos, basado en el contenido entregado o devuelto
Contenido devuelto	S	–	AM	El valor se fija a **verdadero** si el contenido devuelto está presente en una entrega de informe y en **falso** si no está presente
Tipo de contenido	S	**tipo de contenido**	EM EI	Si está representado por IDENTIFICADOR DE OBJETO, el valor del parámetro. Si está representado por ENTERO, convertido al IDENTIFICADOR DE OBJETO correspondiente
Prohibición de conversión con pérdida	S	**prohibición de conversión con pérdida**	EM	El valor del parámetro es el valor del atributo
TIC convertidos	M	**tipos de información codificada convertidos**	EM	Se genera un valor correspondiente a partir de cada bit fijado a **1** en el parámetro de **tipos de información codificada incorporada** y de cada **tipo de información codificada externa** presente en el parámetro **tipo de información codificada externa**
Hora de creación	S	–	AM	La hora de creación del asiento
TIC entregados	M	**TIC convertidos** y **TIC originales**	AM	Una unión de los otros dos tipos de atributos generales

CUADRO 2/X.413 *(cont.)*

Nombre de tipo de atributo	Uno/ múltiples valores	Parámetro fuente	Generado en la fuente por	Reglas de generación
Banderas de entrega	S	**banderas de entrega**	EM	El valor del parámetro es el valor del atributo. Si no hay **banderas de entrega** en el EM, se ha de generar un valor por defecto sin banderas asignadas
Historia de la ampliación LD	M	**historia de la ampliación LD**	EM EI	Se genera un valor correspondiente a partir de cada componente de la SECUENCIA
Estado de la inscripción	S	–	MS	Generado cuando la inscripción se crea con el valor «nuevo»
Tipo de inscripción	S	**ARGUMENTO entrega de mensaje** **ARGUMENTO entrega de informe**	AM AM	El valor se fija a «mensaje entregado» El valor se fija a «informe entregado». Si está presente un contenido devuelto, se crea una inscripción vástago que contenga el contenido devuelto. Para la inscripción vástago el valor de este atributo se fija a «contenido devuelto»
Nombre del destinatario deseado	S	**nombre del destinatario deseado**	EM	El valor del parámetro es el valor del atributo
Sobre de entrega de mensaje	S	**sobre**	EM	El valor del parámetro es el valor del atributo
Hora de entrega de mensaje	S	**hora de entrega de mensaje**	EM	El valor del parámetro es el valor del atributo
Identificador de entrega de mensaje	S	**identificador de entrega de mensaje**	EM	El valor del parámetro es el valor del atributo
Verificación de autenticación de origen del mensaje	S	**verificación de autenticación de origen del mensaje**	EM	El valor del parámetro es el valor del atributo
Etiqueta de seguridad del mensaje	S	**etiqueta de seguridad del mensaje**	EM EI	El valor del parámetro es el valor del atributo
Hora de depósito del mensaje	S	**hora de depósito del mensaje**	EM	El valor del parámetro es el valor del atributo
Testigo de mensaje	S	**testigo de mensaje**	EM	El valor del parámetro es el valor del atributo
TIC originales	M	**tipos de información codificada originales**	EM EI	Se genera un valor correspondiente a partir de cada bit fijado a **1** en el parámetro de **tipos de información codificada incorporada** y del **tipo de información codificada externa** presente en el parámetro **tipo de información codificada externa**
Certificado del originador	S	**certificado del originador**	EM	El valor del parámetro es el valor del atributo

CUADRO 2/X.413 *(fin)*

Nombre de tipo de atributo	Uno/ múltiples valores	Parámetro fuente	Generado en la fuente por	Reglas de generación
Nombre del originador	S	**nombre del originador**	EM	El valor del parámetro es el valor del atributo
Nombres de otros destinatarios	M	**nombres de otros**	EM	Se genera un valor correspondiente a partir de cada componente de la SECUENCIA
Número del secuencial de progenitor	S	–	AM	Al crear una inscripción vástago se genera este atributo con el valor correspondiente del número secuencial de la inscripción progenitora
Campos de entrega de informes para cada destinatario	M	**campos para cada destinatario**	EI	Se genera un valor correspondiente a partir de cada componente de la SECUENCIA
Prioridad	S	**prioridad**	EM	El valor del parámetro es el valor del atributo
Petición de prueba de entrega	S	**petición de prueba de entrega**	EM	El valor del parámetro es el valor del atributo
Historia del redireccionamiento	M	**historia del redirecciona-miento**	EM	Se genera un valor correspondiente a partir de cada componente de la SECUENCIA
Sobre de entrega de informe	S	**sobre**	EI	El valor del parámetro es el valor del atributo
Nombre de la LD informante	S	**nombre de la LD informante**	EI	El valor del parámetro es el valor del atributo
Certificado del ATM informante	S	**certificado del ATM informante**	EI	El valor del parámetro es el valor del atributo
Verificación de autenticación de origen del informe	S	**verificación de autenticación del informe**	EI	El valor del parámetro es el valor del atributo
Clasificación de seguridad	S	**clasificación de seguridad**	EM EI	El valor del parámetro es el valor del atributo
Número secuencial	S	–	AM	Cuando se crea una inscripción, el AM asigna un valor único para este atributo, en orden ascendente
Identificador de depósito del asunto	S	**identificador de depósito del asunto**	EI	El valor del parámetro es el valor del atributo
Nombre de este destinatario	S	**nombre de este destinatario**	EM	El valor del parámetro es el valor del atributo

Nota – Cuando se crea una inscripción de entrega de mensaje, no se generan atributos generales por separado para los argumentos de entrega física y método de entrega, ya que la información en estos argumentos no tiene interés para el AM. Sin embargo, el AU puede extraer toda la información contenida en estos argumentos extrayendo el atributo general sobre de entrega del mensaje.

11.4 *Abono a tipos de atributo*

El abono a tipos de atributo es un asunto local. Si se cambia el abono a tipos de atributo, el AU puede recibir todos los atributos en el abono original para mensajes presentes en el AM cuando se cambió el abono. El tratamiento de estos atributos no abonados es un asunto local. Igualmente cuando se abona un nuevo atributo, el AU puede no recibir dicho atributo para mensajes que estaban ya en el AM cuando tuvo lugar el abono.

12 Tipos de acciones automáticas generales

Los **tipos de acciones automáticas generales** son válidos para todos los tipos de contenido de mensaje. Sin embargo, su efecto detallado puede ser específico de un contenido y así la descripción de los procedimientos que se presentan en esta Recomendación pueden requerir el complemento de las Recomendaciones respectivas, por ejemplo el procedimiento específico del SMIP para el **tipo de acción automática general** de retransmisión automática que se describe en el § 19.4 de la Recomendación X.420. Otros **tipos de acción automática**, que son específicos del contenido, pueden definirse en sus Recomendaciones respectivas.

Las **acciones automáticas** se presentan en el § 6.5, y se registran y eliminan utilizando la operación abstracta registro en AM descrita en el § 8.6.

Se definen los siguientes tipos de **acciones automáticas generales**:

a) retransmisión automática;

b) alerta automática.

La operación de las **acciones automáticas** puede llevarse a cabo estableciendo una política de seguridad.

Los puntos siguientes contienen una breve descripción de cada **tipo de acción automática general** junto con su sintaxis abstracta, mediante la macro **AUTO-ACCIÓN** definida en el § 6.5.

12.1 *Retransmisión automática*

La **acción automática retransmisión automática** permite al proveedor del servicio abstracto AM **retransmitir** automáticamente cualquier mensaje que haya sido entregado a la base de información de mensajes almacenados. La definición exacta de retransmisión depende del contenido, pero siempre implica el depósito de un nuevo mensaje que incorpora el contenido entregado al servicio abstracto STRM.

El **tipo de acción automática retransmisión automática** permite que uno o más conjuntos de parámetros **retransmisión automática** sean registrados en el AM, cada uno identificado por su **identificador de registro de retransmisión automática**. Cada **parámetro registro de retransmisión automática** especifica los criterios que determinarán si se aplica o no a un mensaje entregado en particular, y si es así, una copia de dicho mensaje se **retransmite automáticamente** utilizando la operación abstracta de depósito de mensaje. Esto quiere decir, que si un mensaje concuerda con más de un conjunto de criterios, el mensaje será **retransmitido automáticamente** tantas veces como conjuntos de criterios hayan sido satisfechos por el mensaje.

El **parámetro registro de retransmisión automática** especifica si la inscripción principal (y cualesquiera de las inscripciones vástagos asociadas) que corresponden al mensaje deben o no suprimirse después de la **retransmisión automática**. Si cualquiera de los parámetros sobre los que se actúa indica no-supresión (o si falla cualquiera de los depósitos), la inscripción no se suprime.

```
auto-forward AUTO-ACTION
        REGISTRATION PARAMETER IS AutoForwardRegistrationParameter
        ::= id-act-auto-forward

AutoForwardRegistrationParameter ::= SET{
        filter                      [0] Filter OPTIONAL,
        auto-forward-arguments      [1] AutoForwardArguments,
        delete-after-auto-forwarding [2] BOOLEAN DEFAULT FALSE,
        other-parameters            [3] OCTET STRING OPTIONAL}

AutoForwardArguments ::= SET{
        COMPONENTS OF PerMessageAutoForwardFields,
        per-recipient-fields        [1] IMPLICIT SEQUENCE (1..ub-recipients) OF
                                        PerRecipientAutoForwardFields}
```

```
PerMessageAutoForwardFields ::= SET{
        originator-name             OriginatorName,
        content-identifier          ContentIdentifier OPTIONAL,
        priority                    Priority DEFAULT normal,
        per-message-indicators      PerMessageIndicators DEFAULT {},
        deferred-delivery-time      [0] IMPLICIT DeferredDeliveryTime OPTIONAL,
        extensions                  [2] IMPLICIT PerMessageSubmissionExtensions DEFAULT {}}

PerRecipientAutoForwardFields ::= SET{
        recipient-name              RecipientName,
        originator-report-request   [0] IMPLICIT OriginatorReportRequest,
        explicit-conversion         [1] IMPLICIT ExplicitConversion OPTIONAL,
        extentions                  [2] IMPLICIT PerRecipientMessageSubmissionExtensions
                                        DEFAULT {}}
```

Los parámetros del **parámetro registro de retransmisión automática** tienen los siguientes significados:

1) **Filtro** (F): Es un conjunto de criterios que una inscripción nueva que representa un mensaje entregado debe satisfacer para que el proveedor del servicio abstracto AM pueda **retransmitirla automáticamente** utilizando este conjunto de parámetros.

   La ausencia de este parámetro indica que todas las inscripciones nuevas son **retransmitidas automáticamente.**

2) **Argumentos de retransmisión automática** (O): Es un conjunto de argumentos registrados que han de utilizarse para cada operación abstracta de depósito de mensajes (véase el § 8.2.1.1.1 de la Recomendación X.411). Cualquier argumento que no sea ni registrado ni obligatorio, no mencionado específicamente más adelante, estará ausente en cada depósito de mensaje.

   Si los argumentos siguientes no son registrados o bien son registrados con sus valores por defecto, los valores utilizados para cada operación abstracta de depósito de mensaje son los de los correspondientes argumentos de entrega de mensaje: **prioridad**, **prohibición implícita de conversión**, y **prohibición de conversión con pérdida**.

   Si los argumentos siguientes no son registrados o bien son registrados con sus valores por defecto, su presencia como argumentos de depósito de mensaje depende de la presencia de los argumentos de entrega de mensaje correspondientes, transformándose sus valores cuando proceda: **testigo de mensaje**, **identificador de algoritmo de confidencialidad de contenido**, **verificación de integridad de contenido**, **verificación de autenticación de origen de mensaje**, y **etiqueta de seguridad del mensaje**.

   Ciertos argumentos de depósito de mensaje pueden no ser registrados. Estos son: **petición de prueba de depósito**, **tipo de información codificada originales**, **tipo de contenido**, y **contenido**.

3) **Supresión tras retransmisión automática** (F): Indica si una inscripción debe ser o no suprimida una vez que el depósito se haya hecho correctamente.

   La ausencia de este parámetro indica que no se debe suprimir el mensaje.

4) **Otros parámetros** (F): no es necesario que este parámetro que es específico al contenido esté presente. Cuando lo esté, la información que contiene se utilizará durante el procedimiento de **retransmisión automática.**

   Nota – Así, por ejemplo, con la mensajería interpersonal, este parámetro puede contener el **comentario de retransmisión automática** que se devuelve en una notificación de no recepción, un prefijo especificado por el usuario y una nota de portada que acompaña al mensaje IP que es retransmitido automáticamente. Para una descripción del uso de **comentarios de retransmisión automática**, véase el § 19.4 de la Recomendación X.420.

12.2 *Alerta automática*

La **acción automática alerta automática** permite al proveedor del servicio abstracto AM *alertar* automáticamente al usuario que está detrás del usuario del servicio abstracto AM acerca de la entrega de cualquier mensaje que haya sido entregado a la base de información de mensajes almacenados. La **alerta automática** únicamente se efectuará para inscripciones de mensajes entregados.

El **tipo de acción automática alerta automática** permite que uno o más conjuntos de parámetros **alerta automática** sean registrados en el AM, cada uno identificado por su **identificador de registro de alerta automática.** Cada **parámetro registro de alerta automática** especifica criterios que determinan si se aplica o no a un determinado mensaje entregado. Si un mensaje concuerda con el filtro de más de un registro de alerta automática, se procesará el registro concordante que tenga el identificador de registro de alerta automática más bajo, y si al menos se ha alertado con éxito a una dirección (o al AU), no se procesa ningún otro registro. Si no se puede alertar con éxito a ninguna de estas direcciones, se procesará el registro de alerta automática con el identificador que siga al más alto. Esto continúa así hasta que al menos una o más direcciones del registro hayan sido alertadas correctamente o se haya agotado la lista de registros.

La **operación abstracta de alerta** sólo será invocada si se considera que las direcciones alerta en el registro de alerta automática tienen como miembro al AU (véase el 2) más abajo). Si esta operación abstracta de alerta tiene éxito, no se alertará ninguna otra dirección contenida en el registro de alerta automática.

```
Auto-alert AUTO-ACTION
        REGISTRATION PARAMETER IS AutoAlertRegistrationParameter
        ::= id-act-auto-alert

AutoAlertRegistrationParameter ::= SET{
        filter                  [0] Filter OPTIONAL,
        alert-addresses         [1] SEQUENCE SIZE (1..ub-alert-addresses) OF AlertAddress
                                    OPTIONAL,
        requested-attributes    [2] EntryInformationSelection OPTIONAL}
```

Los parámetros del **parámetro registro de alerta automática** tienen los siguientes significados:

1) **Filtro** (F): Es un conjunto de criterios que debe satisfacer una inscripción nueva, que representa mensaje entregado, para que el proveedor de servicios abstractos AM le **alerte automáticamente** utilizando este conjunto de parámetros.

   La ausencia de este parámetro indica que se realizará la **alerta automática** para todas las inscripciones de mensajes entregadas.

2) **Direcciones de alerta** (F): Este argumento identifica los tipos de servicio de **alerta** que han de invocarse junto con cualquier información requerida para ganar acceso a un caso específico del servicio de **alerta**, y cualquier otra información que necesite ser transmitida durante esas **alertas**.

   La ausencia de este argumento significa que la operación abstracta de alerta informa al usuario del servicio AM de la existencia de una condición de alerta, sea utilizando la operación abstracta de alerta (véase el § 8.7), (que sólo es posible si existe ya una asociación abstracta entre el usuario del servicio abstracto AM y el proveedor del servicio abstracto AM) o llamando mediante una bandera a la operación abstracta de vinculación la próxima vez que el usuario del servicio abstracto AM establezca una asociación abstracta (véase el § 7). Si está presente el parámetro atributos solicitados, se considerará que el usuario de servicio abstracto AM (AU) figura entre las direcciones que han de alertarse.

   Algunos tipos de **alerta** se normalizarán en el plano internacional, otros serán definidos por autoridades administrativas nacionales y organizaciones privadas. Esto implica que varias autoridades distintas serán responsables de la asignación de tipos de una manera que garantice que cada uno es distinto de todos los demás asignados. Esto se logra identificando cada tipo con un identificador de objeto en el momento de definir el tipo, y definiendo el tipo de datos NSA.1 de la información auxiliar de direccionamiento.

   El **calificativo de alerta** contiene cualquier otra información que deba ser transmitida durante la **alerta automática**. La ausencia de ese parámetro significa que no se transmitirá ninguna información adicional al usuario del servicio abstracto AM.

```
AlertAddress ::= SEQUENCE{
    address             EXTERNAL,
    alert-qualifier     OCTET STRING OPTIONAL}
```

3) **Atributos solicitados** (F): Indica que información de las inscripciones seleccionadas debe incluirse en la alerta automática. Véase el § 8.1.4.

   La ausencia de este parámetro significa que únicamente el **identificador de registro de alerta** estará presente en el **argumento de alerta**.

SECCIÓN 4 – PROCEDIMIENTOS PARA ALMACENAMIENTO DE MENSAJES Y REALIZACIÓN DE PUERTOS

13 Visión de conjunto

Esta sección describe los procedimientos para el AM y la realización de puertos. Contiene una descripción del consumo del servicio abstracto STRM en el § 14. La prestación del servicio abstracto AM se describe en el § 15. La realización de puertos bajo la forma de elementos de servicio se describe en el § 16.

La realización de las operaciones abstractas descritas en los § 14 y 15 estará sujeta a las exigencias de la política de seguridad (si hay alguna en vigor) que se aplica a los servicios abstractos STRM y a los servicios abstractos AM.

14 Consumo del servicio abstracto de transferencia de mensajes

Este punto especifica cómo un AM consumirá el servicio abstracto STRM que se define en el § 8 de la Recomendación X.411. Se trata el consumo de los puertos de entrega, depósito y administración STRM.

14.1 *Consumo de los servicios abstractos de puerto de entrega*

Este punto trata la realización de las operaciones abstractas entrega de mensaje y entrega de informe y la invocación de la operación abstracta control de entrega. El consumo AM de servicios abstractos de puerto de entrega presupone que existe una asociación abstracta entre el suministrador del puerto de entrega (el ATM) y el consumidor del puerto de entrega (el AM). La realización de las operaciones abstractas es secuencial, sin que tenga lugar un procesamiento paralelo. Los casos de error no se describen.

14.1.1 *Realización de la operación abstracta de entrega de mensajes*

Cuando el AM recibe una operación abstracta de entrega de mensaje, del ATM, sigue los pasos siguientes:

1) Devuelve un resultado de entrega de mensaje al ATM para indicar que la entrega tuvo éxito. El resultado de entrega de mensaje contendrá información de prueba de entrega si el mensaje entregado contiene un argumento de petición de prueba de entrega. Esta prueba de entrega puede calcularse utilizando la clave secreta-AM-asunto; para más detalles véanse los § 8.5.7 y 8.3.1.1.2.2 de la Recomendación X.411.
2) El paso siguiente consiste en examinar si hay algunas acciones automáticas activadas. Las acciones automáticas son, en parte, específicas del contenido, por lo que se describen también en Recomendaciones específicas del contenido. La descripción específica del contenido tiene que contener reglas sobre el orden en que se ejecutan las acciones automáticas. La ejecución de acciones automáticas puede dar como resultado alertas, presentaciones, la creación de nuevas inscripciones y la posible supresión del mensaje entregado o de otros mensajes en el AM. Véase el § 12.1.
   a) Si mediante una operación abstracta de registro en el AM se registran criterios de retransmisión automática, la nueva inscripción se hace concordar los criterios especificados. La concordancia se busca secuencialmente para cada conjunto especificado de criterios de selección. Para cada «golpe», se genera un nuevo mensaje que el AM deposita en el ATM utilizando la operación abstracta de depósito de mensaje (véase el § 15.2.1).

      Las reglas sobre la manera de construir el nuevo mensaje retransmitido son asimismo específicas del contenido y por tanto se describen en las respectivas Recomendaciones específicas del contenido. Otros sucesos específicos del contenido deben efectuarse también en esta etapa (por ejemplo, la supresión de bucles de mensajes retransmitidos automáticamente y la expedición de una notificación de no recepción como se describe para el SMIP en el § 19.4 de la Recomendación X.420. En función de los valores del argumento de la operación abstracta de registro en el AM para retransmisión automática, puede retenerse en el AM una copia del mensaje entregado. Si fracasa la tentativa de retransmisión automática, se mantiene siempre una copia a fin de evitar la pérdida de los mensajes.

      Nota – El tratamiento de un resultado o error sobre la base de tal depósito es un asunto local.

   b) Si se han hecho registros automáticos de alertas a través de la operación abstracta de registro en el AM, la nueva inscripción se hace concordar con el filtro de cada registro especificado. La concordancia se busca secuencialmente para cada registro. Si se encuentra un «golpe», se hace una tentativa de invocar una operación abstracta de alerta desde el AM al AU. Esto sólo puede hacerse si hay una asociación abstracta existente entre el AM y el AU. Si no existe ninguna asociación abstracta, puede que el AM disponga de un medio local o no normalizado para

invocar una alerta. Cuando se han hecho tentativas de alertar todas las direcciones registradas para una primera concordancia del parámetro de registro, y se ha tenido éxito al menos en una de las alertas, la acción automática de alerta ha sido completada con éxito y no se procesará ningún otro registro de alerta. Si no se encontró un trayecto para dar la alerta, el AM pone la bandera de alerta, que se comunica al AU la próxima vez que el AU inicia una asociación abstracta hacia el AM.

Nota – Si el mensaje entregado se suprimió como resultado de una acción de retransmisión automática en a), es evidente que no se efectúa la alerta automática.

3) Sólo después de haberse dado los pasos mencionados se hace visible una nueva inscripción fuera del AM a través del puerto de extracción. Si el mensaje entregado se suprimió como resultado de una acción automática, todo número secuencial que se atribuyó en el paso 2) no será reutilizado (a fin de no entrar en conflicto con las ampliaciones del registro cronológico mencionado en normas de la ISO). El estado de la inscripción (de esa inscripción) se fija a nuevo.

14.1.1.1 *Reglas de generación para atributos generales*

Los atributos facultativos se generan únicamente si están realizados por el AM y el usuario está abonado a los mismos. Los atributos generados forman una nueva inscripción (en algunos casos una inscripción progenitora e inscripciones vástagos, véase el § 6) en el AM.

Para las reglas sobre la manera de generar los atributos generales, véanse el cuadro 1/X.413 y el § 11.3. Obsérvese que para los atributos generales que están ausentes en el sobre de entrega correspondiente, se genera, en la inscripción, un atributo con un valor o por defecto.

14.1.2 *Realización de la operación abstracta entrega de informe*

Cuando el AM recibe una operación abstracta de entrega de informe procedente del ATM, sigue los pasos siguientes:

1) Devuelve un resultado de entrega de informe al ATM para indicar que la entrega tuvo éxito. El resultado de entrega de informe no tiene parámetros. Para más detalles véase el § 8.3.1.2.2 de la Recomendación X.411.
2) Seguidamente, si alguna de las acciones automáticas u otros procedimientos internos están activados, se ejecutan dichas acciones o procedimientos. Estos son específicos del contenido y se describen en las respectivas Recomendaciones específicas del contenido.

14.1.2.1 *Reglas de generación para atributos generales*

Pueden generarse atributos cuando se recibe un mensaje o cuando se realiza una operación abstracta en el AM, activada por una invocación del AU.

Se generan todos los atributos obligatorios, véase el cuadro 1/X.413. Los atributos opcionales sólo se generan si están realizados por el AM y el usuario se ha abonado a los mismos. Los atributos generados forman una nueva inscripción (en algunos casos una inscripción progenitora e inscripciones vástagos, véase el § 6) en el AM. Como parte del proceso pueden producirse las siguientes clases de atributos generales:

a) atributos generales generados por el propio AM (por ejemplo, número secuencial);
b) atributos generales generados a partir de las componentes del sobre de entrega de informe. Para los componentes que no están presentes, pero para los cuales se definen valores por defecto, se genera un atributo general que contiene el valor por defecto.

Las reglas de generación para a) y b) se describen en el § 14.1.1.1. Las reglas de generación para los atributos de contenido específicos se describen en las Recomendaciones respectivas específicas del contenido, por ejemplo, los atributos específicos al SMIP se describen en el anexo C de la Recomendación X.420.

Para las reglas sobre la manera de generar atributos generales, véanse el cuadro 1/X.413 y el § 11.3. Obsérvese que para los atributos generales que están ausentes del sobre de entrega correspondiente, se genera en la inscripción un atributo con valor por defecto.

14.1.3 *Invocación de la operación abstracta de control de entrega*

Si el AM desea detener temporalmente el envío de mensajes e informes por el STRM, o modificar la máxima longitud de contenido o la prioridad más baja de los mensajes emitidos por el ATM, sigue los siguientes pasos:

1) Invoca una operación abstracta de control de entrega, que contiene los parámetros a cambiar. Para más detalles véase el § 8.3.1.3 de la Recomendación X.411.
2) Obtiene la devolución de un resultado cuando el servicio abstracto STRM ha aceptado los cambios. El resultado contiene información sobre si hay o no mensajes y/o informes en espera en el ATM, debido a las restricciones en vigor. Para más detalles, véase el § 8.3.1.3.2 de la Recomendación X.411.

3) Cuando el AM es capaz de aceptar cualquier mensaje o sonda en espera debe, a su vez, invocar una nueva operación abstracta de control de entrega para mitigar las restricciones. Los efectos de una operación abstracta de control de entrega se anulan cuando una nueva operación abstracta de control de entrega modifica las restricciones o cuando se libera la asociación abstracta.

14.2 *Consumo de servicios abstractos de puerto de depósito*

Este punto trata la invocación de las operaciones abstractas depósito de mensaje, depósito de sonda, y anulación de entrega diferida, y el consumo de la operación abstracta de control de depósito. El consumo del servicio abstracto AM por el de los servicios abstractos de puerto de depósito presupone que existe una asociación abstracta entre el suministrador del puerto de depósito (el ATM) y el consumidor del puerto de depósito (el AM). Las operaciones abstractas se realizan en orden secuencial, sin que tenga lugar un procesamiento paralelo. Los casos de error no se describen.

14.2.1 *Invocación de la operación abstracta de depósito de mensaje*

La iniciación de una operación abstracta de depósito de mensaje puede provenir de una acción automática dentro del AM o por el hecho de que el AU invocó una operación abstracta de depósito de mensaje al AM. A fin de depositar el mensaje en el ATM, el AM sigue los siguientes pasos:

1) Si el argumento de depósito de mensaje no contiene la ampliación de petición de retransmisión (véase el § 6.6), invoca una operación abstracta de depósito de mensaje, que contiene el mensaje a depositar y sus parámetros asociados. Para más detalles véase el § 8.2.1.1 de la Recomendación X.411. En caso contrario, verifica que la inscripción es un mensaje entregado e incorpora información procedente de un asiento de mensaje entregado en la base de información de los mensajes almacenados, y, entonces, invoca la operación abstracta de entrega de mensaje con el nuevo concepto. La retransmisión de inscripciones que no son mensajes entregados será objeto de ulterior estudio.

   Obsérvese que aunque esta petición de inscripción es genérica, no tiene necesariamente que tener sentido para todos los tipos de contenido. Cuando tiene sentido, el tipo de contenido de la inscripción del mensaje entregado referenciado debe ser apropiado para incorporación en el argumento del contenido.

2) Obtiene la devolución de un resultado de depósito de mensaje cuando el ATM ha aceptado el depósito. El resultado de depósito de mensaje contiene entre otras cosas información sobre la identificación de, y la hora de depósito para, el mensaje depositado. Para más detalles, véase el § 8.2.1.1.2 de la Recomendación X.411.

3) Si la operación abstracta de depósito de mensaje fue desencadenada por una operación abstracta correspondiente de depósito de mensaje al AM, proveniente del AU, el resultado de la operación abstracta se devuelve al AU en forma de un resultado de depósito de mensaje expedido por el AM. Este comportamiento garantiza que el mensaje ha sido efectivamente aceptado por el ATM antes de devolver el resultado al AU.

4) Si el ATM no ha aceptado el depósito de mensaje debido a problemas tales como un número secuencial no válido o un tipo de contenido inapropiado, el AM generará un error de petición incoherente. Obsérvese que todos los errores generados por el ATM son retransmitidos a través del AU.

5) Si está en vigor una política de seguridad, entonces, a fin de garantizar que tal política de seguridad no va a ser violada durante el depósito de un mensaje, el AM verifica la etiqueta de seguridad del mensaje, comparándola con el contexto de seguridad. Si el depósito de mensaje está prohibido sea por la política de seguridad, sea temporalmente por restricciones de seguridad, se indicará un error de seguridad.

14.2.2 *Invocación de la operación abstracta de depósito de sonda*

Una operación abstracta de depósito de sonda se inicia porque el AU invocó una operación abstracta de depósito de sonda hacia el AM. A fin de depositar la sonda para el ATM, el AM sigue los siguientes pasos:

1) Invoca una operación abstracta de depósito de sonda, que contiene la sonda a depositar y sus parámetros asociados. Para más detalles véase el § 8.2.1.2.1 de la Recomendación X.411.

2) Obtiene la devolución de un resultado de depósito de sonda cuando el ATM ha aceptado el depósito. El resultado contiene entre otras cosas información sobre la identificación de la hora de depósito de la sonda depositada. Para más detalles véase el § 8.2.1.2.2 de la Recomendación X.411.

3) El resultado de la operación abstracta se devuelve a AU en forma de un resultado de depósito de sonda expedido por el AM. Este comportamiento garantiza que la sonda ha sido efectivamente aceptada por el ATM antes de que se devuelva el resultado al AU.

4) Si se está aplicando una política de seguridad, para garantizar que no se incumple tal política de seguridad durante el depósito de la sonda, el AM verifica la etiqueta de seguridad de mensaje de la sonda con respecto al contexto de seguridad. Si el depósito de sonda está prohibido sea por la política de seguridad o temporalmente por restricciones de seguridad, se genera un error de depósito de sonda.

14.2.3 *Invocación de la operación abstracta anulación entrega diferida*

Una operación abstracta anulación entrega diferida se inicia porque el AU invocó una operación abstracta de anulación entrega diferida hacia el AM. A fin de enviar la anulación al ATM, el AM sigue los pasos siguientes:

1) Invoca una operación abstracta de anulación entrega diferida, que contiene la anulación que ha de depositarse y sus parámetros asociados. Para más detalles véase el § 8.2.1.3.1 de la Recomendación X.411.
2) Obtiene la devolución de un resultado cuando el ATM ha aceptado la anulación. El resultado devuelto está vacío como indicación de éxito.
3) El resultado de la operación abstracta se devuelve al AU en forma de un resultado de anulación entrega diferida expedido por el AM. Este comportamiento garantiza que la sonda ha sido efectivamente aceptada (o no) por el ATM antes de que se devuelva el resultado al AU.

14.2.4 *Realización de la operación abstracta control de depósito*

Si el ATM desea impedir que el AM deposite temporalmente mensajes o sondas, o modificar la longitud máxima del contenido, o la prioridad más baja de mensajes provenientes del AM, invoca una operación abstracta de control de depósito (para más detalles véase el § 8.2.1.4.1 de la Recomendación X.411) hacia el AM. El AM reacciona con los pasos siguientes:

1) Invoca una correspondiente operación abstracta de control de depósito del AM al AU.
2) Espera a que el AU devuelva un resultado de control de depósito que contiene información sobre la existencia de mensajes o sondas en espera en el AU, debido a las restricciones vigentes. Para más detalles véase el § 8.2.1.4.2 de la Recomendación X.411.
3) El AM devuelve un resultado de control de depósito al ATM, que contiene información procedente del AU.
4) Cuando el ATM es capaz de aceptar de nuevo cualesquiera mensajes o sondas debe asimismo invocar una nueva operación abstracta de control de depósito para mitigar las restricciones. Los efectos de una operación abstracta de control de depósito se anulan cuando una nueva operación abstracta de control de depósito modifica las restricciones o cuando se libera la asociación abstracta. El AM invoca entonces una operación abstracta de control de depósito correspondiente hacia el AU y espera el resultado del control de depósito.

14.3 *Consumo de los servicios abstractos de puerto de administración*

Este punto trata de la realización de operaciones abstractas de registro y cambio de credenciales. El consumo de servicios abstractos de puerto de administración presupone que existe una asociación abstracta entre el suministrador del puerto de administración (el ATM) y el consumidor del puerto de administración (el AM). Las operaciones abstractas se realizan en orden secuencial, sin que tenga lugar un procesamiento paralelo. Los casos de error no se describen.

El uso, por el AM, del puerto de administración, está sujeto a la política de seguridad en vigor.

14.3.1 *Invocación de la operación abstracta de registro*

Una operación abstracta de registro se inicia porque el AU ha invocado una operación abstracta de registro hacia el AM. Para enviar el registro al ATM, el AM sigue los siguientes pasos:

1) Invoca una operación abstracta de registro, que contiene los nuevos datos a registrar. Para más detalles véase el § 8.4.1.1.1 de la Recomendación X.411.
2) Obtiene la devolución de un resultado cuando el ATM ha aceptado el registro. El resultado devuelto está vacío como una indicación de éxito.
3) El ámbito de los cambios permitidos, por el AU a través del AM, en los argumentos de la etiqueta de seguridad de usuario está confinado a la política de seguridad en vigor.

14.3.2 *Invocación de la operación abstracta cambio de credenciales*

Se inicia una operación abstracta de cambio de credenciales porque el AU ha invocado una operación abstracta cambio de credenciales hacia el AM. A fin de retransmitir las nuevas credenciales desde el AU al ATM, el AM sigue los pasos siguientes:

1) Invoca una operación abstracta de cambio de credenciales en el ATM, que contiene las nuevas credenciales a registrar. Para más detalles véase el § 8.4.1.2.1 de la Recomendación X.411.
2) Obtiene la devolución de un resultado de cambio de credenciales cuando el ATM ha aceptado el cambio y almacena las nuevas credenciales. El resultado de cambio de credenciales o de un error proveniente del ATM se retransmite hacia el AU, y está vacío como una indicación de éxito.

14.3.3 *Realización de la operación abstracta de cambio de credenciales*

Cuando el AM recibe una operación abstracta de cambio de credenciales y sus argumentos asociados, del ATM, sigue los pasos siguientes:

1) Establece que la información de argumento es válida para una operación abstracta de cambio de credenciales. Para más detalles, véase el § 8.4.1.2 de la Recomendación X.411.
2) Verifica si existe una asociación abstracta entre el AM y el AU. Si no existe una asociación abstracta entre el AM y el AU, el ATM es informado por una indicación de error de que el cambio de credenciales no puede tener lugar en ese momento, y no se sigue adelante.
3) Si existe la asociación abstracta entre el AM y AU, el AM invoca hacia el AU una operación abstracta de cambio de credenciales.
4) Si el AU devuelve un resultado de cambio de credenciales vacío, que indica éxito, el AM devuelve al ATM un resultado correspondiente de cambio de credenciales y almacena las credenciales. Si el AU devuelve una indicación de error, esta se retransmite al ATM; para indicar el error. Obsérvese que el AM nunca devuelve una indicación de éxito al ATM antes de haber recibido el resultado correspondiente de retorno del AU.

15 Suministro del servicio abstracto de almacenamiento de mensajes

Este punto especifica cómo un AM suministra el servicio abstracto de AM. Se trata el suministro de puertos de extracción, depósito indirecto, y administración.

15.1 *Suministro de servicios abstractos de puerto de extracción*

Este punto trata del suministro de las operaciones abstractas de resumir, listado, captura, supresión, registro en el AM y alerta. El suministro del servicio abstracto AM de los servicios abstractos de puerto de extracción presupone que existe una asociación abstracta entre el suministrador del puerto de extracción (el AM) y el consumidor del puerto de extracción (el AU). Las operaciones abstractas se realizan en orden secuencial, sin que tenga lugar un procesamiento paralelo. No se describen todos los casos de errores.

15.1.1 *Realización de la operación abstracta de resumir*

Cuando el AM recibe una operación abstracta de resumir del AU, sigue los siguientes pasos:

1) Establece qué base de información es direccionada por la operación abstracta de resumir.
2) Verifica si hay inscripciones en la base de información. Si está vacía, se devuelve un resultado de resumir con una longitud cero y no se sigue adelante.
3) Verifica que los atributos generales de argumento y cualesquiera atributos específicos de contenido reconocidos por el AM son válidos para una operación abstracta de resumir. Para más detalles véase el § 8.2.1.
4) Acumula cómputos de conformidad con los atributos generales de argumento suministrados y cualesquiera atributos específicos de contenido reconocidos por el AM.
5) Devuelve al AU el resultado de resumir. Para más detalles véase el § 8.2.2.
6) Si se está aplicando una política de seguridad, a fin de garantizar que no se incumple esta política durante la operación abstracta de resumir, el AM verifica la clasificación de seguridad de la etiqueta de seguridad con respecto al contenido de seguridad. Si la política de seguridad prohíbe el resumir, deberá abandonarse tal operación abstracta e indicarse un error de seguridad.

15.1.2 *Realización de la operación abstracta de listado*

Cuando el AM recibe una operación abstracta de listado del AU, sigue los pasos siguientes:

1) Establece la base de información que resulta direccionada por la operación abstracta de listado.
2) Verifica que los atributos generales de argumento suministrados y cualesquiera atributos específicos de contenido reconocidos por el AM son válidos para una operación abstracta de listado. Para más detalles véase el § 8.3.1.
3) Identifica cero o varias inscripciones como solicitadas en el argumento de la operación abstracta, hasta cualquier límite especificado. Las inscripciones vástagos de una inscripción progenitora no se tienen en cuenta, a menos que hayan sido seleccionadas explícitamente en el argumento.

4) Si se ha especificado un conjunto de atributos generales solicitados como argumentos en la operación abstracta, se devuelven estos atributos generales, si están presentes, al AU, para cada inscripción seleccionada. Si no se ha hecho ninguna petición, se devuelven los valores por defecto de la operación abstracta de listado tal y como fueron especificados en una operación abstracta anterior de registro en el AM, si están presentes. Para más detalles véase el § 8.3.2. El estado de la inscripción de cada mensaje seleccionado se fija a listado.

5) Si se está aplicando una política de seguridad, a fin de garantizar que no se viola dicha política de seguridad durante la operación abstracta de listado, el AM verifica la etiqueta de seguridad del mensaje con respecto al contexto de seguridad. Si la operación de listado está prohibida, ya sea por la política de seguridad, o como consecuencia de restricciones provisionales de seguridad, se abandonará la operación abstracta de listado y se indicará un error de seguridad.

15.1.3 *Realización de la operación abstracta de captura*

Cuando el AM recibe una operación abstracta de captura del AU, sigue los pasos siguientes:

1) Establece qué base de información resulta direccionada por la operación abstracta de captura.

2) Verifica que los atributos generales de argumento suministrados son válidos para una operación abstracta de captura. Para más detalles véase el § 8.4.1.

3) Identifica cero o más inscripciones como solicitadas en el argumento de la operación abstracta, hasta cualquier límite especificado. Se excluyen las inscripciones vástagos de una inscripción progenitora, a menos que hayan sido seleccionadas expresamente en el argumento.

4) Si se ha especificado un conjunto de atributos generales como argumentos de una operación abstracta, se devuelven estos atributos generales, si están presentes, al AU, para la primera inscripción seleccionada. Si no se ha hecho ninguna petición, se devuelven los valores por defecto de la operación abstracta de captura, como se especifica en la operación abstracta anterior de registro en el AM, si están presentes. Si se encuentran varias inscripciones que satisfacen el criterio de búsqueda, se devuelven los números secuenciales para los asientos segundo y siguientes, en orden creciente. Si había más inscripciones concordantes que las especificadas en el límite, se devuelve también el número secuencial siguiente que rebasa el límite. Para más detalles véase el § 8.4.2.

5) Si se está aplicando una política de seguridad, entonces garantizar que tal política de seguridad no será violada durante la operación abstracta de captura, el AM verifica la etiqueta de seguridad del mensaje con respecto al contexto de seguridad. Si la operación abstracta de captura está prohibida por la política de seguridad, o por restricciones temporales de seguridad, deberá abandonarse la operación abstracta de captura e indicarse un error de seguridad.

15.1.4 *Realización de la operación abstracta de supresión*

Cuando el AM recibe una operación abstracta de supresión, del AU, sigue los siguientes pasos:

1) Establece qué base de información resulta direccionada por la operación abstracta de supresión.

2) Verifica que los argumentos suministrados son válidos para una operación abstracta de supresión. Para más detalles véase el § 8.5.1.

3) Identifica la inscripción o lista de inscripciones solicitadas en el argumento de la operación abstracta.

4) Si cualquiera de las inscripciones tiene restricciones a la supresión véase el § 8.5, no se efectuará ninguna de las supresiones. En otro caso se efectúan todas las supresiones y se devuelve un resultado de supresión vacío al AU como indicación de éxito.

15.1.5 *Realización de la operación abstracta de registro en el AM*

Cuando el AM recibe del AU una operación abstracta de registro en el AM sigue los pasos siguientes:

1) Verifica que los argumentos suministrados son válidos para una operación abstracta de registro en el AM. Para más detalles véase el § 8.6.1.

2) Reemplaza cualesquiera parámetros antiguos por los correspondientes parámetros nuevos. Las acciones automáticas afectan a las transacciones, tales como entregas de mensaje y entregas de informe, que se producen después de la iniciación o supresión de peticiones de acción automática, sin que haya procesamiento de inscripciones que ya residen en el AM en ese instante.

3) Devuelve un resultado de registro en el AM vacío al AU, para indicar que la operación abstracta ha sido realizada con éxito.

4) Si se está aplicando una política de seguridad, la operación abstracta de registro en el AM estará sujeta a dicha política. Algunas políticas de seguridad pueden solamente permitir que las etiquetas de seguridad de usuario se cambien si se emplea un enlace seguro. Pueden preverse otros medios locales para cambiar las etiquetas de seguridad de usuario de una manera segura.

15.1.6 *Invocación de la operación abstracta de alerta*

La invocación de la operación abstracta de alerta es el resultado del consumo del servicio abstracto de puerto de entrega (véase el § 14.1.1).

Si la acción automática de alerta automática es iniciada por el AU, mediante una operación abstracta de registro en el AM, el servicio abstracto AM sigue los pasos siguientes:

1) Verifica si existe una asociación abstracta. En caso contrario, el AM no establecerá nunca una asociación abstracta, y no podrá invocarse una operación abstracta de alerta.
2) Si existe una operación abstracta, el AM invoca una operación abstracta que contiene la información de argumento pertinente (para más detalles véase el § 8.7.1) y espera a que el AU le devuelva un resultado de alerta vacío como indicación de éxito.
3) Si no existe una asociación abstracta, existe la posibilidad de utilizar un protocolo no normalizado para informar al usuario. La señal de alerta en este caso puede darse en el terminal de usuario, pero, alternativamente, se puede dar por teléfono, por un indicador acústico, o por cualquier equipo terminal adecuado asociado con el usuario. Este último método puede utilizarse también en casos en que no se haya realizado la operación abstracta de alerta.
4) Si se está aplicando una política de seguridad, para garantizar que tal política no será violada durante la alerta, el AM verifica la etiqueta de seguridad de mensaje con respecto al contexto de seguridad. Si la operación abstracta de alerta está prohibida por la política de seguridad o por restricciones temporales de seguridad, la acción será definida por la política de seguridad en vigor.

15.2 *Suministro de los servicios abstractos de puerto de depósito indirecto*

Este punto se refiere a la realización de las operaciones abstractas de depósito de mensaje, depósito de sonda y anulación de entrega diferida, y a la invocación de la operación abstracta de control de depósito. El suministro del servicio abstracto AM de los servicios abstractos de puerto de depósito indirecto presupone que existe una asociación abstracta entre el suministrador del puerto de depósito indirecto (el AM) y el consumidor del puerto de depósito indirecto (el AU). Las operaciones abstractas se realizan en orden secuencial, sin que tenga lugar un procesamiento paralelo. No se describen todos los casos de error.

15.2.1 *Realización de la operación abstracta de depósito de mensaje*

Cuando el AM recibe una operación abstracta de depósito de mensaje y sus argumentos asociados, del AU, sigue los siguientes pasos:

1) Establece que la información de argumento es válida para una operación abstracta de depósito de mensaje; para más detalles véase el § 8.2.1.1.1 de la Recomendación X.411.
2) Verifica los argumentos que han de establecerse si el contenido del mensaje fue suministrado por el AU, o si tiene que ser insertado por el AM (es decir, si está presente la ampliación de petición de retransmisión). En este último caso, si la inscripción es una inscripción de mensaje entregado, se inserta el mensaje correspondiente y se suprimen los argumentos relacionados con el AM. La retransmisión de inscripciones que no son mensajes entregados será objeto de ulterior estudio.
3) Verifica si existe ya una asociación abstracta entre el AM y el ATM. En caso contrario, el AM inicia tal asociación abstracta. Si no puede establecerse una asociación abstracta, se informa al AU, por una indicación de error, de que el depósito no tiene lugar en este momento, y no se sigue adelante.
4) Si existe la asociación abstracta entre el AM y el ATM, el AM invoca una operación abstracta de depósito de mensaje hacia el ATM, después de las eventuales modificaciones que se mencionan en el paso 2).
5) Si el ATM devuelve un resultado de depósito de mensaje (para más detalles véase el § 8.2.1.1.2 de la Recomendación X.411), que indica éxito, el AM devuelve al AU un resultado correspondiente de depósito de mensaje que indica éxito. Obsérvese que el AM nunca devuelve una indicación de éxito al AU hasta haber recibido el correspondiente resultado de retorno del ATM. Esto tiene por objeto asegurar un servicio coherente desde el punto de vista del usuario, es decir, que el depósito entraña siempre que el ATM ha asumido la responsabilidad del mensaje, cuando el resultado regresa.
6) El AM puede elegir entre terminar la asociación abstracta con el ATM después de un cierto periodo de inactividad, o cuando el AU termina su asociación abstracta correspondiente con el AM.

15.2.2 *Realización de la operación abstracta depósito de sonda*

Cuando el AM recibe una operación abstracta de depósito de sonda y sus argumentos asociados, del AU, sigue los pasos siguientes:

1) Establece que la información de argumento es válida para una operación abstracta de depósito de sonda. Para más detalles véase el § 8.2.1.2.1 de la Recomendación X.411.

2) Verifica si ya existe una relación abstracta entre el AM y el ATM. En caso contrario, el AM inicia tal asociación abstracta. Si no puede establecerse una asociación abstracta, el AU es informado, mediante una indicación de error, de que el depósito no puede tener lugar en ese momento, y no se sigue adelante.

3) Si existe la asociación abstracta entre el AM y el ATM, el AM invoca una operación abstracta de depósito de sonda hacia el ATM.

4) Si el ATM devuelve un resultado de depósito de sonda (para más detalles véase el § 8.2.1.2.2 de la Recomendación X.411), que indica éxito, el AM devuelve al AU un resultado correspondiente de depósito de sonda que indica éxito. Obsérvese que el AM nunca devuelve una indicación de éxito al AU antes de haber recibido el resultado correspondiente de retorno del ATM. Esto tiene por objeto asegurar un servicio coherente desde el punto de vista del usuario, es decir, que un depósito siempre entraña que el STRM ha asumido la responsabilidad de la sonda cuando el resultado regresa.

5) El AM puede elegir entre terminar la asociación abstracta con el ATM después de un cierto periodo de inactividad, o cuando el AU termina su asociación abstracta correspondiente con el AM.

15.2.3 *Realización de la operación abstracta anulación de entrega diferida*

Cuando el AM recibe del AU una operación abstracta anulación de entrega diferida y sus argumentos asociados, sigue los pasos siguientes:

1) Establece que la información de argumento es válida para una operación abstracta anulación de entrega diferida. Para más detalles véase el § 8.2.1.3.1 de la Recomendación X.411.

2) Verifica si existe una asociación abstracta entre el AM y el ATM. Si no, el AM inicia tal asociación abstracta. Si no puede establecerse una asociación abstracta el AU es informado por una indicación de error de que la operación de anulación de entrega diferida no puede realizarse en ese momento y dejan de seguirse los demás pasos.

3) Si existe la asociación abstracta entre el AM y el ATM, el AM invoca una operación abstracta anulación de entrega diferida hacia el ATM.

4) Si el ATM devuelve un resultado de anulación de entrega diferida (para más detalles véase el § 8.2.1.3.2 de la Recomendación X.411), que indica éxito, el AM devuelve al AU un resultado correspondiente de anulación de entrega diferida que indica éxito. Obsérvese que el AM nunca devuelve una indicación de éxito al AU antes de haber recibido el resultado correspondiente de retorno del ATM. Esto tiene por objeto asegurar un servicio coherente desde el punto de vista del usuario, es decir, que un depósito entraña siempre que el STM ha asumido la responsabilidad de la sonda, cuando el resultado regresa.

5) El AM puede elegir entre terminar la asociación abstracta con el ATM después de un cierto periodo de inactividad, o cuando el AU termina su asociación abstracta correspondiente con el AM.

15.2.4 *Invocación de la operación abstracta de control de depósito*

Si el AM recibe del ATM una operación abstracta de control de depósito, o si el AM por algún motivo interno, desea detener temporalmente el depósito de mensajes o sondas por el AU, o modificar la longitud máxima o la prioridad más baja de los mensajes procedentes del AU, el AM sigue los pasos siguientes:

1) Invoca una operación abstracta de control de depósito hacia el AU. Para más detalles véase el § 8.2.1.4.1 de la Recomendación X.411.

2) Espera un resultado de control de depósito del AU (para más detalles véase el § 8.2.1.4.2 de la Recomendación X.411), en el que se confirma la aceptación de la operación abstracta de control de depósito.

3) Si la operación abstracta de control de depósito había sido desencadenada por una operación abstracta correspondiente, del ATM al AM, el resultado de control de depósito procedente del AU se pasa del AM al ATM, y el AM espera a que el AU le devuelva el resultado de control de depósito.

15.3 *Suministro de los servicios abstractos de puerto de administración*

Este punto trata la realización de operaciones abstractas de registro y cambio de credenciales. El suministro del servicio abstracto AM de los servicios abstractos de puerto de administración presupone que existe una asociación abstracta entre el suministrador del puerto de depósito indirecto (AM) y el consumidor del puerto de depósito indirecto (AU). Las operaciones abstractas se realizan en orden secuencial, sin que tenga lugar un procesamiento paralelo. No se describen todos los casos de error.

15.3.1 *Realización de la operación abstracta de registro*

Cuando el AM recibe del AU una operación abstracta de registro y sus argumentos asociados, sigue los pasos siguientes:

1) Establece que la información de argumento es válida para una operación abstracta de registro. Para más detalles véase el § 8.4.1.1.1 de la Recomendación X.411.
2) Verifica si ya existe una asociación abstracta entre el AM y el ATM. En caso contrario, el AM inicia tal asociación abstracta. Si no puede establecerse una asociación abstracta, el AU es informado por una indicación de error de que el depósito no puede tener lugar en este momento y no se sigue adelante.
3) Si existe la asociación abstracta entre el AM y el ATN, el AM invoca una operación abstracta de registro, hacia el ATM.
4) Si el ATM devuelve un resultado de registro (para más detalles véase el § 8.4.1.1.2 de la Recomendación X.411) que indica éxito, el AM devuelve al AU el resultado correspondiente de registro que indica éxito. Obsérvese que el AM nunca devuelve al AU una indicación de éxito antes de haber recibido el resultado correspondiente devuelto por el ATM. Esto tiene por objeto asegurar un servicio coherente desde el punto de vista del usuario, es decir, que un depósito entraña siempre que el STRM ha asumido la responsabilidad del registro cuando regresa el resultado.
5) El AM puede elegir entre terminar la asociación abstracta con el ATM después de un cierto periodo de inactividad, o cuando el AU termina su asociación abstracta correspondiente con el AM.
6) El ámbito de los cambios que el AU está autorizado a introducir en las etiquetas de seguridad de usuario estará circunscrito por la política de seguridad en vigor. Algunas políticas de seguridad pueden permitir solamente que se cambien la etiquetas de seguridad de usuario de esta manera si se emplea un enlace seguro. Pueden preverse otros medios locales para cambiar las etiquetas de seguridad de usuario de una manera segura.

15.3.2 *Invocación de la operación abstracta de cambio de credenciales*

Se inicia una operación abstracta de cambio de credenciales porque el ATM invocó una operación abstracta de cambio de credenciales, hacia el AM. A fin de retransmitir las credenciales nuevas desde el ATM al AU, el AM sigue los pasos siguientes:

1) Establece que la información de argumentos es válida para una operación abstracta de cambio de credenciales. Para más detalles véase el § 8.4.1.2 de la Recomendación X.411. Si las credenciales antiguas son incorrectas y las credenciales nuevas no son aceptables, se devuelve una indicación de error, y no se sigue adelante.
2) Invoca una operación abstracta de cambio de credenciales sobre el AU, la cual contiene las nuevas credenciales a registrar. Para más detalles véase el § 8.4.1.2 de la Recomendación X.411.
3) Obtiene en retorno un resultado de cambio de credenciales cuando el AU ha aceptado el cambio y almacena las nuevas credenciales. El resultado de cambio de credenciales, o un error resultante, proveniente del AU, se retransmiten al ATM.

15.3.3 *Realización de la operación abstracta de cambio de credenciales*

Cuando el AM recibe una operación abstracta de cambio de credenciales y sus argumentos asociados desde el AU, sigue los pasos siguientes:

1) Establece que la información de argumento es válida para una operación abstracta de cambio de credenciales. Para más detalles, véase el § 8.4.1.2 de la Recomendación X.411.
2) Verifica si ya existe una asociación abstracta entre el AM y el ATM. Si no existe, el AM inicia tal asociación abstracta. Si no puede establecerse una asociación abstracta, el AU es informado por una indicación de error de que el depósito no tiene lugar en ese momento, y dejan de efectuarse los pasos siguientes.
3) Si existe la asociación abstracta entre el AM y el ATM, el AM invoca una operación abstracta de cambio de credenciales hacia el ATM.

4) Si el ATM devuelve un resultado de cambio de credenciales, que indica éxito, el AM devuelve un resultado correspondiente de cambio de credenciales que indica éxito al AU, y almacena las credenciales. Si el ATM devuelve un error, este se retransmite hacia el AU para indicar ese error. Obsérvese que el AM nunca devuelve una indicación de éxito al AU antes de haber recibido la devolución del resultado correspondiente del ATM.

5) El AM puede elegir entre terminar la asociación abstracta con el ATM después de cierto periodo de inactividad, o cuando el AU termina su operación abstracta correspondiente con el AM.

16 Realización de puertos

Este punto describe cómo se proporcionan los puertos de extracción, depósito y administración del servicio abstracto AM. Para una descripción de la forma en que el servicio abstracto STRM proporciona los puertos de entrega, depósito y administración, véase el § 8 de la Recomendación X.411.

16.1 *Puerto de extracción*

Los servicios abstractos de puerto de extracción se realizan mediante una correspondencia biunívoca entre operaciones abstractas y operaciones reales en el elemento de servicio de extracción de mensajes (ESEM) descrito en la Recomendación X.419.

16.2 *Puerto de depósito indirecto*

Los servicios abstractos de puerto de depósito indirecto se realizan mediante una correspondencia biunívoca entre operaciones abstractas y operaciones reales en el elemento de servicio de depósito de mensajes (ESDM) que se describe en la Recomendación X.419.

16.3 *Puerto de administración*

Los servicios abstractos de puerto de administración se realizan mediante una correspondencia biunívoca entre operaciones abstractas y operaciones reales en el elemento de servicio de administración de mensaje (ESAM) que se describe en la Recomendación X.419.

ANEXO A

(a la Recomendación X.413)

Asignación formal de identificadores de objeto

Este anexo es parte integrante de esta Recomendación.

Todos los identificadores de objeto asignados por esta Recomendación son asignados formalmente en el presente anexo utilizando la NSA.1. Los valores especificados se citan en los módulos NSA.1 de los anexos siguientes.

Este anexo es definitivo para todos los valores salvo para los módulos NSA.1 y para toda la materia relativa a esta Recomendación. Las asignaciones definitivas para los valores primeramente mencionados se presentan en los módulos propiamente dichos. La asignación para los segundos es fija. Otras referencias a los valores asignados a los módulos figuran en cláusulas IMPORT.

```
MSObjectIdentifiers
        {joint-iso-ccitt mhs-motis(6) ms(4) modules(0) object-identifiers(0)}
DEFINITIONS ::=
BEGIN


-- Prólogo
-- Exporta todo

IMPORTS
        ID, id-ms
            FROM MHSObjectIdentifiers {joint-iso-ccitt mhs-motis(6) arch(5) modules(0) object-identifiers(0)};
```

-- *Categorías*

```
id-mod -- modules           -- ID ::= {id-ms 0}
id-ot  -- objects           -- ID ::= {id-ms 1}
id-pt  -- port types        -- ID ::= {id-ms 2}
id-att -- attribute types   -- ID ::= {id-ms 3}
id-act -- auto-action types -- ID ::= {id-ms 4}
```

-- *Módulos*

```
id-mod-object-identifiers   ID ::= {id-mod 0} -- not definitive
id-mod-abstract-service     ID ::= {id-mod 1} -- not definitive
id-mod-attribute-types      ID ::= {id-mod 2} -- not definitive
id-mod-action-types         ID ::= {id-mod 3} -- not definitive
id-mod-upper-bounds         ID ::= {id-mod 4} -- not definitive
```

-- *Objetos*

```
id-ot-ms                    ID ::= {id-ot 0}
id-ot-ms-user               ID ::= {id-ot 1}
```

-- *Tipos de puerto*

```
id-pt-retrieval             ID ::= {id-pt 0}
```

-- *Tipos de atributo*

```
id-att-child-sequence-numbers                       ID ::= {id-att 0}
id-att-content                                      ID ::= {id-att 1}
id-att-content-confidentiality-algorithm-identifier ID ::= {id-att 2}
id-att-content-correlator                           ID ::= {id-att 3}
id-att-content-identifier                           ID ::= {id-att 4}
id-att-content-integrity-check                      ID ::= {id-att 5}
id-att-content-length                               ID ::= {id-att 6}
id-att-content-returned                             ID ::= {id-att 7}
id-att-content-type                                 ID ::= {id-att 8}
id-att-conversion-with-loss-prohibited              ID ::= {id-att 9}
id-att-converted-EITs                               ID ::= {id-att 10}
id-att-creation-time                                ID ::= {id-att 11}
id-att-delivered-EITs                               ID ::= {id-att 12}
id-att-delivery-flags                               ID ::= {id-att 13}
id-att-dl-expansion-history                         ID ::= {id-att 14}
id-att-entry-status                                 ID ::= {id-att 15}
id-att-entry-type                                   ID ::= {id-att 16}
id-att-intended-recipient-name                      ID ::= {id-att 17}
id-att-message-delivery-envelope                    ID ::= {id-att 18}
id-att-message-delivery-identifier                  ID ::= {id-att 19}
id-att-message-delivery-time                        ID ::= {id-att 20}
id-att-message-origin-authentication-check          ID ::= {id-att 21}
id-att-message-security-label                       ID ::= {id-att 22}
id-att-message-submission-time                      ID ::= {id-att 23}
id-att-message-token                                ID ::= {id-att 24}
id-att-original-EITs                                ID ::= {id-att 25}
id-att-originator-certificate                       ID ::= {id-att 26}
id-att-originator-name                              ID ::= {id-att 27}
id-att-other-recipient-names                        ID ::= {id-att 28}
```

```
id-att-parent-sequence-number                    ID ::= { id-att 29 }
id-att-per-recipient-report-delivery-fields      ID ::= { id-att 30 }
id-att-priority                                  ID ::= { id-att 31 }
id-att-priority-of-delivery-request              ID ::= { id-att 32 }
id-att-redirection-history                       ID ::= { id-att 33 }
id-att-report-delivery-envelope,                 ID ::= { id-att 34 }
id-att-reporting-DL-name                         ID ::= { id-att 35 }
id-att-reporting-MTA-certificate                 ID ::= { id-att 36 }
id-att-report-origin-authentication-check        ID ::= { id-att 37 }
id-att-security-classification                   ID ::= { id-att 38 }
id-att-sequence-number                           ID ::= { id-att 39 }
id-att-subject-submission-identifier             ID ::= { id-att 40 }
id-att-this-recipient-name                       ID ::= { id-att 41 }
```

-- *Tipos de acciones automáticas*

```
id-act-auto-forward                              ID ::= { id-act 0 }
id-act-auto-alert                                ID ::= { id-act 1 }
```

END -- *de Identificadores de objeto MSI*

ANEXO B

(a la Recomendación X.413)

Definición formal del servicio abstracto de almacenamiento de mensajes

Este anexo es parte integrante de esta Recomendación.

Este anexo, que es un suplemento a la sección 2, define formalmente el servicio abstracto de almacenamiento de mensajes. Emplea la NSA.1 y las macro OBJECT, PORT, ABSTRACT-BIND, ABSTRACT-UNBIND, ABSTRACT-OPERATION, y ABSTRACT-ERROR de la Recomendación X.407.

Nota – La utilización de las macros ABSTRACT-BIND, ABSTRACT-UNBIND, ABSTRACT-OPERATION, y ABSTRACT-ERROR que se derivan de las macros BIND, UNBIND, OPERATION y ERROR del servicio de operaciones a distancia (SOD) no implica que las operaciones abstractas y errores abstractos sean invocados e informados a través de la frontera entre sistemas abiertos en cada caso. Sin embargo, frecuentemente se hará esto. Precisamente la manera de realizar esto es el tema de la Recomendación X.419.

```
MSAbstractService { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) abstract-service(1) }
DEFINITIONS ::=

BEGIN


-- Prólogo
-- Exporta todo

IMPORTS


-- Macros de servicios abstractos

ABSTRACT-BIND, ABSTRACT-ERROR, ABSTRACT-OPERATION, ABSTRACT-UNBIND, OBJECT, PORT
        FROM AbstractServiceNotation { joint-iso-ccitt mhs-motis(6) asdc(2) modules(0) notation(1) }


-- Puertos AM

administration, delivery, submission,
```

```
-- Macro STM

EXTENSION,


-- Macros de servicios abstractos

ContentLength, ContentType, Credentials, InitiatorCredentials, ORAddressAndOrDirectoryName,
ResponderCredentials, SecurityContext, SecurityError, SecurityLabel
        FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }


-- Objetos AM

id-ot-ms, id-ot-ms-user, id-pt-retrieval
        FROM MSObjectIdentifiers { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) object-identifiers(0) }

-- Cota superior del servicio abstracto AM

ub-attributes-supported, ub-attribute-values, ub-auto-actions, ub-auto-registrations,
ub-default-registrations, ub-error-reasons, ub-information-bases, ub-messages,
ub-nested-filters, ub-per-auto-action, ub-per-entry, ub-summaries
        FROM MSUpperBounds { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) upper-bounds(4) }


-- Cota superior del servicio abstracto STRM

ub-content-types, ub-encoded-information-types, ub-labels-and-redirections
        FROM MTSUpperBounds { joint-iso-ccitt mhs-motis(6) mts(3) modules(0) upper-bounds(3) };


-- Objetos abstractos AM

MS OBJECT
        PORTS { retrieval[S],
                        indirectSubmission[S],
                        administration[S],
                        delivery[C],
                        submission[C],
                        administration[C] }
        ::= id-ot-ms

msUser OBJECT
        PORTS { retrieval[C],
                        indirectSubmission[C],
                        administration[C] }
        ::= id-ot-ms-user


-- Tipos de puerto

indirectSubmission PORT ::= submission

retrieval PORT
        CONSUMER INVOKES {
                Summarize,
                List,
                Fetch,
                Delete,
                Register-MS }
        SUPPLIER INVOKES {
                Alert }
        ::= id-pt-retrieval
```

```
-- Macros

AUTO-ACTION MACRO ::=
BEGIN
        TYPE NOTATION   ::= Registration
        VALUE NOTATION  ::= value (VALUE OBJECT IDENTIFIER)
        Registration    ::= "REGISTRATION PARAMETER IS" type

END


-- Tipos de datos comunes relacionados con el modelo de información

InformationBase ::= INTEGER {
                stored-messages     (0),
                inlog               (1),
                outlog              (2) } (0. .ub-information-bases)

SequenceNumber ::= INTEGER (0. .ub-messages)

CreationTime ::= UTCTime

Attribute ::= SEQUENCE {
                type        AttributeType,
                values      SEQUENCE SIZE (1. .ub-attribute-values) OF ANY -- DEFINED BY TYPE -- }

AttributeType ::= OBJECT IDENTIFIER

AutoActionRegistration ::= SEQUENCE {
        type                        AutoActionType,
        registration-identifier     [0] INTEGER (1. .ub-per-auto-action) DEFAULT 1,
        registration-parameter      [1] ANY DEFINED BY type }

AutoActionType ::= OBJECT IDENTIFIER

EntryStatus ::= INTEGER {
        new         (0),
        listed      (1),
        processed   (2) }


-- Vinculación abstracta

MSBind ::= ABSTRACT-BIND
        TO { indirectSubmission[S], retrieval[S], administration[S] }
        BIND
                ARGUMENT        MSBindArgument
                RESULT          MSBindResult
                BIND-ERROR      MSBindError

MSUnbind ::= ABSTRACT-UNBIND
        FROM { indirectSubmission[S], retrieval[S], administration[S] }

MSBindArgument ::= SET {
        initiator-name              ORAddressAndOrDirectoryName,
        initiator-credentials       [2] InitiatorCredentials,
        security-context            [3] IMPLICIT SecurityContext OPTIONAL,
        fetch-restrictions          [4] Restrictions OPTIONAL -- por defecto: ninguno --,
        ms-configuration-request    [5] BOOLEAN DEFAULT FALSE, }

Restrictions ::= SET {
        allowed-content-types       [0] SET SIZE (1. .ub-content-types) OF OBJECT IDENTIFIER
                                        OPTIONAL
            -- default is no restriction --,
        allowed-EITs                [1] MS-EITs OPTIONAL -- por defecto: sin restricción --,
        maximum-content-length      [2] ContentLength OPTIONAL -- por defecto: sin restricción -- }
```

```
MS-EITs ::= SET SIZE (1..ub-encoded-information-types) OF MS-EIT

MS-EIT ::= OBJECT IDENTIFIER

MSBindResult ::= SET{
        responder-credentials           [2] ResponderCredentials,
        available-auto-actions          [3] SET SIZE (1..ub-auto-actions) OF AutoActionType OPTIONAL,
        available-attribute-types       [4] SET SIZE (1..ub-attributes-supported) OF AttributeType
                                            OPTIONAL,
        alert-indication                [5] BOOLEAN DEFAULT FALSE,
        content-types-supported         [6] SET SIZE (1..ub-content-types) OF OBJECT IDENTIFIER
                                            OPTIONAL}

MSBindError ::= ENUMERATED{
        authentication-error            (0),
        unacceptable-security-context   (1),
        unable-to-establish-association (2)}


-- Tipos de datos comunes para operaciones abstractas

Range ::= CHOICE{
        sequence-number-range           [0] NumberRange,
        creation-time-range             [1] TimeRange}

NumberRange ::= SEQUENCE{
        from        [0] SequenceNumber OPTIONAL -- omitido significa sin cota inferior --,
        to          [1] SequenceNumber OPTIONAL -- omitido significa sin cota superior --}

TimeRange ::= SEQUENCE{
        from        [0] CreationTime OPTIONAL -- omitido significa sin cota inferior --,
        to          [1] CreationTime OPTIONAL -- omitido significa sin cota superior --}

Filter ::= CHOICE{
        item        [0] FilterItem,
        and         [1] SET SIZE (1..ub-nested-filters) OF Filter,
        or          [2] SET SIZE (1..ub-nested-filters) OF Filter,
        not         [3] Filter}

FilterItem ::= CHOICE{
        equality                [0] AttributeValueAssertion,
        substrings              [1] SEQUENCE{
            type                AttributeType,
            strings             SEQUENCE SIZE (1..ub-attribute-values) OF CHOICE{
                initial             [0] ANY -- DEFINED BY type --,
                any                 [1] ANY -- DEFINED BY type --,
                final               [2] ANY -- DEFINED BY type --}},
        greater-or-equal        [2] AttributeValueAssertion,
        less-or-equal           [3] AttributeValueAssertion,
        present                 [4] AttributeType,
        approximate-match       [5] AttributeValueAssertion}

AttributeValueAssertion ::= SEQUENCE{
        type        AttributeType,
        value       ANY DEFINED BY type}

Selector ::= SET{
        child-entries   [0] BOOLEAN DEFAULT FALSE,
        range           [1] Range OPTIONAL -- por defecto: no vinculado --,
        filter          [2] Filter OPTIONAL -- por defecto: todos los asientos dentro de la gama especificadd --,
        limit           [3] INTEGER (1..ub-messages) OPTIONAL,
        override        [4] OverrideRestrictions OPTIONAL -- por defecto: cualquier restricción en vigor si se
                            aplica --}

OverrideRestrictions ::= BIT STRING{
        overrideContentTypesRestriction     (0),
        overrideEITsRestriction             (1),
        overrideContentLengthRestriction    (2)} (SIZE (1..ub-information-bases))

EntryInformationSelection::= SET SIZE(0..ub-per-entry) OF AttributeSelection
```

```
AttributeSelection ::= SET{
        type            AttributeType,
        from            [0] INTEGER (1..ub-attribute-values) OPTIONAL -- se usa si el tipo es de múltiples
                        valores --,
        count           [1] INTEGER (1..ub-attribute-values) OPTIONAL -- se usa si el tipo es de múltiples
                        valores -- }

EntryInformation ::= SEQUENCE{
        sequence-number         SequenceNumber,
        attributes              SET SIZE (1..ub-per-entry) OF Attribute OPTIONAL }


-- Parámetro de petición de retransmisión para depósito indirecto

forwarding-request EXTENSION
        SequenceNumber
        CRITICAL FOR SUBMISSION
        ::= 36


-- Operaciones abstractas

Summarize ::= ABSTRACT-OPERATION
        ARGUMENT        SummarizeArgument
        RESULT          SummarizeResult
        ERRORS{
                AttributeError,
                InvalidParametersError,
                RangeError,
                SecurityError,
                SequenceNumberError,
                ServiceError }

SummarizeArgument ::= SET{
        information-base-type   [0] InformationBase DEFAULT stored-messages,
        selector                [1] Selector,
        summary-requests        [2] SEQUENCE SIZE (1..ub-summaries) OF Attribute Type OPTIONAL
                -- ausente si no se solicitan resúmenes -- }

SummarizeResult ::= SET{
        next            [0] SequenceNumber OPTIONAL,
        count           [1] INTEGER (0..ub-messages) -- de las inscripciones solicitadas --,
        span            [2] Span OPTIONAL -- de las inscripciones seleccionadas, se omite si cuenta es cero --,
        summaries       [3] SEQUENCE SIZE (1..ub-summaries) OF Summary OPTIONAL }

Span ::= SEQUENCE{
        lowest          [0] SequenceNumber,
        highest         [1] SequenceNumber }

Summary ::= SET{
        absent          [0] INTEGER (1..ub-messages) OPTIONAL -- cómputo de inscripciones donde el atributo
                            está ausente --,
        present         [1] SET SIZE (1..ub-attribute-values) OF -- uno para cada valor de atributo presente --
                                SEQUENCE{
                                    type        AttributeType,
                                    value       ANY DEFINED BY type,
                                    count       INTEGER (1..ub-messages) } OPTIONAL }

List ::= ABSTRACT-OPERATION
                ARGUMENT        ListArgument
                RESULT          ListResult
                ERRORS{
                    AttributeError,
                    InvalidParametersError,
                    RangeError,
                    SecurityError,
                    SequenceNumberError,
                    ServiceError }
```

```
ListArgument ::= SET{
        information-base-type       [0] InformationBase DEFAULT stored-messages,
        selector                    [1] Selector,
        requested-attributes        [3] EntryInformationSelection OPTIONAL}

ListResult ::= SET{
        next            [0] SequenceNumber OPTIONAL,
        requested       [1] SEQUENCE SIZE (1..ub-messages) OF EntryInformation OPTIONAL -- omitido si no
                            se encuentra ninguno --}

--

Fetch ::= ABSTRACT-OPERATION
                ARGUMENT            FetchArgument
                RESULT              FetchResult
                ERRORS{
                    AttributeError,
                    FetchRestrictionError,
                    InvalidParametersError,
                    RangeError,
                    SecurityError,
                    SequenceNumberError,
                    ServiceError}

FetchArgument ::= SET{
        information-base-type       [0] InformationBase DEFAULT stored-messages,
        item                            CHOICE{
                search                          [1] Selector,
                precise                         [2] SequenceNumber},
        requested-attributes        [3] EntryInformationSelection OPTIONAL}

FetchResult ::= SET{
        entry-information           [0] EntryInformation OPTIONAL -- si se seleccionó alguna inscripción --,
        list                        [1] SEQUENCE SIZE (1..ub-messages) OF SequenceNumber OPTIONAL,
        next                        [2] SequenceNumber OPTIONAL}

--

Delete ::= ABSTRACT-OPERATION
                ARGUMENT            DeleteArgument
                RESULT              DeleteResult
                ERRORS{
                    DeleteError,
                    InvalidParametersError,
                    RangeError,
                    SecurityError,
                    SequenceNumberError,
                    ServiceError}

DeleteArgument ::= SET{
        information-base-type       [0] InformationBaseDEFAULT stored-messages,
        items                           CHOICE{
                selector                        [1] Selector
                sequence-numbers                [2] SET SIZE (1..ub-messages) OF SequenceNumber}}

DeleteResult ::= NULL

--

Register-MS ::= ABSTRACT-OPERATION
                ARGUMENT            Register-MSArgument
                RESULT              Register-MSResult
                ERRORS{
                    AttributeError,
                    AutoActionRequestError,
                    InvalidParametersError,
                    SecurityError,
                    ServiceError}
```

```
Register-MSArgument ::= SET{
        auto-action-registrations       [0] SET SIZE (1..ub-auto-registrations) OF AutoActionRegistration
                                            OPTIONAL,
        auto-action-deregistrations     [1] SET SIZE (1..ub-auto-registrations) OF AutoActionDeregistration
                                            OPTIONAL,
        list-attribute-defaults         [2] SET SIZE (1..ub-default-registrations) OF AttributeType OPTIONAL,
        fetch-attribute-defaults        [3] SET SIZE (1..ub-default-registrations) OF AttributeType OPTIONAL,
        change-credentials              [4] SEQUENCE{
                old-credentials                 [0] IMPLICIT Credentials,
                new-credentials                 [1] IMPLICIT Credentials} OPTIONAL
                    -- same CHOICE as for old-credentials --,
        user-security-labels            [5] SET SIZE (1..ub-labels-and-redirections) OF SecurityLabel OPTIONAL}

AutoActionDeregistration ::= AutoActionRegistration
                                (WITH COMPONENTS{..., registration-parameter ABSENT})

Register-MSResult ::= NULL

--

Alert ::= ABSTRACT-OPERATION
                ARGUMENT        AlertArgument
                RESULT          AlertResult
                ERRORS{
                    SecurityError}

AlertArgument ::= SET{
        alert-registration-identifier   [0] INTEGER (1..ub-auto-actions),
        new-entry                       [2] EntryInformation OPTIONAL}

AlertResult ::= NULL


-- Errores abstractos

AttributeError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problems [0]        SET SIZE (1..ub-per-entry) OF SET{
                    problem         [0] AttributeProblem,
                    type            [1] AttributeType,
                    value           [2] ANY DEFINED BY type OPTIONAL}}

AttributeProblem ::= INTEGER{
        invalid-attribute-value         (0),
        unavailable-attribute-type      (1),
        inappropriate-matching          (2),
        attribute-type-not-subscribed   (3),
        inappropriate-for-operation     (4)} (0..ub-error-reasons)

--

AutoActionRequestError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problems [0]        SET SIZE (1..ub-auto-registrations) OF SET{
                    problem         [0] AutoActionRequestProblem,
                    type            [1] AutoActionType}}

AutoActionRequestProblem ::= INTEGER{
        unavailable-auto-action-type    (0),
        auto-action-type-not-subscribed (1)} (0..ub-error-reasons)

--
```

```
DeleteError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problems [0]            SET SIZE (1. .ub-messages) OF SET{
                    problem             [0] DeleteProblem,
                    sequence-number     [1] SequenceNumber}}

DeleteProblem ::= INTEGER{
        child-entry-specified           (0),
        delete-restriction-problem      (1)} (0. .ub-error-reasons)

--

FetchRestrictionError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problems [0]                SET SIZE (1. .ub-default-registrations) OF SET{
                    problem                 [3] FetchRestrictionProblem,
                    restriction             CHOICE{
                        content-type            [1] ContentType,
                        eit                     [2] MS-EITs,
                        content-length          [3] ContentLength}}}

FetchRestrictionProblem ::= INTEGER{
        content-type-problem    (1),
        eit-problem             (2),
        content-length-problem  (3)} (0. .ub-error-reasons)

--

InvalidParametersError ::= ABSTRACT-ERROR
        PARAMETER  NULL

--

RangeError ::= ABSTRACT-ERROR

        PARAMETER           SET{
                problem     [0] RangeProblem}

RangeProblem ::= INTEGER{
        reversed    (0)} (0. .ub-error-reasons)

--

SequenceNumberError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problems [1]            SET SIZE (1. .ub-messages) OF SET{
                    problem             [0] SequenceNumberProblem,
                    sequence-number     [1] SequenceNumber}}

SequenceNumberProblem ::= INTEGER{
        no-such-entry    (0)} (0. .ub-error-reasons)

--

ServiceError ::= ABSTRACT-ERROR
        PARAMETER           SET{
                problem     [0] ServiceProblem}

ServiceProblem ::= INTEGER{
        busy                    (0),
        unavailable             (1),
        unwilling-to-perform    (2)} (0. .ub-error-reasons)


END  -- del servicio abstracto MSA
```

ANEXO C

(a la Recomendación X.413)

Definición formal de tipos de atributos generales

Este anexo es parte integrante de esta Recomendación.

Este anexo, que es un suplemento a la sección 3, define formalmente los tipos de atributos generales aplicables a todas las formas de tratamiento de mensajes, y no solamente a una. Emplea la NSA.1 y la macro ATTRIBUTE.

```
MSGeneralAttributeTypes { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) general-attribute-types(2) }
DEFINITIONS ::=

BEGIN


-- Prólogo
-- Exporta todo


IMPORTS

    -- Identificadores de objeto de tipos de atributos generales
    id-att-child-sequence-numbers, id-att-content, id-att-content-confidentiality-algorithm-identifier,
    id-att-content-correlator, id-att-content-identifier, id-att-content-integrity-check, id-att-content-length,
    id-att-content-returned, id-att-content-type, id-att-conversion-with-loss-prohibited, id-att-converted-EITs,
    id-att-creation-time, id-att-delivered-EITs, id-att-delivery-flags, id-att-dl-expansion-history,
    id-att-entry-status, id-att-entry-type, id-intended-recipient-name, id-att-message-delivery-envelope,
    id-att-message-delivery-identifier, id-att-message-delivery-time, id-att-message-origin-authentication-check,
    id-att-message-security-label, id-att-message-submission-time, id-att-message-token, id-att-original-EITs,
    id-att-originator-certificate, id-att-originator-name, id-att-other-recipient-names,
    id-att-parent-sequence-number, id-att-priority, id-att-proof-of-delivery-request, id-att-redirection-history,
    id-att-report-delivery-envelope, id-att-reporting-DL-name, id-att-reporting-MTA-certificate,
    id-att-report-origin-authentication-check, id-att-sequence-number, id-att-subject-submission-identifier,
    id-att-this-recipient-name
        FROM MSObjectIdentifiers { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) object-identifiers(0) }

    -- Macros de atributo
    ATTRIBUTE, ATTRIBUTE-SYNTAX
        FROM InformationFramework { joint-iso-ccitt ds(5) modules(1) informationFramework(1) }

    -- Tipos de datos del servicio abstracto AM
    CreationTime, EntryStatus, MS-EIT, SequenceNumber
        FROM MSAbstractService { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) abstract-service(1) }

    -- Tipos de datos del servicio autenticación
    AlgorithmIdentifier
        FROM AuthenticationFramework { joint-iso-ccitt ds(5) modules(1) authentication-framework(7) }

    -- Tipos de datos del servicio abstracto STRM
    Content, ContentCorrelator, ContentIdentifier, ContentIntegrityCheck, ContentLength,
    ConversionWithLossProhibited, DeliveryFlags, DLExpansionHistory, MessageDeliveryEnvelope,
    MessageDeliveryIdentifier, MessageDeliveryTime, MessageOriginAuthenticationCheck,
    MessageSecurityLabel, MessageSubmissionTime, MessageToken, OriginatorCertificate, ORName,
    PerRecipientReportDeliveryFields, Priority, ProofOfDeliveryRequest, RedirectionHistory,
    ReportDeliveryEnvelope, ReportingDLName, ReportingMTACertificate,
    ReportOriginAuthenticationCheck, SecurityClassification, subjectSubmissionIdentifier
        FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
        mts-abstract-service(1) }

    -- Cota superior del servicio abstracto AM
    ub-entry-types
        FROM MSUpperBounds { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) upper-bounds(4) };
```

-- *Tipos de atributo*

```
ms-child-sequence-numbers ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MULTI VALUE
        ::= id-att-child-sequence-numbers


ms-content ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Content
        SINGLE VALUE
        ::= id-att-content


mt-content-confidentiality-algorithm-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AlgorithmIdentifier
        SINGLE VALUE
        ::= id-att-content-confidentiality-algorithm-identifier


mt-content-correlator ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ContentCorrelator
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-content-correlator


mt-content-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ContentIdentifier
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-content-identifier


mt-content-integrity-check ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ContentIntegrityCheck
        SINGLE VALUE
        ::= id-att-content-integrity-check


ms-content-length ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ContentLength
        MATCHES FOR ORDERING
        SINGLE VALUE
        ::= id-att-content-length


ms-content-returned ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX BOOLEAN
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-content-returned


mt-content-type ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OBJECT IDENTIFIER
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-content-type


mt-conversion-with-loss-prohibited ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ConversionWithLossProhibited
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-conversion-with-loss-prohibited
```

```
ms-converted-EITs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EIT
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-att-converted-EITs

ms-creation-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX CreationTime
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-creation-time

ms-delivered-EITs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EIT
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-att-delivered-EITs

mt-delivery-flags ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DeliveryFlags
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-delivery-flags

mt-dl-expansion-history ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DLExpansionHistory
        MULTI VALUE
        ::= id-att-dl-expansion-history

ms-entry-status ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EntryStatus
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-entry-status

ms-entry-type ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EntryType
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-entry-type

EntryType ::= INTEGER {
        delivered-message       (0),
        delivered-report        (1),
        returned-content        (2) (0. .ub-entry-types) }

mt-intended-recipient-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-intended-recipient-name

mt-message-delivery-envelope ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryEnvelope
        SINGLE VALUE
        ::= id-att-message-delivery-envelope

mt-message-delivery-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryIdentifier
        SINGLE VALUE
        ::= id-att-message-delivery-identifier

mt-message-delivery-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageDeliveryTime
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-message-delivery-time
```

```
mt-message-origin-authentication-check ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageOriginAuthenticationCheck
        SINGLE VALUE
        ::= id-att-message-origin-authentication-check

mt-message-security-label ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageSecurityLabel
        SINGLE VALUE
        ::= id-att-message-security-label

mt-message-submission-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageSubmissionTime
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-message-submission-time

mt-message-token ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageToken
        SINGLE VALUE
        ::= id-att-message-token

ms-original-EITs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EIT
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-att-original-EITs

mt-originator-certificate ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OriginatorCertificate
        SINGLE VALUE
        ::= id-att-originator-certificate

mt-originator-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-originator-name

mt-other-recipient-names ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-att-other-recipient-names

ms-parent-sequence-number ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-parent-sequence-number

mt-per-recipient-report-delivery-fields ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX PerRecipientReportDeliveryFields
        MULTI VALUE
        ::= id-att-per-recipient-report-delivery-fields

mt-priority ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Priority
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-priority

mt-proof-of-delivery-request ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ProofOfDeliveryRequest
        SINGLE VALUE
        ::= id-att-proof-of-delivery-request

mt-redirection-history ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RedirectionHistory
        MULTI VALUE
        ::= id-att-redirection-history
```

```
mt-report-delivery-envelope ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportDeliveryEnvelope
        SINGLE VALUE
        ::= id-att-report-delivery-envelope

mt-reporting-DL-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportingDLName
        SINGLE VALUE
        ::= id-att-reporting-DL-name

mt-reporting-MTA-certificate ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportingMTACertificate
        SINGLE VALUE
        ::= id-att-reporting-MTA-certificate

mt-report-origin-authentication-check ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReportOriginAuthenticationCheck
        SINGLE VALUE
        ::= id-att-report-origin-authentication-check

mt-security-classification ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SecurityClassification
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-security-classification

ms-sequence-number ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-att-sequence-number

mt-subject-submission-identifier ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectSubmissionIdentifier
        SINGLE VALUE
        ::= id-att-subject-submission-identifier

mt-this-recipient-name ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORName
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-att-this-recipient-name


END  -- de tipos de atributos generales MSG
```

ANEXO D

(a la Recomendación X.413)

Definición formal de tipos de acciones automáticas generales

Este anexo, es parte integrante de esta Recomendación.

Este anexo, que es un suplemento a la sección 3, define formalmente los tipos de acciones automáticas generales aplicables a todas las formas de tratamiento de mensajes, y no sólo a una de ellas. Emplea la NSA.1 y la macro AUTO-ACTION.

```
MSGeneralAutoActionTypes { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) general-auto-action-types(3) }
DEFINITIONS ::=

BEGIN

-- Prólogo


EXPORTS

        -- Tipos de acciones automáticas generales
        auto-forward, auto-alert;
```

```
IMPORTS
        -- Identificadores de objeto de tipo de acción automática general
        id-act-auto-forward, id-act-auto-alert
                FROM MSObjectIdentifiers {joint-iso-ccitt mhs-motis(6) ms(4) modules(0) object-identifiers(0)}

        -- Macro de acción automática
        AUTO-ACTION,

        -- Tipos de datos del servicio abstracto AM
        Content, Filter, EntryInformationSelection
                FROM MSAbstractService {joint-iso-ccitt mhs-motis(6) ms(4) modules(0) abstract-service(1)}

        -- Tipos de datos del servicio abstracto STRM
        ContentIdentifier, DeferredDeliveryTime, ExplicitConversion, OriginatorName, OriginatorReportRequest,
        PerMessageIndicators, PerMessageSubmissionExtensions, PerRecipientMessageSubmissionExtensions,
        Priority, RecipientName
                FROM MTSAbstractService {joint-iso-ccitt mhs-motis(6) mts(3) modules(0) mts-abstract-
                service(1)}

        -- Cota superior del servicio abstracto AM
        ub-alert-addresses
                FROM MSUpperBounds {joint-iso-ccitt mhs-motis(6) ms(4) modules(0) upper-bounds(4)};

        -- Tipos de acciones
        auto-forward AUTO-ACTION
                REGISTRATION PARAMETER IS AutoForwardRegistrationParameter
                ::= id-act-auto-forward

AutoForwardRegistrationParameter ::= SET{
                filter                          [0] Filter OPTIONAL,
                auto-forward-arguments          [1] AutoForwardArguments,
                delete-after-auto-forwarding    [2] BOOLEAN DEFAULT TRUE,
                other-parameters                [3] OCTET STRING OPTIONAL}

AutoForwardArguments ::= SET{
                COMPONENTS OF PerMessageAutoForwardFields,
                per-recipient-fields    [1] IMPLICIT SEQUENCE SIZE (1..ub-recipients) OF PerRecipient-
                                            AutoForwardFields}

PerMessageAutoForwardFields ::= SET{
                originator-name         OriginatorName,
                content-identifier      ContentIdentifier OPTIONAL,
                priority                Priority DEFAULT normal,
                per-message-indicators  PerMessageIndicators DEFAULT {},
                deferred-delivery-time  [0] IMPLICIT DeferredDeliveryTime OPTIONAL,
                extensions              [2] IMPLICIT PerMessageSubmissionExtensions DEFAULT {}}

PerRecipientAutoForwardFields ::= SET{
                recipient-name          RecipientName,
                originator-report-request [0] IMPLICIT OriginatorReportRequest,
                explicit-conversion     [1] IMPLICIT ExplicitConversion OPTIONAL,
                extensions              [2] IMPLICIT PerRecipientMessageSubmissionExtensions
                                            DEFAULT {}}

auto-alert AUTO-ACTION
                REGISTRATION PARAMETER IS AutoAlertRegistrationParameter
                ::= id-act-auto-alert

AutoAlertRegistrationParameter ::= SET{
                filter                  [0] Filter OPTIONAL,
                alert-addresses         [1] SEQUENCE SIZE (1..ub-alert-addresses) OF AlertAddress
                                            OPTIONAL,
                requested-attributes    [2] EntryInformationSelection OPTIONAL}

AlertAddress ::= SEQUENCE{
                address         EXTERNAL,
                alert-qualifier OCTET STRING OPTIONAL}


END  -- de tipos de acciones automáticas generales MSG
```

ANEXO E

(a la Recomendación X.413)

Definición formal de límites superiores de parámetros AM

Este anexo es parte integrante de esta Recomendación.

Este anexo define para fines de referencia los límites superiores de diversos tipos de datos de longitud variable cuyas sintaxis abstractas se definen en módulos NSA.1 en el cuerpo de esta Recomendación.

```
MSUpperBounds { joint-iso-ccitt mhs-motis(6) ms(4) modules(0) upper-bounds(4) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo
IMPORTS -- nada --;


-- Cota superior
ub-alert-addresses          INTEGER ::= 16
ub-attribute-values         INTEGER ::= 32767        -- (2^15 - 1) el mayor entero que puede representarse con
                                                        16 bits --
ub-attributes-supported     INTEGER ::= 1024
ub-auto-actions             INTEGER ::= 16
ub-auto-registrations       INTEGER ::= 1024
ub-default-registrations    INTEGER ::= 1024
ub-entry-types              INTEGER ::= 16
ub-error-reasons            INTEGER ::= 16
ub-information-bases        INTEGER ::= 16
ub-messages                 INTEGER ::= 2147483647   -- (2^31 - 1) el mayor entero que puede representarse con
                                                        32 bits --
ub-nested-filters           INTEGER ::= 32
ub-per-auto-action          INTEGER ::= 32767        -- (2^15 - 1) el mayor entero que puede representarse con
                                                        16 bits --
ub-per-entry                INTEGER ::= 1024
ub-summaries                INTEGER ::= 16


END -- de cotas superiores MSU
```

ANEXO F

Ejemplos de la operación abstracta de resumir

Este anexo no es parte integrante de esta Recomendación.

Este anexo contiene un ejemplo del uso de la operación abstracta de resumir.

F.1 *Las inscripciones en el ejemplo AM*

Considérese un AM que contiene las siguientes inscripciones, una por cada línea. Las columnas muestran los valores de los tipos de atributo indicados. Un «–» indica que el atributo está ausente de la inscripción.

CUADRO F-1/X.413

Mensajes almacenados en el ejemplo

Número secuencial	Tipo de la inscripción	Estado de la inscripción	Prioridad
3	mensaje	listado	urgente
5	mensaje	listado	baja
8	informe	listado	–
10	mensaje	listado	normal
15	informe	nuevo	–
18	mensaje	nuevo	normal
20	mensaje	nuevo	urgente
22	mensaje	nuevo	normal
23	mensaje	nuevo	normal

Nota – Si se omite la prioridad en un sobre de entrega de un mensaje de un mensaje y el valor por defecto es «normal», el atributo correspondiente está presente y se le da su valor por defecto.

F.2 *Ejemplo de una petición de resumen*

Supóngase que se requiere resumir todas las inscripciones «nuevas» por prioridad. El resultado requerido es la siguiente lista de cómputos. Los números entre paréntesis son números secuenciales de los mensajes que contribuyen a ese cómputo. Véase el cuadro F-2/X.413.

CUADRO F-2/X.413

Resultado esperado de listar-resumir

Prioridad	Cómputo
–	1 (15)
urgente	1 (20)
normal	3 (18,22,23)
baja	0

Los componentes del argumento-resumir deben establecerse como sigue:

selector:

filtro:	Estado de la inscripción = nueva
peticiones de resumir	tipo de atributo = Prioridad

Los componentes del resultado de resumir podrían ser los siguientes:

cómputo:	5
intervalo:	
más bajo:	15
más alto:	23
resúmenes:	
{ ausente:	1
presente:	{ valor = normal, cómputo = 3 }
	{ valor = urgente, cómputo = 1 } }

ANEXO G

Diferencias entre el texto de la Recomendación X.413 del CCITT y el texto de la Norma ISO/CEI 10021-5

Este anexo no es parte integrante de esta Recomendación.

Sólo existen tres diferencias entre la Recomendación X.413 del CCITT y el MOTIS de la Norma ISO/CEI 10021-5.

1) El texto del CCITT contiene una restricción en el § 7.1 según la cual sólo puede existir en cualquier momento una asociación abstracta entre el AM y el usuario AM. Esta restricción *no* está incluida en el texto ISO/CEI.

2) Las partes de la notación NSA.1 que expresan límites superiores y se documentan en el anexo E, no se consideran constitutivas de la norma MOTIS, pero con una parte formal de la Recomendación X.413.

   En la ISO, este nivel de funcionalidad está bajo la responsabilidad del Grupo Especial sobre Normalización Funcional, que publica *Internationally Standardized Profiles* (ISP); esta publicación contiene, por ejemplo, límites superiores para elementos de protocolo.

Recomendación X.419

SISTEMAS DE TRATAMIENTO DE MENSAJES: ESPECIFICACIONES DE PROTOCOLO [1]

(Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y servicios de mensajes con almacenamiento y retransmisión controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) la necesidad de transferir y almacenar mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones especificadas por el CCITT;

(e) que las Recomendaciones de la serie X.500 definen los sistemas de guías;

(f) que los sistemas de tratamiento de mensajes se definen en la serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419; y

g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

(1) que el protocolo para el acceso al sistema de transferencia de mensajes (protocolo de acceso STRM-P3) se define en la sección 2;

(2) que el protocolo para el acceso al almacenamiento de mensajes (protocolo de acceso AM-P7) se define también en la sección 2;

(3) que el protocolo utilizado entre agentes de transferencia de mensajes (AMT) para proporcionar la operación distribuida del sistema de transferencia de mensajes (protocolo de transferencia STRM-P1) se define en la sección 3.

ÍNDICE

Sección 1 – *Introducción*

0 Introducción

1 Campo de aplicación

2 Referencias

3 Definiciones

4 Abreviaturas

5 Convenios

[1] La Recomendación X.419 y la Norma ISO 10021-6 [Information Processing Systems – Text Communication – MOTIS – Protocol Specifications] fueron preparadas en estrecha colaboración y están técnicamente armonizadas, salvo en lo que respecta a las diferencias indicadas en el anexo D.

Sección 2 – *Especificaciones del protocolo de acceso al sistema de tratamiento de mensajes (STM)*

6 Descripción general de los protocolos de acceso STM

7 Definición de la sintaxis abstracta del protocolo de acceso al sistema de transferencia de mensajes (STRM)

8 Definición de la sintaxis abstracta del protocolo de acceso al almacenamiento de mensajes (AM)

9 Relación de correspondencia con los servicios utilizados

10 Conformidad

Sección 3 – *Especificaciones del protocolo de transferencia del sistema de transferencia de mensajes (STRM)*

11 Visión de conjunto del protocolo de transferencia del STRM

12 Definición de la sintaxis abstracta del protocolo de transferencia del STRM

13 Relación de correspondencia con los servicios utilizados

14 Conformidad

Anexo A – Definición de referencia de identificadores de objeto del protocolo del sistema de tratamiento de mensajes (STM)

Anexo B – Interfuncionamiento con los sistemas de 1984

Anexo C – Diferencias entre los protocolos del sistema de tratamiento de mensajes de 1984 y de 1988

Anexo D – Diferencias entre las versiones del CCITT y de la ISO

0 Introducción

Esta Recomendación pertenece a un conjunto de Recomendaciones que definen el tratamiento de mensajes en un entorno de sistemas abiertos distribuidos.

El tratamiento de mensajes proporciona el intercambio de mensajes entre usuarios sobre la base de almacenamiento y retransmisión. Un mensaje depositado por un usuario (el *originador*) es transferido a través del sistema de transferencia de mensajes (STRM) y entregado a uno o más usuarios (los *destinatarios*). Un usuario puede interactuar directamente con el STRM, o indirectamente a través de un almacenamiento de mensajes (AM).

El STRM comprende varios agentes de transferencia de mensajes (ATM) que transfieren mensajes y los entregan a sus destinatarios deseados.

Esta Recomendación ha sido elaborada conjuntamente por el CCITT y la ISO. El documento equivalente de la ISO es la Norma ISO 10021-6.

1 Campo de aplicación

Esta Recomendación especifica el protocolo de acceso STRM (P3) utilizado entre un agente usuario distante y el STRM para proporcionar acceso al servicio abstracto del STRM definido en la Recomendación X.411.

Esta Recomendación especifica también el protocolo de acceso AM (P7) utilizado entre un agente usuario distante y un almacenamiento de mensajes (AM) para proporcionar acceso al servicio abstracto AM definido en la Recomendación X.413.

Esta Recomendación especifica también el protocolo de transferencia STRM (P1) utilizado entre los ATM para proporcionar la operación distribuida del STRM definida en la Recomendación X.411.

En la Recomendación X.402 se identifican las otras Recomendaciones que especifican otros aspectos de los sistemas de tratamiento de mensajes.

En la sección 2 de esta Recomendación se especifican los protocolos de acceso STM (P3 y P7). En el § 6 figura una visión general de los protocolos de acceso STM. En el § 7 se define la sintaxis abstracta del protocolo de acceso STRM (P3). En el § 8 se define la sintaxis abstracta del protocolo de acceso AM (P7). En el § 9 se define la relación de correspondencia de los protocolos de acceso STM con los servicios utilizados. En el § 10 se especifican los requisitos de conformidad para sistemas que aplican los protocolos de acceso STM.

En la sección 3 de esta Recomendación se especifica el protocolo de transferencia STRM (P1). En el § 11 figura una visión general del protocolo de transferencia STRM (P1). En el § 12 se define la sintaxis abstracta del protocolo de transferencia STRM (P1). En el § 13 se define la relación de correspondencia del protocolo de transferencia STRM (P1) con los servicios utilizados. En el § 14 se especifican los requisitos de conformidad para sistemas que aplican el protocolo de transferencia STRM (P1).

El anexo A proporciona una definición de referencia de los identificadores de objetos de protocolo STM citados en los módulos NSA.1 en el texto de esta Recomendación.

En el anexo B se describen las reglas de protocolo para el interfuncionamiento con realizaciones de la Recomendación X.411 (1984) mediante el protocolo de transferencia STRM (P1).

El anexo C identifica las diferencias entre la Recomendación X.411 (1984) y esta Recomendación.

El anexo D identifica las diferencias técnicas entre las versiones del CCITT y de la ISO, de la Recomendación X.419 del CCITT y la Norma 10021-6 de la ISO.

2 Referencias

Las referencias se indican en la Recomendación X.402.

3 Definiciones

Las definiciones figuran en la Recomendación X.402.

4 Abreviaturas

Las abreviaturas figuran en la Recomendación X.402.

5 Convenios

Esta Recomendación utiliza los convenios descriptivos indicados a continuación.

5.1 *Términos*

En esta Recomendación las palabras de términos definidos y los nombres y valores de parámetros de servicio y campos de protocolo, a menos que sean nombres propios, comienzan con una letra minúscula y están unidos por un guión como sigue: término-definido. Los nombres propios (en el texto inglés) comienzan con una letra mayúscula y no están unidos por un guión: Nombre propio.

5.2 *Definiciones de sintaxis abstracta*

Esta Recomendación define la sintaxis abstracta de los protocolos del STM utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208 y la notación de operaciones a distancia definida en la Recomendación X.219.

SECCIÓN 2 – ESPECIFICACIONES DEL PROTOCOLO DE ACCESO AL SISTEMA DE TRATAMIENTO DE MENSAJES (STM)

6 Descripción general de los protocolos de acceso STM

6.1 *Modelo de protocolos de acceso STM*

El § 6 de la Recomendación X.411 describe un modelo abstracto del sistema de transferencia de mensajes (STRM) y el servicio abstracto STRM que proporciona a sus usuarios-STRM.

El § 6 de la Recomendación X.413 describe un modelo abstracto de un almacenamiento de mensajes (AM) y el servicio abstracto AM que proporciona a su usuario-AM.

Este punto describe cómo se proporcionan el servicio abstracto STRM y el servicio abstracto AM por casos de comunicación de ISA cuando un usuario de servicio abstracto y un proveedor de servicio abstracto son realizados como procesos de aplicación situados en diferentes sistemas abiertos.

En el entorno de ISA, la comunicación entre procesos de aplicación se representa en términos de comunicación entre un par de entidades de aplicación (EA) que utilizan el servicio de presentación. La funcionalidad de una entidad de aplicación se descompone en un conjunto de uno o más elementos de servicio de aplicación (ESA). La interacción entre las EA se describe en términos de su utilización de los servicios proporcionados por los ESA.

El acceso al servicio abstracto STRM se consigue mediante tres elementos del servicio de aplicación, cada uno de los cuales proporciona un tipo de puerto que forma parte de un par entre un usuario STRM y el STRM en el modelo abstracto. El elemento de servicio de depósito de mensaje (ESDM) proporciona los servicios del puerto de depósito; el elemento de servicio de entrega de mensajes (ESEM) proporciona los servicios del puerto de entrega y el elemento de servicio de administración de mensajes (ESAM) proporciona los servicios del puerto de administración. Los ESDM, ESEM y ESAM son ESA asimétricos; es decir, los usuarios-ESA del STRM actúan como el consumidor, y los ESA del STRM actúan como el suministrador, del servicio abstracto STRM.

De manera similar, el acceso al servicio abstracto AM se efectúa mediante tres elementos de servicio de aplicación: el elemento de servicio de depósito de mensajes (ESDM) que proporciona el puerto de depósito indirecto; el elemento de servicio de extracción de mensajes (ESEXM) que proporciona los servicios del puerto de extracción; y el elemento de servicio de administracion de mensajes (ESAM) que proporciona los servicios del puerto de administración. Los ESA usuarios-AM actúan como el consumidor, y los ESA de AM actúan como el suministrador del servicio abstracto AM.

Estos elementos-de-servicio-de-aplicación son apoyados a su vez por otros elementos de servicio de aplicación.

El elemento de servicio de operaciones a distancia (ESOD) proporciona el paradigma petición/respuesta de las operaciones abstractas que se producen en los puertos en el modelo abstracto. Los ESDM, ESEM, ESEXM y ESAM proporcionan la función de correspondencia de la notación de sintaxis abstracta de un servicio abstracto con los servicios proporcionados por el ESOD.

Facultativamente, puede utilizarse el elemento de servicio de transferencia fiable (ESTF) para transferir de forma fiable las unidades de datos de protocolo de aplicación (UDPA) que contienen los parámetros de las operaciones entre las EA.

El elemento de servicio de control de asociación (ESCA) propoporciona el establecimiento y la liberación de una asociación de aplicación entre un par de EA Las asociaciones entre un usuario-STRM y el STRM pueden ser establecidas por el usuario STRM o el STRM. Las asociaciones entre un usuario-AM y un AM pueden ser establecidas solamente por el usuario-AM. Solo el iniciador de una asociación establecida puede liberarla.

La combinación de uno o más de los ESDM, ESEM, ESEXM y ESAM, junto con sus ESA de apoyo, define el contexto-aplicación de una asociación de aplicación. Obsérvese que puede utilizarse una sola asociación de aplicación para proporcionar uno o más tipos de puertos que forman parte de un par entre dos objetos en el modelo abstracto.

En el cuadro 1/X.419 se identifican los contextos de aplicación definidos en esta Recomendación para el protocolo de acceso STRM y el protocolo de acceso AM.

Si se soporta el protocolo de acceso STRM (P3), el soporte para los contextos de aplicación **acceso-strm** y **acceso-forzado-strm** es obligatorio para un ATM. Si un ATM apoya el contexto de aplicación **acceso-fiable-strm**, apoyará también el **acceso-fiable-forzado-strm**, y viceversa. El apoyo para cada uno de los contextos de aplicación del protocolo de acceso STRM (P3) es facultativo para un usuario-STRM.

Si se soporta el protocolo de acceso AM (P7), el soporte para el contexto de aplicación **acceso-am** es obligatorio para un AM, y el apoyo para el contexto de aplicación **acceso-fiable-am** es facultativo. El apoyo para cada uno de los contextos de aplicación en el protocolo de acceso AM (P7) es facultativo para un usuario AM.

En la figura 1/X.419 se modela un contexto de aplicación entre un usuario STRM y el STRM. La función de consumidor de los ESA usuario-STRM y la función de suministrador de los ESA STRM se indica mediante un subíndice «c», o «s», respectivamente.

De manera similar, en la figura 2/X.419 se modela un contexto de aplicación entre un usuario AM y el AM.

CUADRO 1/X.419

Contextos de aplicación de protocolo de acceso STM

Contextos de aplicación	ESA de tratamiento de mensajes				ESA de apoyo		
	ESDM	ESEM	ESEXM	ESAM	ESOD	ESTF	ESCA
Protocolo de acceso STRM							
acceso-strm	C	C	–	C	X	–	X
acceso-forzado-strm	S	S	–	S	X	–	X
acceso-fiable-strm	C	C	–	C	X	X	X
acceso-fiable-forzado-strm	S	S	–	S	X	X	X
Protocolo de acceso AM							
acceso-am	C	–	C	C	X	–	X
acceso-fiable-am	C	–	C	C	X	X	X

X presente

– ausente

C presente con el consumidor como iniciador

S presente con el suministrador como iniciador

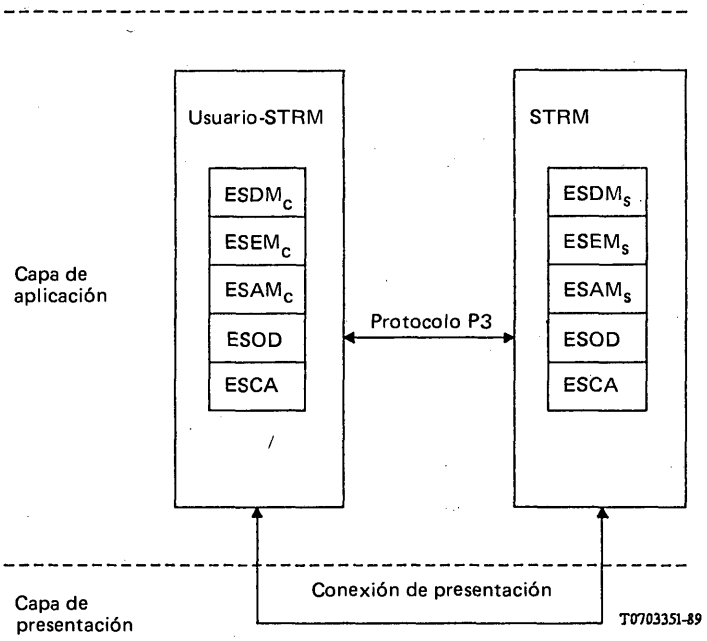


FIGURA 1/X.419

Modelo de protocolo de acceso STRM

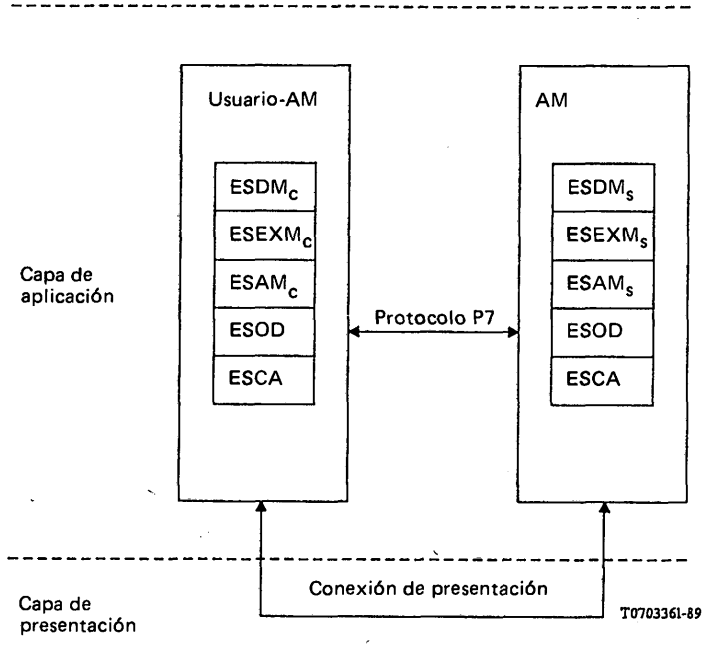


FIGURA 2/X.419

Modelo de protocolo de acceso AM

6.2 *Servicios proporcionados por el protocolo de acceso STRM*

El protocolo de acceso STRM (P3) comprende las siguientes operaciones que proporcionan los servicios definidos en la Recomendación X.411:

Vinculación-STRM y desvinculación-STRM

a) vinculación-STRM

b) desvinculación-STRM

Elemento de servicio de depósito de mensajes (ESDM)

c) depósito-mensaje

d) depósito-sonda

e) cancelación-entrega-diferida

f) control-depósito

Elemento de servicio de entrega de mensajes (ESEM)

g) entrega-mensaje

h) entrega-informe

i) control-entrega

Elemento de servicio de administración de mensajes (ESAM)

j) registro

k) cambio-credenciales.

6.3 *Servicios proporcionados por el protocolo de acceso AM*

El protocolo de acceso AM (P7) comprende las siguientes operaciones que proporcionan los servicios definidos en la Recomendación X.413:

Vinculación-AM y desvinculación-AM

a) vinculación-AM

b) desvinculación-AM

Elemento de servicio de depósito de mensajes (ESDM)

c) depósito-mensaje

d) depósito-sonda

e) cancelación-entrega-diferida

f) control-depósito

Elemento de servicio de extracción de mensajes (ESEXM)

g) resumen

h) listado

i) captura

j) supresión

k) registro-AM

l) alerta

Elemento de servicio de administración de mensajes (ESAM)

m) registro

n) cambio-credenciales.

6.4 *Utilización de servicios subyacentes*

Los protocolos de acceso STM utilizan servicios subyacentes como se describe a continuación.

6.4.1 *Utilización de servicios ESOD*

El elemento de servicio de operaciones a distancia (ESOD) se define en la Recomendación X.219.

El ESOD proporciona el paradigma petición/respuesta de operaciones a distancia.

Los ESDM, ESEM, ESEXM y ESAM son los únicos usuarios de los servicios OD-INVOCACION, OD-RESULTADO, OD-ERROR, OD-RECHAZO-U y OD-RECHAZO-P del ESOD.

Las operaciones a distancia del protocolo de acceso STRM (P3) y los protocolos de acceso AM (P7) son operaciones clase 2 (asíncronas).

6.4.2 *Utilización de los servicios ESTF*

El elemento de servicio de transferencia fiable (ESTF) se define en la Recomendación X.218.

El ESTF proporciona la transferencia fiable de unidades de datos de protocolo de aplicación (UDPA). El ESTF asegura que cada UDPA se transfiere completamente, exactamente una vez, o que se avisa al remitente de una excepción. El ESTF efectúa la recuperación tras el fallo de la comunicación y sistema final y minimiza el volumen de retransmisión necesaria para la recuperación.

Se definen contextos de aplicación alternativos con o sin servicios ESTF para apoyar los protocolos de acceso STM.

El ESTF se utiliza en el modo normal. La utilización del modo normal del ESTF implica la utilización del modo normal del ESCA y el modo normal del servicio de presentación.

Si el ESTF está incluido en un contexto de aplicación, vinculación-STRM y desvinculación-STRM (o vinculación-AM y desvinculación-AM) del protocolo de acceso STM son los únicos usuarios de los servicios TF-APERTURA y TF-CIERRE del ESTF. El ESOD es el único usuario de los servicios TF-TRANSFERENCIA, TF-SOLICITUD-TURNO, TF-CESIÓN-TURNO, TF-P-ABORTO y TF-U-ABORTO del ESTF.

6.4.3 *Utilización de los servicios ESCA*

El elemento de servicio de control de aplicación (ESCA) se define en la Recomendación X.217.

El ESCA proporciona el control (establecimiento, liberación, aborto) de asociaciones de apliación entre las EA.

Si el ESTF está incluido en un contexto de aplicación, vinculación-STRM y desvinculación-STRM (o vinculación-AM y desvinculación-AM) del protocolo de acceso STM son los únicos usuarios de los servicios A-ASOCIACIÓN y A-LIBERACIÓN del ESCA en modo normal. El ESOD es el usuario de los servicios A-ABORTO y A-P-ABORTO del ESCA.

Si el ESTF está incluido en el contexto de aplicación, el ESTF es el único usuario de los servicios A-ASOCIACIÓN, A-LIBERACIÓN, A-ABORTO y A-P-ABORTO del ESCA. La utilización del modo normal del ESTF implica la utilización del modo normal del ESCA y del modo normal del servicio de presentación.

6.4.4 *Utilización del servicio de presentación*

El servicio de presentación se define en la Recomendación X.216.

La capa de presentación coordina la representación (sintaxis) de las semánticas en la capa de aplicación que deberán intercambiarse.

En modo normal, se utiliza un contexto de presentación diferente para cada sintaxis abstracta incluida en el contexto de aplicación.

El ESCA es el único usuario de los servicios P-CONEXIÓN, P-LIBERACIÓN, P-U-ABORTO y P-P-ABORTO del servicio de presentación.

Si el ESTF no está incluido en el contexto de aplicación, el ESOD es el único usuario del servicio P-DATOS del servicio de presentación.

Si el ESTF está incluido en un contexto de aplicación, el ESTF es el único usuario de los servicios P-COMIENZO-ACTIVIDAD, P-DATOS, P-SINCRONIZACIÓN-MENOR, P-FIN-ACTIVIDAD, P-INTERRUPCIÓN- ACTIVIDAD, P-DESCARTE-ACTIVIDAD, P-U-INFORME-EXCEPCIÓN, P-REANUDACIÓN-ACTIVIDAD, P-P-INFORME-EXCEPCIÓN, P-SOLICITUD-TESTIGO y P-CESIÓN-CONTROL del servicio de presentación. La utilización del modo normal del ESTF implica la utilización del modo normal del ESCA y del modo normal del servicio de presentación.

6.4.5 *Utilización de servicios de capa inferior*

El servicio de sesión se define en la Recomendación X.215. La capa de sesión estructura el diálogo del flujo de información entre sistemas finales.

Si el ESTF está incluido en la asociación de aplicación, la capa de presentación utiliza las unidades funcionales núcleo, semidúplex, excepciones, sincronización menor y gestión de actividad del servicio de sesión.

Si el ESTF no está incluido en la asociación de aplicación, la capa de presentación utiliza las unidades funcionales núcleo y dúplex del servicio de sesión.

El servicio de transporte se define en la Recomendación X.214. La capa de transporte proporciona la transferencia transparente de extremo a extremo de datos por la conexión de red subyacente.

La elección de la clase de servicio de transporte utilizado por la capa de sesión depende de los requisitos de multiplexación y recuperación tras los errores. El apoyo para la clase de transporte 0 (sin multiplexación) es obligatorio. No se utiliza el servicio acelerado de transporte.

El apoyo para otras clases es facultativo. Puede utilizarse una clase de multiplexación para multiplexar un protocolo de acceso STM y otros protocolos de acceso (por ejemplo, el protocolo de acceso de guía (PAG) definido en la Recomendación X.519) por la misma conexión de red. Puede elegirse una clase de recuperación tras los errores si se omite el ESTF de un contexto de aplicación en una conexión de red con una tasa de error residual inaceptable.

Se supone una red subyacente que apoya el servicio de red de ISA definido en la Recomendación X.213.

Una dirección de red es la que se define en las Recomendaciones X.121, E.163/E.164 o X.200 (dirección PASR de ISA).

7 Definición de la sintaxis abstracta del protocolo de acceso al sistema de transferencia de mensajes (STRM)

La sintaxis abstracta del protocolo de acceso STRM (P3) se define en la figura 3/X.419.

La sintaxis abstracta del protocolo de acceso STRM (P3) se define utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208 y la notación de operaciones a distancia definida en la Recomendación X.219.

La definición de sintaxis abstracta del protocolo de acceso STRM (P3) tiene las siguientes partes principales:

- *Prólogo:* declaración de las exportaciones desde, e importaciones al módulo de protocolo de acceso STRM (P3) (figura 3/X.419, parte 1).
- *Contextos de aplicación:* definiciones de contextos de aplicación que pueden utilizarse entre un usuario-STRM y el STRM (figura 3/X.419, partes 2 y 3).
- *Elemento de servicio de depósito de mensaje:* definiciones del elemento de servicio de depósito de mensaje (ESDM) y sus operaciones a distancia y errores (figura 3/X.419, parte 4).
- *Elemento de servicio de entrega de mensaje:* definiciones del elemento de servicio de entrega de mensaje (ESEM) y sus operaciones a distancia y errores (figura 3/X.419, parte 5).
- *Elemento de servicio de administración de mensaje:* definiciones del elemento de servicio de administración de mensaje (ESAM) y sus operaciones a distancia y errores (figura 3/X.419, parte 6).

```
MTSAccessProtocol { joint-iso-ccitt mhs-motis(6) protocols(0) modules(0) mts-access-protocol(1) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


-- Prólogo

EXPORTS
        -- Elementos de servicio de aplicación
        mSSE, mDSE, mASE;

IMPORTS
        -- Elementos de servicio de aplicación y contextos de aplicación
        APPLICATION-SERVICE-ELEMENT, APPLICATION-CONTEXT, aCSE
                FROM Remote-Operations-Notation-extension { joint-iso-ccitt remote-operations(4)
                    notation-extension(2) }

        rTSE
                FROM Reliable-Transfer-APDUs { joint-iso-ccitt reliable-transfer(3) apdus(0) }

        -- Parámetros de servicio abstracto STRM
        MTSBind, MTSUnbind, MessageSubmission, ProbeSubmission, CancelDeferredDelivery,
        SubmissionControl, MessageDelivery, ReportDelivery, DeliveryControl, Register,
        ChangeCredentials, SubmissionControlViolated, ElementOfServiceNotSubscribed,
        DeferredDeliveryCancellationRejected, OriginatorInvalid, RecipientImproperlySpecified,
        MessageSubmissionIdentifierInvalid, InconsistentRequest, SecurityError,
        UnsupportedCriticalFunction, RemoteBindError, DeliveryControlViolated, ControlViolatesRegistration,
        RegisterRejected, NewCredentialsUnacceptable, OldCredentialsIncorrectlySpecified
                FROM MTSAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    mts-abstract-service(1)}

        -- Identificadores de objeto
        id-ac-mts-access, id-ac-mts-forced-access, id-ac-mts-reliable-access, id-ac-mts-forced-reliable-access,
        id-as-acse, id-as-msse, id-as-mdse, id-as-mrse, id-as-mase, id-as-mts, id-as-mts-rtse,
        id-ase-msse, id-ase-mdse, id-ase-mase
                FROM MHSProtocolObjectIdentifiers { joint-iso-ccitt mhs-motis(6) protocols(0)
                    modules(0) object-identifiers(0) };
```

FIGURA 3/X.419 (parte 1 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

```
-- Contextos de aplicación que omiten el ESTF

-- Iniciado por el usuario-STRM

mts-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND MTSBind
        UNBIND MTSUnbind
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { mSSE, mDSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mdse,         -- of MDSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-mts           -- of MTSBind and MTSUnBind -- }
        ::= id-ac-mts-access


-- Iniciado por el STRM

mts-forced-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND MTSBind
        UNBIND MTSUnbind
        REMOTE OPERATIONS { rOSE }
        RESPONDER CONSUMER OF { mSSE, mDSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mdse,         -- of MDSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-mts           -- of MTSBind and MTSUnbind -- }
        ::= id-ac-mts-forced-access
```

FIGURA 3/X.419 (parte 2 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

```
-- Contextos de aplicación que incluyen el ESTF en modo normal

-- Iniciado por el usuario-STRM

mts-reliable-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE, rTSE }
        BIND MTSBind
        UNBIND MTSUnbind
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { mSSE, mDSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mdse,         -- of MDSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-mts-rtse      -- of MTSBind and MTSUnbind, including RTSE -- }
        ::= id-ac-mts-reliable-access


-- Iniciado por el STRM

mts-forced-reliable-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE, rTSE }
        BIND MTSBind
        UNBIND MTSUnbind
        REMOTE OPERATIONS { rOSE }
        RESPONDER CONSUMER OF { mSSE, mDSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mdse,         -- of MDSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-mts-rtse      -- of MTSbind and MTSUnBind, including RTSE -- }
        ::= id-ac-mts-forced-reliable-access
```

FIGURA 3/X.419 (parte 3 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

```
-- Elemento de servicio de depósito de mensaje

mSSE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                message-submission,
                probe-submission,
                cancel-deferred-delivery }
        SUPPLIER INVOKES {
                submission-control }
        ::= id-ase-msse


-- Operaciones a distancia

message-submission MessageSubmission ::= 3

probe-submission ProbeSubmission ::= 4

cancel-deferred-delivery CancelDeferredDelivery ::= 7

submission-control SubmissionControl ::= 2


-- Errores a distancia

submission-control-violated SubmissionControlViolated ::= 1

element-of-service-not-subscribed ElementOfServiceNotSubscribed ::= 4

deferred-delivery-cancellation-rejected DeferredDeliveryCancellationRejected ::= 8

originator-invalid OriginatorInvalid ::= 2

recipient-improperly-specified RecipientImproperlySpecified ::= 3

message-submission-identifier-invalid MessageSubmissionIdentifierInvalid ::= 7

inconsistent-request InconsistentRequest ::= 11

security-error SecurityError ::= 12

unsupported-critical-function UnsupportedCriticalFunction ::= 13

remote-bind-error RemoteBindError ::= 15
```

FIGURA 3/X.419 (parte 4 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

```
-- Elemento de servicio de entrega de mensaje

mDSE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                delivery-control }
        SUPPLIER INVOKES {
                message-delivery,
                report-delivery }
        ::= id-ase-mdse


-- Operaciones a distancia

message-delivery MessageDelivery ::= 5

report-delivery ReportDelivery ::= 6

delivery-control DeliveryControl ::= 2


-- Errores a distancia

delivery-control-violated DeliveryControlViolated ::= 1

control-violates-registration ControlViolatesRegistration ::= 14


-- security-error ::= 12, defined in Part 4

-- unsupported-critical-function ::= 13, defined in Part 4
```

FIGURA 3/X.419 (parte 5 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

```
-- Elemento de servicio de administración de mensaje

mASE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                register,
                change-credentials }
        SUPPLIER INVOKES {
                change-credentials }
        ::= id-ase-mase


-- Operaciones a distancia

register Register ::= 1

change-credentials ChangeCredentials ::= 8


-- Errores a distancia

register-rejected RegisterRejected ::= 10

new-credentials-unacceptable NewCredentialsUnacceptable ::= 6

old-credentials-incorrectly-specified OldCredentialsIncorrectlySpecified ::= 5


END  -- de protocolo de acceso STRM
```

FIGURA 3/X.419 (parte 6 de 6)

Definición de sintaxis abstracta del protocolo de acceso STRM (P3)

8 Definición de la sintaxis abstracta del protocolo de acceso al almacenamiento de mensajes (AM)

La sintasis abstracta del protocolo de acceso AM (P7) se define en la figura 4/X.419.

La sintaxis abstracta del protocolo de acceso AM (P7) se define utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208, y la notación de operaciones a distancia definida en la Recomendación X.219.

La definición de sintaxis abstracta del protocolo de acceso AM (P7) tiene las siguientes partes principales:

- *Prólogo:* declaración de las exportaciones desde, e importaciones al módulo de protocolo de acceso AM (P7) (figura 4/X.419, parte 1).
- *Contextos de aplicación:* definiciones de contextos de aplicación que pueden utilizarse entre un usuario-AM y un AM (figura 4/X.419, parte 2).
- *Elemento de servicio de extracción de mensajes:* definiciones del elemento de servicio de extracción de mensajes (ESEXM) y sus operaciones a distancia y errores (figura 4/419, partes 3 y 4).

```
MSAccessProtocol { joint-iso-ccitt mhs-motis(6) protocols(0) modules(0) ms-access-protocol(2) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


-- Prólogo

EXPORTS
        mRSE;

IMPORTS
        -- Elementos de servicio de aplicación y contextos de aplicación
        APPLICATION-SERVICE-ELEMENT, APPLICATION-CONTEXT, aCSE
                FROM Remote-Operations-Notation-extension { joint-iso-ccitt remote-operations(4)
                    notation-extension(2) }

        rTSE
                FROM Reliable-Transfer-APDUs { joint-iso-ccitt reliable-transfer(3) apdus(0) }

        mSSE, mASE
                FROM MTSAccessProtocol { joint-iso-ccitt mhs-motis(6) protocols(0)
                    modules(0) mts-access-protocol(1) }

        -- Parámetros del servicio abstracto AM
        MSBind, MSUnbind, Summarize, List, Fetch, Delete, Register-MS, Alert, AttributeError,
        AutoActionRequestError, DeleteError, FetchRestrictionError, RangeError, SecurityError,
        ServiceError, SequenceNumberError
                FROM MSAbstractService { joint-iso-ccitt mhs-motis(6) ms(4) modules(0)
                    abstract-service(1) }

        -- Identificadores de objeto
        id-ac-ms-access, id-ac-ms-reliable-access, id-as-acse, id-as-msse, id-as-mrse, id-as-mase, id-as-ms, id-as-ms-rtse,
        id-ase-mrse
                FROM MHSProtocolObjectIdentifiers { joint-iso-ccitt mhs-motis(6) protocols(0)
                    modules(0) object-identifiers(0) };
```

FIGURA 4/X.419 (parte 1 de 4)

Definición de sintaxis abstracta del protocolo de acceso AM (P7)

```
-- Contexto de aplicación que omite el ESTF

ms-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE }
        BIND MSBind
        UNBIND MSUnbind
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { mSSE, mRSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mrse,         -- of MRSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-ms            -- of MSBind and MSUnbind -- }
        ::= id-ac-ms-access


-- Contexto de aplicación que incluye el ESTF

ms-reliable-access APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE, rTSE }
        BIND MSBind
        UNBIND MSUnbind
        REMOTE OPERATIONS { rOSE }
        INITIATOR CONSUMER OF { mSSE, mRSE, mASE }
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-msse,         -- of MSSE, including ROSE
                id-as-mrse,         -- of MRSE, including ROSE
                id-as-mase,         -- of MASE, including ROSE
                id-as-ms-rtse       -- of MSBind and MSUnbind, including RTSE -- }
        ::= id-ac-ms-reliable-access
```

FIGURA 4/X.419 (parte 2 de 4)

Definición de sintaxis abstracta del protocolo de acceso AM (P7)

```
-- Elemento de servicio de extracción de mensajes

mRSE APPLICATION-SERVICE-ELEMENT
        CONSUMER INVOKES {
                summarize,
                list,
                fetch,
                delete,
                register-MS, }
        SUPPLIER INVOKES {
                alert }
        ::= id-ase-mrse


-- Operaciones a distancia

summarize Summarize ::= 20

list List ::= 21

fetch Fetch ::= 22

delete Delete ::= 23

register-ms Register-MS ::= 24

alert Alert ::= 25


-- Errores a distancia

attribute-error AttributeError ::= 21

auto-action-request-error AutoActionRequestError ::= 22

delete-error DeleteError ::= 23

fetch-restriction-error FetchRestrictionError ::= 24

range-error RangeError ::= 25

security-error SecurityError ::= 26

service-error ServiceError ::= 27
```

FIGURA 4/X.419 (parte 3 de 4)

Definición de sintaxis abstracta del protocolo de acceso AM (P7)

```
sequence-number-error SequenceNumberError::= 28


END  -- de protocolo de acceso AM
```

FIGURA 4/X.419 (parte 4 de 4)

Definición de sintaxis abstracta del protocolo de acceso AM (P7)

9 Relación de correspondencia con los servicios utilizados

A continuación se define la relación de correspondencia de los protocolos de acceso STM con los servicios utilizados.

En el § 9.1 se define la correspondencia con los servicios utilizados para contextos de aplicación que omiten el ESTF. En el § 9.2 se define la relación de correspondencia con los servicios utilizados para contextos de aplicación que incluyen el ESTF.

9.1 *Contextos de aplicación que omiten el ESTF*

Este punto define la relación de correspondencia de los protocolos de acceso STM con los servicios utilizados para contextos de aplicación que omiten el ESTF. El apoyo para esta correspondencia es facultativo para la conformidad con esta Recomendación.

9.1.1 *Relación de correspondencia con ESCA*

Este punto define la relación de correspondencia de los servicios abstractos-vinculación (vinculación-STRM o vinculación-AM) y servicios abstractos-desvinculación (desvinculación-STRM o desvinculación-AM) con los servicios del ESCA en modo normal para contextos de aplicación que omiten el ESTF. El ESCA se define en la Recomendación X.217.

9.1.1.1 *Servicio abstracto-vinculación con A-ASOCIACIÓN*

El servicio abstracto-vinculación se corresponde con el servicio A-ASOCIACIÓN del ESCA. A continuación se califica la utilización de los parámetros del servicio A-ASOCIACIÓN.

9.1.1.1.1 *Modo*

Este parámetro será suministrado por el indicador de la asociación en la primitiva Petición A-ASOCIACIÓN, y tendrá el valor «modo normal».

9.1.1.1.2 *Nombre de contexto de aplicación*

El iniciador de la asociación propondrá uno de los contextos de aplicación definidos en esta Recomendación que omiten el ESTF en una primitiva Petición A-ASOCIACIÓN (véase el cuadro 1/X.419).

9.1.1.1.3 *Información de usuario*

La correspondencia de la operación-vinculación del servicio abstracto-vinculación con el parámetro información de usuario de la primitiva Petición A-ASOCIACIÓN se define en la Recomendación X.219.

9.1.1.1.4 *Lista de definición de contexto de presentación*

El iniciador de la asociación suministra la lista de definiciones de contexto de presentación en la primitiva Petición A-ASOCIACIÓN.

La lista de definiciones de contexto de presentación comprende una definición de contexto de presentación para cada sintaxis abstracta incluida en el contexto de aplicación. Una definición de contexto de presentación comprende un identificador de contexto de presentación y un nombre de sintaxis abstracta para el ESA. Cada sintaxis abstracta denominada para los ESDM, ESEM, ESEXM y ESAM comprende las UDPA de ESOD.

En los § 7 y 8 se definen las sintaxis abstractas incluidas en los contextos de aplicación.

9.1.1.1.5 *Calidad de servicio*

Este parámetro será suministrado por el iniciador de la asociación en la primitiva Petición A-ASOCIACIÓN y por el respondedor de la asociación en la primitiva Respuesta A-ASOCIACIÓN. Los parámetros «control ampliado» y «transferencia de diálogo optimizada» se pondrán a no requeridos. Los parámetros restantes serán tales que se utilicen valores por defecto.

9.1.1.1.6 *Requisitos de sesión*

Este parámetro será fijado por el iniciador de la asociación en la primitiva Petición A-ASOCIACIÓN y por el respondedor de la asociación en la primitiva Respuesta A-ASOCIACIÓN. El parámetro se fijará para especificar las siguientes unidades funcionales:

a) núcleo
b) dúplex.

9.1.1.2 *Servicio abstracto-desvinculación con A-LIBERACIÓN*

El servicio abstracto-desvinculación se corresponde con el servicio A-LIBERACIÓN del ESCA. A continuación se califica la utilización de los parámetros del servicio A-LIBERACIÓN.

9.1.1.2.1 *Resultado*

Este parámetro tendrá el valor «afirmativo».

9.1.1.3 *Utilización de los servicios A-ABORTO y A-P-ABORTO*

El ESOD es el usuario de los servicios A-ABORTO y A-P-ABORTO del ESCA.

9.1.2 *Relación de correspondencia con ESOD*

Los servicios ESDM, ESEM, ESEXM y ESAM se corresponden con los servicios OD-INVOCACIÓN, OD-RESULTADO, OD-ERROR, OD-RECHAZO-U y OD-RECHAZO-P del ESOD. La relación de correspondencia de la notación de sintaxis abstracta de los ESDM, ESEM, ESEXM y ESAM con los servicios ESOD se define en la Recomendación X.219.

9.2 *Contextos de aplicación que incluyen el ESTF*

Este punto define la relación de correspondencia de los protocolos de acceso STM con los servicios utilizados para contextos de aplicación que incluyen el ESTF de modo normal. El apoyo para esta correspondencia es facultativo para la conformidad con esta Recomendación. No se definen correspondencias con el ESTF en el modo X.410-1984. El ESTF se define en la Recomendación X.218.

9.2.1 *Relación de correspondencia con TF-APERTURA y TF-CIERRE*

Este punto define la correspondencia de los servicios abstractos-vinculación (vinculación-STRM o vinculación-AM) y los servicios abstractos-desvinculación (desvinculación-STRM o desvinculación-AM) con los servicios TF-APERTURA y TF-CIERRE del ESTF en modo normal.

9.2.1.1 *Servicio abstracto-vinculación con TF-ABRIR*

El servicio abstracto-vinculación corresponde con el servicio TF-APERTURA del ESTF. A continuación se califica la utilización de los parámetros del servicio TF-APERTURA.

9.2.1.1.1 *Modo*

Este parámetro será suministrado por el iniciador de la asociación en la primivita Petición TF-APERTURA y tendrá el valor «modo normal».

9.2.1.1.2 *Nombre de contexto de aplicación*

El iniciador de la asociación propondrá uno de los contextos de aplicación definidos en esta Recomendación que incluyen el ESTF en modo normal en la primitiva Petición TF-APERTURA (véase el cuadro 1/X.419).

9.2.1.1.3 *Datos de usuario*

La relación de correspondencia de la operación-vinculación del servicio abstracto-vinculación con el parámetro datos de usuario de la primitiva Petición TF-APERTURA se define en la Recomendación X.219.

9.2.1.1.4 *Lista de definiciones de contexto de presentación*

El iniciador de la asociación suministrará la lista de definiciones de contexto de presentación en la primitiva Petición TF-APERTURA.

La lista de definiciones de contexto de presentación comprende una definición de contexto de presentación para cada sintaxis abstracta incluida en el contexto de aplicación. Una definición de contexto de presentación comprende un identificador de contexto de presentación y un nombre de sintaxis abstracta para el ESA. Cada sintaxis abstracta denominada para los ESDM, ESEM, ESEXM y ESAM incluye las UDPA del ESOD. La sintaxis abstracta denominada para el ESTF incluye la sintaxis abstracta para la operación-vinculación del servicio abstracto-vinculación.

En los § 7 y 8 se definen las sintaxis abstractas incluidas en los contextos de aplicación.

9.2.1.2 *Servicio abstracto-desvinculación con TF-CIERRE*

El servicio abstracto-desvinculación se corresponde con el servicio TF-CIERRE del ESTF.

9.2.2 *Relación de correspondencia con ESOD*

Los servicios ESDM, ESEM y ESAM se corresponden con los servicios OD-INVOCACIÓN, OD-RESULTADO, OD-ERROR, OD-RECHAZO-U y OD-RECHAZO-P del ESOD. La correspondencia de la notación de sintaxis abstracta de los ESDM, ESEM, ESEXM y ESAM con los servicios ESOD se efectúa como se define en la Recomendación X.219.

ESOD es el usuario de los servicios TF-TRANSFERENCIA, TF-SOLICITUD-TURNO, TF-CESIÓN-TURNO, TF-P-ABORTO y TF-U-ABORTO del ESTF. La utilización de los servicios ESTF por el ESOD se define en la Recomendación X.229.

9.2.2.1 *Gestión del turno*

La Recomendación X.229 define la utilización por el ESOD de los servicios TF-SOLICITUD-TURNO y TF-CESIÓN-TURNO del ESTF para gestionar el turno.

En el cuadro 2/X.419 se definen los valores del parámetro prioridad del servicio TF-SOLICITUD-TURNO utilizado por el ESOD para pedir el turno.

La prioridad cero es la prioridad máxima y se reserva para la acción de liberación de la asociación por el iniciador.

La prioridad uno es la utilizada por el ESOD para la UDPA, ODRCH y la UDPA ODER para proporcionar los servicios OD-RECHAZO-U y OD-ERROR del ESOD.

La prioridad dos es utilizada por el ESOD para la UDPA OBRS para proporcionar los servicios OD-RESULTADO del ESOD.

Las prioridades tres a siete se utilizarán para la UDPA ODIV para proporcionar el servicio OD-INVOCACIÓN para las operaciones a distancia del protocolo de acceso STM. En el caso de una operación a distancia cuyos argumentos incluyen un mensaje, la UDPA ODIV tiene prioridad como una función de la prioridad del mensaje, **urgente**, **normal** o **no urgente**.

CUADRO 2/X.419

Prioridades de operaciones a distancia

Prioridad	ESDM	ESEM	ESEXM	ESAM
0	Liberar asociación			
1	OD-RECHAZO-U OD-ERROR			
2	OD-RESULTADO			
3	Control-de-depósito	Control-de-entrega		
4	Depósito-de-mensaje (urgente)	Entrega-de-mensaje (urgente)	Alerta	
5	Depósito-de-sonda	Entrega-de-informe	Registro-AM Resumen Listado Captura Supresión	Registro Cambio-credenciales
6	Depósito-de-mensaje (normal)	Entrega-de-mensaje (normal)		
7	Depósito-de-mensaje (no urgente)	Entrega-de-mensaje		

10 Conformidad

Un sistema (AU, AM o ATM) que pretenda la conformidad con los protocolos de acceso STM especificados en esta Recomendación cumplirá los requisitos indicados en los § 10.1, 10.2 y 10.3.

10.1 *Requisitos de declaración*

Se declarará lo siguientes:

a) el tipo de sistema para el cual se pretende la conformidad (AU, AM, ATM o ATM/AM);

b) los contextos de aplicación definidos en la sección 2 de esta Recomendación para los cuales se pretende la conformidad.

Puede pretenderse la conformidad para el protocolo de acceso STRM (P3), para el protocolo de acceso AM (P7), o para ambos. En el cuadro 3/X.419, se clasifica el apoyo para contextos de aplicación requeridos para la conformidad con el protocolo de acceso STRM (P3). En el cuadro 4/X.419, se clasifica el apoyo para contextos de aplicación requeridos para la conformidad con el protocolo de acceso AM (P7).

CUADRO 3/X.419

Requisitos de conformidad del protocolo de acceso STRM

Contexto de aplicación	ATM	Usuario-STRM
Protocolo de acceso STRM		
acceso-strm	Obligatorio	Facultativo
acceso-forzado-strm	Obligatorio	Facultativo
acceso-fiable-strm	Facultativo (véase la nota)	Facultativo
acceso-fiable-forzado-strm	Facultativo (véase la nota)	Facultativo

Nota – Si un ATM pretende la conformidad con el contexto de aplicación acceso-fiable-strm, pretenderá también la conformidad con el contexto de aplicación acceso-fiable-forzado-strm, y viceversa.

CUADRO 4/X.419

Requisitos de conformidad del protocolo de acceso AM

Contexto de aplicación	AM	Usuario-AM
Protocolo de acceso AM		
acceso-am	Obligatorio	Facultativo
acceso-fiable-am	Facultativo	Facultativo

10.2 *Requisitos estáticos*

El sistema:

a) será conforme con la(s) definición(es) de sintaxis abstracta de los protocolos de acceso STM definidos en los § 7 y 8 de esta Recomendación, requeridos por los contextos de aplicación para los cuales se pretende la conformidad.

10.3 *Requisitos dinámicos*

El sistema:

a) será conforme con la relación de correspondencia con servicios utilizados definida en el § 9 de esta Recomendación, requerida por los contextos de aplicación para los cuales se pretende la conformidad.

b) será conforme con la utilización de servicios subyacentes definida en el § 6.4 de esta Recomendación.

SECCIÓN 3 – ESPECIFICACIONES DEL PROTOCOLO DE TRANSFERERENCIA DEL SISTEMA DE TRANSFERENCIA DE MENSAJES (STRM)

11 Visión de conjunto del protocolo de transferencia del STRM

11.1 *Modelo*

El § 10 de la Recomendación X.411 perfecciona el modelo abstracto del sistema de transferencia de mensajes (STRM), presentado primero en el § 6 de dicha Recomendación, para mostrar que el objeto STRM comprende una colección de objetos de agente de transferencia de mensaje (ATM) que cooperan juntos para formar el STRM y ofrecer el servicio abstracto STRM a sus usuarios.

En el modelo abstracto perfeccionado se modelan interacciones entre los ATM como un conjunto de operaciones abstractas que se producen en el puerto de transferencia que forma parte de un par, entre los ATM.

En este punto se describe cómo los casos de comunicación de ISA proporcionan el servicio abstracto ATM, cuando los ATM son realizados como procesos de aplicación situados en diferentes sistemas abiertos.

En el entorno de ISA, la comunicación entre procesos de aplicación se representa en términos de comunicación entre un par de entidades de aplicación (EA) que utilizan el servicio de presentación. La funcionalidad de una EA se descompone en un conjunto de uno o más elementos de servicio de aplicación (ESA). La interacción entre las EA se describe en términos de su utilización de los servicios proporcionados por los ESA.

Los servicios de puerto de transferencia del modelo abstracto son apoyados por un elemento de servicio de aplicación, el elemento de servicio de transferencia de mensaje (ESTM), que a su vez es apoyado por otros dos elementos de servicio de aplicación, el elemento de servicio de transferencia fiable (ESTF) y el elemento de servicio de control de asociación (ESCA).

El elemento de servicio de transferencia fiable (ESTF) se utiliza para transferir fiablemente unidades de datos de protocolo de aplicación (CUDPA) que contienen el mensaje, sondas e informes entre las EA.

El elemento de servicio de control de asociación (ESCA) permite el establecimiento y la liberación de una asociación de aplicación entre un par de EA. Cualquiera de los dos ATM puede establecer las asociaciones entre los ATM. Sólo el iniciador de una asociación establecida puede liberarla.

La combinación del ESTM, el ESTF y el ESCA define el contexto de aplicación de una asociación de aplicación.

En la figura 4/X.419 se presenta un modelo del contexto de aplicación entre los ATM.

Se definen tres contextos de aplicación para el protocolo de transferencia STRM como se indica en el cuadro 5/X.419.

CUADRO 5/X.419

Contexto de aplicación de protocolo de transferencia del STRM

Contexto de aplicación	P1	Modo ESTF
protocolo-transferencia-strm-1984	P1 1984	X.410-1984
protocolo-transferencia-strm	P1 1988	X.410-1984
transferencia-strm	P1 1988	Normal

Se define el **protocolo-transferencia-strm-1984** para el interfuncionamiento con aplicaciones de la Recomendación X.411 de 1984. En este contexto de aplicación, la sintaxis abstracta del ESTM está restringida a la definida en la Recomendación X.411 de 1984. Estas restricciones se identifican subrayando las extensiones de 1988 a la sintaxis abstracta del ESTM en el módulo NSA.1 definido en la Recomendación X.411. Los cambios se indican también en el anexo C a esta Recomendación a efectos de referencia. El **protocolo-transferencia-strm-1984** es apoyado por el ESTF en el modo X.410-1984. El apoyo para el **protocolo-transferencia-strm-1984** es obligatorio para la conformidad con esta Recomendación.

Se define el **protocolo-transferencia-strm** para permitir el interfuncionamiento entre aplicaciones que apoyan la funcionalidad ampliada de 1988 mediante sistemas que han tenido una mejora mínima con respecto a la conformidad con la Recomendación X.411 de 1984. El **protocolo-transferencia-strm** proporciona la transparencia controlada del sistema mejorado a las extensiones de 1988. El **protocolo-transferencia-strm** es apoyado por el ESTF en el modo X.410-1984. El apoyo para el **protocolo-transferencia-strm** es obligatorio para la conformidad con esta Recomendación.

El contexto de aplicación **transferencia-strm** es apoyado por el ESTF en modo normal. Se prevé que, con el tiempo, la mayoría de los sistemas pasarán a apoyar el contexto de aplicación **transferencia-strm**. El apoyo para el contexto de aplicación **transferencia-strm** es facultativo para la conformidad con esta Recomendación. Obsérvese que en la Norma ISO 10021-6, el apoyo para el contexto de aplicación **transferencia-strm** es obligatorio. Es probable que en una futura versión de esta Recomendación el apoyo al contexto de aplicación **transferencia-strm** sea obligatorio, como parte de la estrategia de migración para permitir el apoyo para funcionalidad ampliada y maximizar el interfuncionamiento.

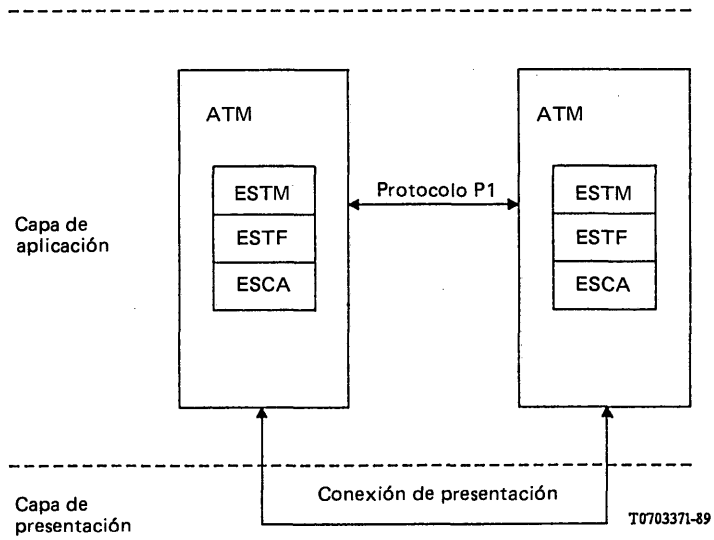


FIGURA 4/X.419

Modelo de protocolo de transferencia STRM

11.2 *Servicios proporcionados por el protocolo de transfererencia STRM*

El protocolo de transferencia STRM (P1) proporciona los siguientes servicios definidos en la Recomendación X.411:

Vinculación-ATM y desvinculación-ATM

a) vinculación-ATM

b) desvinculación-ATM

Elemento de servicio de transferencia de mensajes (ESTM)

c) transferencia de mensaje

d) transferencia de sonda

e) transferencia de informe.

11.3 *Utilización de servicios subyacentes*

El protocolo de transferencia STRM (P1) utiliza los servicios subyacentes como se describe a continuación.

11.3.1 *Utilización de los servicios ESTF*

El elemento de servicio de transferencia fiable (ESTF) se define en la Recomendación X.218.

El ESTF proporciona la transferencia fiable de unidades de datos de protocolo de aplicación (UDPA). El ESTF asegura que cada UDPA se transfiere completamente una sola vez, o que se avisa al remitente de una excepción. El ESTF efectúa la recuperación tras el fallo de comunicación y del sistema final y minimiza el volumen de retransmisión necesario para la recuperación.

Los servicios ESTF se utilizan para apoyar el protocolo de transferencia STRM (P1). El apoyo para el ESTF en el modo X.410-1984 es obligatorio. El apoyo al ESTF en modo normal es facultativo. Obsérvese que en la Norma ISO 10021-6, el apoyo al ESTF en modo normal es obligatorio, y el apoyo al ESTF en el modo X.410-1984 es facultativo.

La utilización del modo X.410-1984 del ESTF implica la utilización del modo X.410-1984 del ESCA y el modo X.410-1984 del servicio de presentación. La utilización del modo normal del ESTF implica la utilización del modo normal del ESCA y el modo normal del servicio de presentación.

El protocolo de transferencia STMR (P1) es el único usuario de los servicios TF-APERTURA,TF-CIERRE, TF-TRANSFERENCIA, TF-SOLICITUD-TURNO, TF-CESIÓN-TURNO, TF-P-ABORTO y TF-U-ABORTO del ESTF.

11.3.2 *Utilización de servicios ESCA*

El elemento de servicio de control de asociación (ESCA) se define en la Recomendación X.217.

El ESCA proporciona el control (establecimiento, liberación, aborto) de asociaciones de aplicación entre las EA.

El ESTF es el único usuario de los servicios A-ASOCIACIÓN, A-LIBERACIÓN, A-ABORTO y A-P-ABORTO del ESCA. La utilización del modo X.410-1984 del ESTF implica la utilización del modo X.410-1984 del ESCA y el modo X.410-1984 del servicio de presentación. La utilización del modo normal del ESTF implica la utilización del modo normal del ESCA y modo normal del servicio de presentación.

11.3.3 *Utilización del servicio de presentación*

El servicio de presentación se define en la Recomendación X.216.

La capa de presentación coordina la representación (sintaxis) de las semánticas de la capa de aplicación que han de intercambiarse.

En modo X.410-1984, se utiliza un solo contexto de presentación por defecto para la conexión de presentación subyacente. Este contexto de presentación incluye una sola sintaxis abstracta para todos los ESA incluidos en el contexto de aplicación (es decir, ESTM, ESTF y ESCA).

En modo normal, se utiliza un contexto de presentación diferente para cada sintaxis abstracta incluida en el contexto de aplicación.

No se utiliza el direccionamiento de capa de presentación para el protocolo de transferencia de mensaje (P1) en el modo X.410-1984.

El ESCA es el único usuario de los servicios P-CONEXIÓN, P-LIBERACIÓN, P-U-ABORTO y P-P-ABORTO del servicio de presentación.

El ESTF es el único usuario de los servicios P-COMIENZO-ACTIVIDAD, P-DATOS, P-SINCRONIZACIÓN-MENOR, P-FINALIZACIÓN-ACTIVIDAD, P-INTERRUPCIÓN-ACTIVIDAD, P-DESCARTE-ACTIVIDAD, P-U-INFORME-EXCEPCIÓN, P-REANUDACIÓN-ACTIVIDAD, P-P-INFORME-EXCEPCIÓN, P-SOLICITUD-TESTIGO y P-CESIÓN-CONTROL del servicio de presentación. La utilización del modo X.410-1984 del ESTF implica la utilización del modo X.410-1984 del ESCA y del modo X.410-1984 del servicio de presentación. La utilización del modo normal del ESTF implica la utilización del modo normal del ESA y del modo normal del servicio de presentación.

11.3.4 *Utilización de servicios de capa inferior*

El servicio de sesión se define en la Recomendación X.215. La capa de sesión estructura el diálogo del flujo de información entre los sistemas finales.

La utilización del ESTF requiere la utilización de las unidades funcionales núcleo, semidúplex, excepciones, sincronización menor y gestión de actividad por la capa de presentación.

El direccionamiento de la capa de sesión no se utilliza para el protocolo de transferencia STRM (P1) cuando se emplea el ESTF en el modo X.410-1984. Es decir, no se pasará una dirección de sesión en la UDPS conexión de la capa de sesión.

El servicio de transporte se define en la Recomendación X.214. La capa de transporte proporciona la transferencia transparente de extremo a extremo de datos por la conexión de red subyacente.

La elección de la clase de servicio de transporte utilizado por la capa de sesión depende de los requisitos de multiplexión y recuperación tras los errores. El apoyo para la clase 0 es obligatorio. No se utiliza el servicio acelerado de transporte.

El apoyo para otras clases es facultativo. La utilización de una clase de recuperación tras los errores junto con el ESTF duplica mecanismos para la recuperación tras los errores.

La dirección de transporte comprende una dirección de red y un identificador de punto de acceso de servicio de transporte (identificador PAST). El identificador PAST es transportado en el protocolo de capa de transporte. Cuando se utiliza el ESTF en el modo X.410-1984, este consta de hasta dieciséis dígitos del AI5.

Se supone una red subyacente que admite el servicio de red de ISA definido en la Recomendación X.213.

La dirección de red se define en las Recomendaciones X.121, E.163/E.164 o X.200 (dirección PASR de ISA).

11.4 *Establecimiento y liberación de asociaciones*

Las asociaciones entre dos EATM se crean mediante acuerdos bilaterales que abarcan:

a) el número máximo de asociaciones que pueden existir simultáneamente;

b) el uso o no de asociaciones de monólogo o bidireccionales alternadas;

c) el contexto de aplicación que se ha de utilizar;

d) el ATM que será responsable del establecimiento de las asociaciones;

e) el hecho de que las asociaciones estén permanentemente establecidas o sean establecidas y liberadas según sea necesario.

12 Definición de la sintaxis abstracta del protocolo de transferencia del STRM

La sintaxis abstracta del protocolo de transferencia STRM (P1) se define en la figura 5/X.419.

La sintaxis abstracta del protocolo de transferencia STRM (P1) se define utilizando la notación de sintaxis abstracta (NSA.1) definida en la Recomendación X.208 y la notación de operaciones a distancia definida en la Recomendación X.219.

La definición de la sintaxis abstracta del protocolo de transferencia STRM (P1) tiene las siguientes partes principales:

- *Prólogo:* Declaración de las exportaciones desde, e importaciones al módulo de protocolo de transferencia STRM (P1) (figura 5/X.419, parte 1).
- *Contextos de aplicación:* Definiciones de los contextos de aplicación utilizados entre los ATM (figura 5/X.419, parte 2).
- *Elemento de servicio de transferencia de mensaje:* Definiciones del elemento de servicio de transferencia de mensaje (ESTM) (figura 5/X.419, parte 3).
- *Unidades de datos de protocolo de aplicación STRM:* Definiciones de las unidades de datos de protocolo de aplicación STRM (UDPA): mensaje, sonda e informe (figura 5/X.419, parte 3).

```
MTSTranferProtocol { joint-iso-ccitt mhs-motis(6) protocols(0) modules(0) transfer-protocol(3) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


-- Prólogo

EXPORTS;

IMPORTS
        -- Elementos de servicio de aplicación y contextos de aplicación
        APPLICATION-SERVICE-ELEMENT, APPLICATION-CONTEXT, aCSE
                FROM Remote-Operations-Notation-extension { joint-iso-ccitt remote-operations(4)
                    notation-extension(2) }
        rTSE
                FROM Reliable-Transfer-APDUs { joint-iso-ccitt reliable-transfer(3) apdus(0) }

        -- Parámetros de servicio abstracto de puerto de transferencia de ATM
        MTABind, MTAUnbind, Message, Probe, Report
                FROM MTAAbstractService { joint-iso-ccitt mhs-motis(6) mts(3) modules(0)
                    mta-abstract-service(2) }

        -- Identificadores de objeto
        id-ac-mts-transfer, id-as-acse, id-as-mta-rtse, id-as-mtse, id-ase-mtse
                FROM MHSProtocolObjectIdentifiers { joint-iso-ccitt mhs-motis(6) protocols(0)
                    modules(0) object-identifiers(0) }
```

FIGURA 5/X.419 (parte 1 de 3)

Definición de la sintaxis abstracta del protocolo de transferencia STRM (P1)

```
-- Contexto de aplicación que incluye el ESTF en modo normal

mts-transfer APPLICATION-CONTEXT
        APPLICATION SERVICE ELEMENTS { aCSE, rTSE, mTSE }
        BIND MTABind
        UNBIND MTAUnbind
        ABSTRACT SYNTAXES {
                id-as-acse,         -- of ACSE
                id-as-mts-rtse      -- of MTABind and MTAUnbind, including RTSE
                id-as-mtse          -- of MTSE -- }
        ::= id-ac-mts-transfer


-- Contexto de aplicación que incluye el ESTF en modo X.410-1984

mts-transfer-protocol INTEGER ::= 12


-- Contexto de aplicación para interfuncionamiento con P1 1984

mts-transfer-protocol-1984 INTEGER ::= 1
```

FIGURA 5/X.419 (parte 2 de 3)

Definición de la sintaxis abstracta del protocolo de transferencia STRM (P1)

```
-- Elemento de servicio de transferencia de mensaje

mTSE APPLICATION-SERVICE-ELEMENT
        ::= id-ase-mtse


-- Unidades de datos de protocolo de aplicación del STRM

MTS-APDU ::= CHOICE{
        message [0] Message,
        probe [2] Probe,
        report [1] Report}


END  -- del protocolo de transferencia STRM
```

FIGURA 5/X.419 (parte 3 de 3)

Definición de la sintaxis abstracta del protocolo de transferencia STRM (P1)

13 Relación de correspondencia con los servicios utilizados

A continuación se define la relación de correspondencia del protocolo de transferencia STRM (P1) con los servicios utilizados.

En el § 13.1 se define la correspondencia del protocolo de transferencia STRM (P1) con servicios utilizados para contextos de aplicación que incluyen el ESTF en el modo X.410-1984. En el § 13.2 se define la correspondencia del protocolo de transferencia STRM (P1) con servicios utilizados para contextos de aplicación que incluyen el ESTF en modo normal.

13.1 *Relación de correspondencia con ESTF en modo X.410-1984*

En este punto se define la correspondencia del protocolo de transferencia STRM (P1) con servicios utilizados para contextos de aplicación que incluyen el ESTF en modo X.410-1984. El mantenimiento de esta correspondencia es obligatorio para la conformidad con esta Recomendación.

En el § 13.1.1 se define la relación de correspondencia de los servicios vinculación-ATM y desvinculación-ATM con los servicios TF-APERTURA y TF-CIERRE del ESTF en el modo X.410-1984. En el § 13.1.2 se define la relación de correspondencia de los servicios transferencia de mensaje, transferencia de sonda y transferencia de informe con el servicio TF-TRANSFERENCIA del ESTF. En el § 13.1.3 se describe la gestión del turno utilizando los servicios TF-SOLICITUD-TURNO y T-CESIÓN-TURNO del ESTF. En el § 13.1.4 se define la utilización del servicio TF-P-ABORTO del ESTF. En el § 13.1.5 se define la utilización del servicio TF-U-ABORTO del ESTF (no utilizado en el modo X.410-1984).

13.1.1 *Relación de correspondencia con TF-APERTURA y TF-CIERRE*

Este punto define la correspondencia de los servicios vinculación-ATM y desvinculación-ATM con los servicios TF-APERTURA y TF-CIERRE del ESTF en el modo X.410-1984.

13.1.1.1 *Vinculación-ATM con TF-APERTURA*

El servicio vinculación-ATM se corresponde con el servicio TF-APERTURA del ESTF. A continuación se califica la utilización de los parámetros del servicio TF-APERTURA.

13.1.1.1.1 *Protocolo de aplicación*

Este parámetro será suministrado por el iniciador de la asociación en la primitiva Petición TF-APERTURA y tendrá el valor **protocolo-transferencia-strm** (un valor entero de «12») o **protocolo-transferencia-strm-1984** (un valor entero de «1»).

13.1.1.1.2 *Datos de usuario*

El iniciador de la asociación hace corresponder el valor del tipo definido en la cláusula ARGUMENT del servicio vinculación-ATM con el parámetro datos de usuario de la primitiva Petición TF-APERTURA.

Si el respondedor de la asociación suministra el parámetro resultado de la primitiva Respuesta TF-APERTURA con el valor «aceptado», se hace corresponder el valor del tipo definido en la cláusula RESULT del servicio vinculación-ATM con el parámetro datos de usuario de la primitiva Respuesta TF-APERTURA.

En caso de error, el respondedor de la asociación suministra el parámetro resultado de la primitiva Respuesta TF-APERTURA con el valor «rechazado (permanente)» o «rechazado (transitorio)». En el caso de «rechazado (permanente)», el parámetro datos de usuario de la primitiva Respuesta TF-APERTURA será **error-autentificación**, o **modo-diálogo-inaceptable**.

13.1.1.1.3 *Modo*

Este parámetro será suministrado por el iniciador de la asociación en la primitiva Petición TF-APERTURA y tendrá el valor «modo X.410-1984)».

13.1.1.2 *Desvinculación-ATM con TF-CIERRE*

Desvinculación-ATM se corresponde con el servicio TF-CIERRE del ESTF. En el modo X.410-1984, el servicio TF-CIERRE no tiene parámetros.

13.1.2 *Relación de correspondencia con TF-TRANSFERENCIA*

Los servicios transferencia de mensaje, transferencia de sonda y transferencia de informe se corresponden con el servicio TF-TRANSFERENCIA del ESTF.

Un ESTM puede emitir una primitiva Petición TF-TRANSFERENCIA solamente si posee el turno (véase el § 13.1.3) y si no hay primitiva Confirmación de TF-TRANSFERENCIA pendiente.

A continuación se califica la utilización de los parámetros del servicio TF-TRANSFERENCIA.

13.1.2.1 *UDPA*

El emisor hará corresponder el valor de la UDPA-STRM con el parámetro UDPA de la primitiva Petición P-TRANSFERENCIA.

Para el servicio transferencia de mensaje, la UDPA STRM es un mensaje. Para el servicio transferencia de sonda, la UDPA STRM es una sonda. Para el servicio transferencia de informe, la UDPA STRM es un informe.

13.1.2.2 *Tiempo de transferencia*

El valor de este parámetro se especifica mediante una regla local del emisor. Puede relacionarse con la prioridad de la UDPA (véase el § 13.1.3.1.1).

13.1.3 *Gestión del turno*

Este punto describe la gestión del turno utilizando los servicios TF-SOLICITUD-TURNO y TF-CESIÓN-TURNO del ESTF.

El ESTM debe poseer el turno antes de que pueda utilizar el servicio TF-TRANSFERENCIA para transferir un mensaje, sonda o informe.

El ESTM sin el turno puede emitir una primitiva Petición TF-SOLICITUD-TURNO cuyo parámetro prioridad refleja la UDPA de máxima prioridad que espera transferencia.

El ESTM que posea el turno puede emitir una primitiva Petición TF-CESIÓN-TURNO cuando no tiene otras UDPA para transferir. Emitirá una primitiva Petición TF-CESIÓN-TURNO en respuesta a una primitiva Indicación TF-SOLICITUD-TURNO cuando no tiene otras UDPA para transferir de prioridad igual o mayor que la indicada en la primitiva Indicación TF-SOLICITUD-TURNO. Si tiene UDPA de prioridad inferior aún por transferir, puede emitir una primitiva Petición TF-CESIÓN-TURNO, cuyo parámetro prioridad refleja la UDPA de máxima prioridad que espera transferencia.

13.1.3.1 *Utilización del servicio TF-SOLICITUD-TURNO*

Un ESTM emite la primitiva Petición TF-SOLICITUD-TURNO para pedir el turno. Puede hacerlo así solamente si no posee ya el turno.

Si el iniciador de la asociación suministró un valor del parámetro modo diálogo de «monólogo» y un valor del parámetro turno inicial de «iniciador de asociación», no se utilizará el servicio TF-SOLICITUD-TURNO.

A continuación se califica la utilización del parámetro del servicio TF-SOLICITUD-TURNO.

13.1.3.1.1 *Prioridad*

El valor del parámetro prioridad es suministrado por el ESTM que pide el turno y refleja la UDPA de máxima prioridad que espera transferencia.

La prioridad cero es la prioridad máxima, y se reserva para la acción de liberación de la asociación por el iniciador.

La prioridad uno se asignará a mensajes cuyo campo de prioridad (definido en el § 8.2.1.1.1.8 de la Recomendación X.411) tiene el valor urgente. La prioridad uno se asignará también a sondas e informes.

La prioridad dos se asignará a mensajes cuyo campo de **prioridad** es **normal**.

La prioridad tres se asignará a mensajes cuyo campo de **prioridad** es **no urgente**.

Si se establece más de una asociación entre dos ATM, pueden asignarse las UDPA-STRM a asociaciones de acuerdo con sus prioridades. Pueden utilizarse varias asociaciones para transportar UDPA-STRM de la misma prioridad. En una asociación cualquiera, las UDPA-STRM de más alta prioridad se envían antes que las UDPA-STRM de más baja prioridad; las UDPA-STRM de la misma prioridad se envían «primera en entrar, primera en salir».

13.1.3.2 *Utilización del servicio TF-CESIÓN-TURNO*

Un ESTM emite la primitiva Petición TF-CESIÓN-TURNO para ceder el turno a su par. Puede hacerlo así solamente si posee el turno.

Si el iniciador de la asociación suministró un valor del parámetro modo diálogo de «monólogo» y un valor del parámetro turno inicial de «iniciador de asociación», no se utilizará el servicio TF-CESIÓN-TURNO.

El servicio TF-CESIÓN-TURNO no tiene parámetros.

13.1.4 *Utilización del servicio TF-P-ABORTO*

El proceso de aplicación es el usuario del servicio TF-P-ABORTO del ESTF.

El servicio TF-P-ABORTO proporciona una indicación al proceso de aplicación de que la asociación de aplicación no puede mantenerse (por ejemplo, porque no es posible la recuperación).

El servicio TF-P-ABORTO no tiene parámetros.

13.1.5 *Utilización del servicio TF-U-ABORTO*

El servicio TF-U-ABORTO del ESTF no está disponible en el modo X.410-1984.

13.2 *Relación de correspondencia con ESTF en modo normal*

En este punto se define la relación de correspondencia del protocolo de transferencia STRM (P1) con servicios utilizados para contextos de aplicación que incluyen el ESTF en modo normal. El mantenimiento de esta correspondencia es facultativo para la conformidad con esta Recomendación. Obsérvese que en la Norma ISO 10021-6, el mantenimiento del ESTF en modo normal es obligatorio.

En el § 13.2.1 se define la correspondencia de los servicios vinculación-ATM y desvinculación-ATM con los servicios TF-APERTURA y TF-CIERRE del ESTF en modo normal. En el § 13.2.2 se define la correspondencia de los servicios transferencia de mensajes, transferencia de sonda y transferencia de informe con el servicio TF-TRANSFERENCIA del ESTF. El §13.2.3 describe la gestión del turno utilizando los servicios TF-SOLICITUD-TURNO y TF-CESIÓN-TURNO del ESTF. En el § 13.2.4 se define la utilización del servicio TF-P-ABORTO del ESTF. En el § 13.2.5 se define la utilización del servicio TF-U-ABORTO del ESTF.

13.2.1 *Relación de correspondencia con TF-APERTURA y TF-CIERRE*

Este punto define la correspondencia de los servicios vinculación-ATM y desvinculación-ATM con los servicios TF-APERTURA y TF-CIERRE del ESTF en modo normal.

13.2.1.1 *Vinculación-ATM con TF-APERTURA*

El servicio vinculación-ATM se corresponde con el servicio TF-APERTURA del ESTF. A continuación se califica la utilización de los parámetros del servicio TF-APERTURA.

13.2.1.1.1 *Modo*

Este parámetro será suministrado por el iniciador de la asociación en la primitiva Petición TF-APERTURA y tendrá el valor «modo normal».

13.2.1.1.2 *Nombre de contexto de aplicación*

El iniciador de la asociación propondrá el contexto de aplicación **strm-transferencia**, definido en esta Recomendación, en la primitiva Petición TF-APERTURA.

13.2.1.1.3 *Datos de usuario*

La correspondencia de la operación-vinculación del servicio vinculación-ATM con el parámetro datos de usuario de la primitiva Petición TF-APERTURA se define en la Recomendación X.219.

13.2.1.1.4 *Lista de definiciones de contexto de presentación*

El iniciador de la asociación suministra la lista de definiciones de contexto de presentación en la primitiva Petición TF-APERTURA.

La lista de definiciones de contexto de presentación comprende una definición de contexto de presentación para cada sintaxis abstracta incluida en el contexto de aplicación. Una definición de contexto de presentación comprende un identificador de contexto de presentación y un nombre de sintaxis abstracta para el ESA. La sintaxis abstracta denominada para el ESTF incluye la sintaxis abstracta para la operación-vinculación.

En el § 12 se definen las sintaxis abstractas incluidas en el contexto de aplicación.

13.2.1.2 *Desvinculación-ATM con TF-CIERRE*

Desvinculación-ATM se corresponde con el servicio TF-CIERRE de ESTF.

No se utiliza ningún parámetro del servicio TF-CIERRE en modo normal.

13.2.2 *Relación de correspondencia con TF-TRANSFERENCIA*

Los servicios transferencia de mensaje, transferencia de sonda y transferencia de informe se corresponden con el servicio TRANSFERENCIA del ESTF.

La correspondencia de estos servicios con el servicio TF-TRANSFERENCIA en modo normal es idéntica a la correspondencia en modo X.410-1984, definida en el § 13.1.2.

13.2.3 *Gestión de turno*

El ESTM debe poseer el turno antes de que pueda utilizar el servicio TF-TRANSFERENCIA para transferir un mensaje, sonda o informe.

La gestión del turno en modo normal es idéntica a la gestión del turno en el modo X.410-1984, definida en el § 13.1.3.

13.2.4 *Utilización del servicio TF-P-ABORTO*

El proceso de aplicación es el usuario del servicio TF-P-ABORTO del ESTF.

El servicio TF-P-ABORTO proporciona una indicación al proceso de aplicación de que la asociación de aplicación no puede mantenerse (por ejemplo, porque no es posible la recuperación).

El servicio TF-P-ABORTO no tiene parámetros.

Obsérvese que la utilización del servicio TF-P-ABORTO en el modo normal es idéntica a la utilización del servicio TF-P-ABORTO en el modo X.410-1984.

13.2.5 *Utilización del servicio TF-U-ABORTO*

El proceso de aplicación es el usuario del servicio TF-U-ABORTO del ESTF.

El servicio TF-U-ABORTO permite que el proceso de aplicación aborte la asociación de aplicación. El servicio TF-U-ABORTO puede ser solicitado por el iniciador o por el respondedor de la asociación.

No se utiliza ningún parámetro de servicio TF-U-ABORTO en modo normal.

Obsérvese que el servicio TF-U-ABORTO no está disponible en el modo X.410-1984.

14 Conformidad

Un «DG» que pretende ser conforme con el protocolo de transferencia STRM (P1) especificado en esta Recomendación cumplirá los requisitos indicados en los § 14.1, 14.2 y 14.3.

14.1 *Requisitos en materia de declaración*

Se declara lo siguiente:

a) los contextos de aplicación definidos en la sección 3 de esta Recomendación para los cuales se pretenda la conformidad;
b) si se admite el modo monólogo, bidireccional alternado, o ambos modos, monólogo y diálogo bidireccional alternado;
c) si el DG puede actuar como iniciador o como respondedor, o como iniciador y como respondedor de una asociación.

En el cuadro 6/X.419, se clasifica el apoyo para contextos de aplicación requeridos para la conformidad con el protocolo de transferencia STRM (P1).

CUADRO 6/X.419

Requisitos de conformidad del protocolo de transferencia STRM

Contexto de aplicación	DG
Protocolo de transferencia STRM	
protocolo-tranferencia-strm-1984	Obligatorio
protocolo-transferencia-strm	Obligatorio
transferencia-strm	Facultativo

14.2 *Requisitos estáticos*

El DG:

a) será conforme con la definición de la sintaxis abstracta del protocolo de transferencia STRM (P1) definido en el § 12 de esta Recomendación.

14.3 *Requisitos dinámicos*

El DG:

a) será conforme con los procedimientos para operación distribuida del STRM definidos en la Recomendación X.411;
b) será conforme con la relación de correspondencia con los servicios utilizados definida en el § 13 de esta Recomendación, requerida por los contextos de aplicación para los cuales se pretende la conformidad; el mantenimiento de la relación de correspondencia con el ESTF en modo X.410-1984 es obligatorio, y el mantenimiento de la relación de correspondencia con el ESTF en modo normal es facultativo;
c) será conforme con las reglas para el interfuncionamiento con los DG conformes a la Recomendación X.411 definidos en el anexo B de esta Recomendación;
d) será conforme con la utilización de servicios subyacentes definida en el § 11.3 de esta Recomendación.

ANEXO A

(a la Recomendación X.419)

Definición de referencia de identificadores de objeto del protocolo del sistema de tratamiento de mensajes (STM)

En este anexo se define, con fines de referencia, diversos identificadores de objetos citados en los módulos NSA.1 en el texto de esta Recomendación. Los identificadores de objeto se asignan en la figura 6/X.419.

Todos los identificadores de objeto que esta Recomendación asigna, son asignados en el presente anexo. Sin embargo, dicho anexo no es definitivo para todas las asignaciones. En los módulos del texto de esta Recomendación figuran otras asignaciones definitivas, a las que se hace referencia en este anexo.

```
MHSProtocolObjectIdentifiers { joint-iso-ccitt mhs-motis(6) protocols(0) modules(0) object-identifiers(0) }

DEFINITIONS IMPLICIT TAGS ::=

BEGIN


-- Prólogo
-- Exporta todo

IMPORTS -- nothing -- ;


-- protocolos STM

id-mhs-protocols OBJECT IDENTIFIER ::= { joint-iso-ccitt mhs-motis(6) protocols(0) } -- not definitive


-- Categorías de identificadores de objeto

id-mod OBJECT IDENTIFIER ::= { id-mhs-protocols 0 }          -- modules

id-ac OBJECT IDENTIFIER ::= { id-mhs-protocols 1 }           -- application contexts

id-as OBJECT IDENTIFIER ::= { id-mhs-protocols 2 }           -- abstract syntaxes

id-ase OBJECT IDENTIFIER ::= { id-mhs-protocols 3 }          -- application service elements


-- Módulos

id-mod-object-identifiers OBJECT IDENTIFIER ::= { id-mod 0 }          -- not definitive

id-mod-mts-access-protocol OBJECT IDENTIFIER ::= { id-mod 1 }         -- not definitive

id-mod-ms-access-protocol OBJECT IDENTIFIER ::= { id-mod 2 }          -- not definitive

id-mod-mts-transfer-protocol OBJECT IDENTIFIER ::= { id-mod 3 }       -- not definitive
```

FIGURA 6/X.419 (parte 1 de 3)

Definición de la sintaxis abstracta de identificadores de objeto de protocolo STM

```
-- Contextos de aplicación
-- Protocolo de acceso STRM
id-ac-mts-access OBJECT IDENTIFIER ::= { id-ac 0 }
id-ac-mts-forced-access OBJECT IDENTIFIER ::= { id-ac 1 }
id-ac-mts-reliable-access OBJECT IDENTIFIER ::= { id-ac 2 }
id-ac-mts-forced-reliable-access OBJECT IDENTIFIER ::= { id-ac 3 }

-- Protocolo de acceso AM
id-ac-ms-access OBJECT IDENTIFIER ::= { id-ac 4 }
id-ac-ms-reliable-access OBJECT IDENTIFIER ::= { id-ac 5 }

-- Protocolo de transferencia STRM
id-ac-mts-transfer OBJECT IDENTIFIER ::= { id-ac 6 }

-- Sintaxis abstractas
id-as-acse OBJECT IDENTIFIER ::= { joint-iso-ccitt association-control (2) abstract-syntax (1) opdus (0) version1 (1) }
id-as-msse OBJECT IDENTIFIER ::= { id-as 1 }
id-as-mdse OBJECT IDENTIFIER ::= { id-as 2 }
id-as-mrse OBJECT IDENTIFIER ::= { id-as 5 }
id-as-mase OBJECT IDENTIFIER ::= { id-as 6 }
id-as-mtse OBJECT IDENTIFIER ::= { id-as 7 }
id-as-mts-rtse OBJECT IDENTIFIER ::= { id-as 8 }
id-as-ms OBJECT IDENTIFIER ::= { id-as 9 )
```

FIGURA 6/X.419 (parte 2 de 3)

Definición de la sintaxis abstracta de identificadores de objeto de protocolo STM

```
id-as-ms-rtse OBJECT IDENTIFIER ::= { id-as 10 }
id-as-mts OBJECT IDENTIFIER ::= { id-as 11 }

-- Elemento de servicio de aplicación
id-ase-msse OBJECT IDENTIFIER ::= { id-ase 0 }
id-ase-mdse OBJECT IDENTIFIER ::= { id-ase 1 }
id-ase-mrse OBJECT IDENTIFIER ::= { id-ase 2 }
id-ase-mase OBJECT IDENTIFIER ::= { id-ase 3 }
id-ase-mtse OBJECT IDENTIFIER ::= { id-ase 4 }

END   -- de identificadores de objeto de protocolo
```

FIGURA 6/X.419 (parte 3 de 3)

Definición de la sintaxis abstracta de identificadores de objeto de protocolo STM

ANEXO B

(a la Recomendación X.419)

Interfuncionamiento con los sistemas de 1984

En este anexo se definen las reglas que han de cumplir los DG que pretendan la conformidad con esta Recomendación (denominados en adelante «sistemas de 1988») cuando interfuncionan con realizaciones conformes a la Recomendación X.411 (1984) del CCITT (denominadas en adelante «sistemas 1984») que utilizan el protocolo de transferencia STRM (P1).

En el § B.1 se definen las reglas para establecer las asociaciones que deberá cumplir un sistema 1988 cuando interfunciona con un sistema 1984.

En el § B.2 se definen las reglas que deberá cumplir un sistema 1988 cuando transfiere una UDPA STRM a un sistema 1984.

En el § B.3 se definen las reglas que deberá cumplir un sistema 1988 cuando recibe una UDPA-STRM de un sistema 1984.

Nota – Como la Recomendación X.411 (1984) sólo define las interacciones en la frontera de un dominio de gestión administrativo (DGAD), la reglas de interfuncionamiento en este anexo sólo se aplican en dicha frontera.

Se han añadido otros tipos a la clase universal de tipos NSA.1 comparados con los definidos en la Recomendación X.409 (1984). Por tanto, se amplían las especificaciones de sustitución válidas para un tipo ANY. Obsérvese que los sistemas 1984 pueden ser incapaces de tratar los tipos universales ampliados. Es probable que un sistema 1984 pueda tratar correctamente estos campos incluso si contienen los tipos ampliados. Sin embargo, estos campos destinados a un sistema 1984 deben limitarse a los tipos universales definidos en la Recomendación X.409 (1984).

Las reglas básicas de codificación para NSA.1 ofrecen más flexibilidad que la Recomendación X.409 (1984) para la forma larga de los octetos de longitud. Las primeras permiten utilizar más octetos de longitud que el mínimo necesario, pero no así la segunda. Por lo tanto, en el interfuncionamiento con un sistema 1984, es necesario respetar esta limitación, y utilizar el menor número posible de octetos, sin octetos guía que tengan el valor 0.

B.1 *Establecimiento de la asociación*

Este punto define las limitaciones que observará un sistema 1988 con vinculación-ATM al establecer una asociación con un sistema 1984. No hay restricciones con desvinculación-ATM.

Se utilizará el **protocolo-transferencia-strm-1984**, definido en el § 12, para la compatibilidad con el sistema 1984.

B.1.1 *Credenciales de iniciador/credenciales de respondedor*

No se imponen limitaciones a estos elementos puesto que los elementos correspondientes de la Recomendación X.411 (1984) fueron definidos cada uno para ser un tipo ANY. Sin embargo, obsérvese que un sistema 1984 estará limitado en su utilización de estos elementos al interfuncionar con sistemas 1988 como se describe anteriormente.

B.1.2 *Contexto de seguridad*

Este elemento facultativo no será generado por un sistema 1988 al interfuncionar con un sistema 1984. Obsérvese que un sistema 1984 no es capaz de generar este elemento.

B.1.3 *Error-vinculación*

El valor de error-vinculación **contexto-seguridad-inaceptable** no será generado por un sistema 1988.

B.2 *Reglas para la transferencia a sistemas 1984*

En este punto se definen las reglas de interfuncionamiento que deberá cumplir un sistema 1988 al transferir una UDPA-STRM a un sistema 1984. La transformación de una UDPA-STRM conforme con la Recomendación X.411 en una conforme con la Recomendación X.411 (1984) se denomina *paso a un grado inferior.* Las reglas se expresan en términos de las acciones que han de realizar al sistema 1988 sobre cada elemento de protocolo del protocolo de transferencia STRM (P1).

Para una UDPA-STRM dada, si ninguna de las reglas indica que fallaría el paso a un grado inferior, se pasará la UDPA-STRM a un grado inferior de acuerdo con todas las reglas aplicables antes de ser transferida al sistema 1984.

Si una o más de las reglas consideran que el paso a un grado inferior ha fallado, la acción realizada por el ATM es igual que si la transferencia hubiera fallado (véase el § 14 de la Recomendación X.411).

Nota – La pérdida potencial o real de información causada por la aplicación de estas reglas puede afectar a la estrategia de encaminamiento futura de un ATM.

En el resto de este punto se especifican las reglas para cada uno de los elementos de protocolo. Los elementos de protocolo no mencionados específicamente se transferirán inalterados. A menos que se establezca otra cosa, las reglas especificadas se aplican en cualquier UDPA-STRM que aparece en los elementos de protocolo.

B.2.1 *Ampliaciones*

Si están presentes cualesquiera elementos de **ampliaciones** por mensaje y ningún **campo-de-ampliación** está marcado como **crítico-para-transferencia** o **crítico-para-entrega**, se suprimirán los elementos **ampliaciones**.

Si están presentes cualesquiera elementos de **ampliaciones** por mensaje y cualquier **campo-de-ampliación** está marcado **crítico-para-transferencia** o **crítico-para-entrega**, fracasará el paso a un grado inferior.

Estas reglas se aplicarán antes de cualesquiera de las reglas descritas en los subapartados siguientes.

B.2.2 *Información bilateral por dominio*

Si un elemento de **dominio-privado** está presente en un elemento de **información-bilateral-por-dominio**, se suprimirá el elemento de **información-bilateral-por-dominio**.

En los demás casos, la **información-bilateral-por-dominio** permanecerá inalterada.

B.2.3 *Información de rastreo/información de rastreo intermedia de asunto*

Si un elemento **otras-acciones** está presente en cualquiera de los **elementos-de-información-de-rastreo** o **elementos-de-información-de-rastreo-intermedia-de-asunto**, se suprimirá el elemento **otras-acciones**.

En los demás casos, no se alterará la **información-de-rastreo** o **información-de-rastreo-intermedia-de-asunto**.

B.2.4 *Nombre de originador/nombre de destino de informe*

Si el **nombre-de-originador** en un **sobre-de-transferencia-de-mensaje** o en un **sobre-de-transferencia-de-sonda**, o si el **nombre-de-destino-de-informe** en un **sobre-de-transferencia-de-informe** no pueden pasarse a un grado inferior de acuerdo con las reglas indicadas para **nombre-OD** (véase el § B.2.7), fracasará el paso a un grado inferior.

En los demás casos el elemento no se alterará.

B.2.5 *Campos por destinatario de mensaje o transferencia de sonda*

Si un **nombre-de-destinatario** en los **campos-por-destinatario** de un **sobre-transferencia-de-mensaje** o de un **sobre-de-transferencia-de-sonda**, no pueden pasarse a un grado inferior de acuerdo con las reglas para **nombre-OD** (véase el § B.2.7), o existe cualquier **campo-de-ampliación-por-destinatario** y está marcado **crítico-para-transferencia** o **crítico-para-entrega**:

a) si el elemento de **responsabilidad** correspondiente tiene el valor **responsable**, fracasará el paso a un grado inferior;

b) si el elemento **responsabilidad** correspondiente tiene el valor **no-responsable**, se suprimirá el elemento para dicho destinatario de los **campos-por-destinatario**.

Nota – Las reglas de paso a un grado inferior implican que la **revelación-de-destinatarios** no es ni crítica para transferencia ni crítica para entrega.

B.2.6 *Campos por-destinatario de transferencia-de-informe*

Si un **nombre-de-destinatario-real** o un **nombre-de-destinatario-deseado** en los **campos-por-destinatario** de un **contenido de transferencia de informe** no pueden pasarse a un grado inferior de acuerdo con las reglas indicadas para **nombre-OD** (véase el § B.2.7), se suprimirá el elemento correspondiente de **campos-por-destinatario**. Si todos los elementos de **campos-por-destinatario** se suprimen de esta manera, fracasará el paso a un grado inferior.

B.2.7 *Nombre-OD*

El **nombre-OD** se pasará a un grado inferior suprimiendo el **nombre-de-guía** si está presente, y pasando a un grado inferior la **dirección-OD** (véase el § B.2.8).

B.2.8 *Dirección-OD*

Si la **dirección-OD** contiene cualesquiera atributos codificados tanto como cadenas teletex como cadenas imprimibles, se suprimirán las cadenas teletex.

Si la **dirección-OD** es una **dirección-OD-numérica** o una **dirección-OD-de-terminal** que contiene un **nombre-de-dominio-privado**, la **dirección-OD** no puede pasarse a un grado inferior.

Si la **dirección-OD** es una **dirección-OD-telemática**:

a) que contiene un **nombre-de-país**, un **nombre-de-dominio-de-administración**, una **dirección-de-red**, facultativamente **atributos-definidos-por-el-dominio** y ningún otro, la **dirección-OD** no se alterará.

b) que contiene una **dirección-de-red**, facultativamente un **identificador-de-terminal**, y ningún otro, la **dirección-OD** no se modificará.

c) que contiene combinaciones de atributos distintos a los anteriores, se suprimirán todos los atributos excepto la **dirección-de-red** y el **identificador-del-terminal**, si está presente.

Si la **dirección-OD** contiene cualesquiera atributos codificados como cadenas teletex y las cadenas imprimibles correspondientes están asusentes, la **dirección-OD** no puede pasarse a un grado inferior.

Si después de aplicar todas las reglas anteriores la **dirección-OD** contiene aún cualesquiera **atributos-de-ampliación**, la **dirección-OD** no puede pasarse a un grado inferior.

B.2.9 *Tipos-de-información-codificada*

Los **tipos-de-información-codificada** básicos indicados por identificadores de objeto se corresponderán con el bit correspondiente en **tipos-de-información-codificada-básica**, se suprimirán los identificadores de objetos.

Se harán corresponder otros **tipos-de-información-codificada** indicados por identificadores de objetos con el bit **indefinido** en **tipos-de-información-codificada-básica**, y se suprimirán los identificadores de objetos.

No se alterará ningún **parámetro-no-básico**, excepto los de los tipos **g4-clase-1** y **modo-mixto**. Los **g4-clase-1** y **modo-mixto** pueden transformarse de acuerdo con reglas deducidas de las Recomendaciones T.73 (1984), T.400, T.501 y T.503; si esto no es posible, fracasará el paso a un grado inferior.

No obstante las reglas anteriores, se suprimirán **tipos-de-información-codificada** en un **contenido-de-transferencia-de-informe**.

B.2.10 *Tipo-de-contenido y contenido*

Si el **tipo-de-contenido** en un mensaje o sonda es indicado por un entero, no se alterará. El **contenido** en el mensaje tampoco se alterará.

Si el **tipo-de-contenido** en un mensaje es indicado por un identificador de objeto, se hará corresponder con el valor entero **externo** en vez de con el identificador de objeto. El identificador de objeto y el **contenido** se combinarán juntos en un valor de tipo EXTERNAL y este valor será el contenido del nuevo **contenido**. El identificador de objeto será la referencia directa de EXTERNAL y el contenido del **contenido** OCTET STRING será su codificación alineada en octetos. La codificación del **contenido** OCTET STRING será las de las reglas de codificación básica de la NSA.1.

Si el **tipo-de-contenido** en una sonda es indicado por un identificador de objeto, fracasará el paso al grado inferior.

El **tipo-de-contenido** en un informe se suprimirá. El **contenido-devuelto** no se modificará.

B.3 *Reglas para recibir de los sistemas 1984*

Este punto define las reglas de interfuncionamiento que deberá cumplir un sistema 1988 al recibir una UDPA-STRM de un sistema 1984.

Se han establecido limitaciones de tamaño para varios elementos de protocolo de transferencia STRM (P1). A condición de que el sistema 1984 observe estas restricciones, una UDPA-STRM correctamente codificada recibida de un sistema 1984 es conforme también con el protocolo de transferencia STRM 1988 (P1). Por tanto, el sistema 1988 no tiene que realizar acciones especiales.

B.4 *Irregularidades del servicio*

La utilización de listas de redireccionamiento y distribución en presencia de las fronteras de dominio 1988/1984 pueden conducir a algunas irregularidades, que se enumeran seguidamente:

- los destinatarios pueden no ser capaces de advertir que han recibido un mensaje debido a la ampliación o al redireccionamiento de LD;
- cuando un mensaje atraviesa un dominio 1984, se pierde el historial de la ampliación y el historial del redireccionamiento. Esto puede causar la detección prematura del bucle de encaminamiento y producir como resultado el fallo del redireccionamiento o de la ampliación. Obsérvese que sólo un LD con dirección-OD 1984 compatible puede encontrarse con este problema;
- los ATM 1984 devolverán notificaciones al originador del mensaje en lugar de redireccionarlas por el trayecto de ampliación de la LD;
- los sistemas 1984 pueden contemplar nuevos valores distinguidos para elementos de protocolo de enteros que les son desconocidos.

ANEXO C

(a la Recomendación X.419)

Diferencias entre los protocolos del sistema de tratamiento de mensajes de 1984 y de 1988

En este anexo se identifican las diferencias entre el protocolo de acceso STRM (P3) y el protocolo de transferencia STRM (P1) definido en esta Recomendación y los protocolos P3 y P1 definidos en la Recomendación X.411 (1984). No se mencionan aquí las diferencias de carácter puramente redaccional.

Las diferencias se identifican en términos de las adiciones u otras modificaciones efectuadas en los elementos de protocolo presentes en P3 y P1 definidos en la Recomendación X.411 (1984). Las diferencias se indican con más precisión en las definiciones de sintaxis abstracta en la Recomendación X.411, en la cual cada tipo de datos que ha sido modificado se destaca por medio de un subrayado.

En el § C.1 se identifican las diferencias en el protocolo de acceso STRM (P3). En el § C.2 se identifican las otras diferencias en el protocolo de transferencia STRM (P1).

C.1 *Diferencias del protocolo de acceso STRM (P3)*

Este punto identifica las diferencias entre el protocolo de acceso STRM (P3) definido en esta Recomendación y el protocolo P3 definido en la Recomendación X.411 (1984).

C.1.1 *Limitaciones de tamaño*

Se han establecido restricciones para limitar la longitud de los tipos de cadena, el número de elementos en un tipo SET OF o SEQUENCE OF, y la gama de valores de tipos INTEGER en todos los parámetros definidos en la Recomendación X.411 (1984) con excepción del **contenido** de mensaje.

C.1.2 *Modificaciones a tipos fundamentales*

Se han ampliado los parámetros **nombre-OD**, **tipo-de-contenido**, **tipos-de-información-codificada** y **contenido**, que aparecen en varios lugares en los argumentos y resultados de operaciones, como se describe a continuación.

C.1.2.1 *Nombre-OD*

Se han añadido dos nuevos parámetros facultativos al **nombre-OD**.

El primero de éstos es un conjunto de **atributos-de-ampliación** que proporciona los medios para utilizar el conjunto de caracteres teletex para los **atributos-definidos-de-dominio** y **normalizados**, especificar una **dirección-OD-postal** para entrega física y especificar una **dirección-de-terminal** a partir de una **dirección-de-red-ampliada**.

El segundo de éstos es un **nombre-de-guía**, definido en la Recomendación X.501.

Si solamente están presentes los **atributos-definidos-de-dominio, normalizados** o **atributos de ampliación**, entonces el **nombre-OD** constituye una **dirección-OD**. En los demás casos, un **nombre-de-guía** está también presente. Si un **nombre-de-guía** sólo está presente, puede ser necesario hacer corresponder el **nombre de guía** con una **dirección-OD** (por ejemplo, utilizando la guía).

C.1.2.2 *Tipo-de-contenido*

Se ha añadido la opción de identificar el **tipo-de-contenido** con un identificador de objeto en vez de con un entero. Este es el método preferido para identificar los nuevos **tipos-de-contenido** y se desaconseja la asignación de nuevos valores de enteros. Se han definido tres nuevos valores para la elección de enteros: **indefinido, externo** y **mensajeria-interpersonal-1988.**

C.1.2.3 *Tipos-de-información-codificada*

Se ha añadido la opción de especificar un conjunto de **tipos-de-información-codificada** externos. Todos los nuevos **tipos-de-información-codificada** se añadirán como un identificador de objeto.

Se ha modificado la definición de los **parámetros-no-básicos** para los tipos **g4-clase-1** y **modo-mixto**, ya que la definición referenciada en las Recomendaciones T.400, T.501 y T.503 difiere ahora de la previamente referenciada en la Recomendación T.73 (1984) y que ahora utiliza etiquetado explícito en lugar de implícito.

C.1.2.4 *Contenido*

El **contenido** de un mensaje es aún del tipo OCTET STRING. Si el **tipo-de-contenido** es identificado por el valor de entero **externo**, el **contenido** se denomina un **contenido-externo**. Los valores de OCTET STRING para un **contenido-externo** serán la codificación NSA.1 de un EXTERNAL.

C.1.3 *Ampliaciones*

La mayoría de las ampliaciones del servicio abstracto STRM definido en la Recomendación X.411 se ajustan al protocolo mediante la adición de un solo parámetro de **ampliaciones** en los sobres y resultados de operaciones. El parámetro está ausente cuando no se requieren ampliaciones. Puede estar presente en:

- **Sobre-de-depósito-de-mensaje**, mensaje por mensaje y destinatario por destinatario.
- **Resultado-de-depósito-de-mensaje.**
- **Sobre-de-depósito-de-sonda**, sonda por sonda y destinatario por destinatario.
- **Resultado-de-depósito-de-sonda.**
- **Sobre-de-entrega-de-mensaje.**
- **Sobre-de-entrega-de-informe**, informe por informe y destinatario por destinatario.

C.1.4 *Vinculación*

En la Recomendación X.411 (1984), las credenciales de tipo ANY se intercambian utilizando el argumento y resultado de vinculación. El tipo de ANY está limitado en esta Recomendación a una elección de **credenciales-simples** (una cadena del AI5 o una OCTET STRING), o **credenciales-fuertes** basadas en técnicas criptográficas.

Se ha añadido al argumento un parámetro facultativo para especificar un **contexto-de-seguridad**. Se ha añadido un nuevo error para indicar un **contexto-de-seguridad-inaceptable**.

C.1.5 *Depósito-de-mensaje*

Se han hecho facultativos los parámetros **tipo-de-información-codificada-original** y **conversión-explícita** en el **sobre-de-depósito-de-mensaje.**

Se han añadido dos nuevos errores: **petición-incoherente** y **error-de-seguridad.**

C.1.6 *Depósito-de-sonda*

Igual que para depósito de mensaje, véase el § C.1.5.

C.1.7 *Cancelación-entrega-diferida*

Esta operación no se cambia virtualmente con excepción de las limitaciones de tamaño descritas en el § C.1.1 y la supresión de error de mensaje transferido (subsumido por cancelación de entrega diferida rechazada).

C.1.8 *Control-de-depósito*

Se ha añadido al argumento un parámetro facultativo **contexto-de-seguridad-permisible.**

Se ha añadido al resultado un parámetro facultativo **tipos-de-contenido-de-espera** para especificar los **tipos-de-contenido** de cualesquiera mensajes en espera retenidos debido a controles prevalecientes. Se ha añadido el indicador **otras-etiquetas-de-seguridad** al parámetro **mensajes-en-espera** del resultado.

Se ha añadido un error: **error-de-seguridad.**

C.1.9 *Entrega-de-mensaje*

Se han hecho facultativos los parámetros **tipos-de-información-codificada-original** y **banderas de entrega** en el **sobre-de-entrega-de-mensajes,** y se ha añadido a éste un parámetro facultativo **identificador de contenido.**

La operación se ha hecho confirmada añadiendo una cláusula RESULT, que contiene dos parámetros de seguridad facultativos: **certificado-de-destinatario** y **prueba-de-entrega.**

Se ha añadido un nuevo error: **errror-de-seguridad.**

C.1.10 *Entrega-de-informe*

Se han añadido dos nuevos parámetros facultativos al **sobre-de-entrega-de-informe**: **tipo-de-contenido** y **tipos-de-información-codificada-original** del mensaje original.

Se han definido cinco nuevos **códigos-de-motivo-de-no-entrega** y 35 nuevos **códigos-de-diagnóstico-de-no-entrega.**

Se han añadido cinco nuevos valores del parámetro **tipo-de-usuario-STRM**: **almacenamiento-de-mensaje, lista de distribución, unidad-de-acceso-de-entrega-física, destinatario-físico** y **otros.**

La operación se ha hecho confirmada añadiendo una cláusula RESULT (que no transporta parámetros).

Se ha añadido un nuevo error: **errror-de-seguridad.**

C.1.11 *Control-de-entrega*

Se han añadido dos nuevos parámetros de control facultativos al argumento: **tipos-de-contenido-permisible** y **con texto-de-seguridad-permisible.**

Se ha añadido al resultado un parámetro facultativo **tipos-de-contenido-en-espera.**

Se han añadido dos nuevos errores: **control-que-viola-registro** y **error-de-seguridad.**

C.1.12 *Registro*

Se han añadido dos nuevos parámetros facultativos al argumento: **tipos-de-contenido-entregable** y **etiquetas-y-redirecciones.**

Se han alterado los rótulos sobre los parámetros **operaciones-restringidas, permisibles** y **longitud-de-contenido-máximo-permisible** de los **controles-de-entrega-por-defecto.** Se ha añadido el parámetro **tipos-de-contenido-permisibles.**

C.1.13 *Cambio-de-credenciales*

Se han limitado estos tipos posibles suministrados para las credenciales en esta operación, como se describe en el § C.1.4. Se ha limitado también la relación entre los tipos suministrados para **credenciales-antiguas** y **credenciales-nuevas** (para que sean del mismo tipo).

C.2 *Diferencias del protocolo de transferencia STRM (P1)*

Este punto identifica las diferencias entre el protocolo de transferencia STRM (P1) definido en esta Recomendación y el protocolo P1 definido en la Recomendación X.411 (1984).

Las siguientes modificaciones del protocolo de transferencia STRM (P1) son las mismas que las definidas para el protocolo de acceso STRM (P3): limitaciones de tamaño (véase el § C.1.1), cambios a tipos fundamentales (véase el § C.1.2) y vinculación (véase el § C.1.4).

A continuación se detallan otras modificaciones del protocolo de transferencia STRM (P1).

C.2.1 *Campos-externos*

Se utiliza el nuevo parámetro **ampliaciones** para incluir la mayoría de las ampliaciones del servicio abstracto al protocolo de transferencia STRM (P1) (véase el § C.1.3). El parámetro está ausente cuando no se requieren ampliaciones. Puede estar presente en:

- **Sobre-de-transferencia-de-mensaje**, mensaje por mensaje y destinatario por destinatario.
- **Sobre-de-transferencia-de-sonda** , sonda por sonda y destinatario por destinatario.
- **Sobre-de-transferencia-de-informe.**
- **Contenido-de-transferencia-de-informe**, informe por informe y destinatario por destinatario.

C.2.2 *Otras diferencias*

Se han añadido dos parámetros facultativos a los campos de transferencia informe por informe del **sobre-transferencia-de-informe**: **tipos-de-información-codificada-original** y **tipo-de-contenido.**

Se ha añadido un **identificador-de-dominio-privado** facultativo al parámetro **información-bilateral-por-dominio** de los **sobres-de-transferencia-de-mensaje** y **de-sonda.** Esto permite que la **información-bilateral-por-dominio** sea enviada a los DGPR así como a los DGAD.

Se ha añadido un parámetro facultativo **otras-acciones** a los elementos de **información-de-rastreo.** Los nuevos parámetros transportan dos banderas: **redireccionado** para indicar que el mensaje fue redireccionado por un DG y **ampliado** para indicar que el DG amplió una lista de distribución.

ANEXO D

(a la Recomendación X.419)

Diferencias entre las versiones del CCITT y de la ISO

En este anexo se identifican las diferencias técnicas entre las versiones del CCITT y de la ISO del texto de la Recomendación X.419 y de la Norma ISO 10021-6 según se relacionan con el mantenimiento del protocolo de transferencia STRM (P1)

Estas diferencias son:

1) En la Recomendación X.419 del CCITT es un requisito de conformidad obligatorio tener la capacidad de interfuncionar con realizaciones de la Recomendación X.411 (1984) del CCITT que utilizan el protocolo de transferencia STRM (P1) (para DGAD-DGAD y DGAD-DGPR). En la Norma ISO 10021-6, la capacidad para interfuncionar con sistemas 1984 es facultativa (para DGPR-DGPR y dentro del dominio).
2) En la Recomendación X.419 del CCITT el mantenimiento de la relación de correspondencia del protocolo de transferencia STRM (P1) con el ESTF en el modo X.410-1984, es un requisito de conformidad obligatorio; el mantenimiento de la relación de correspondencia con el ESTF en modo normal es facultativo. En la Norma 10021-6 de la ISO el mantenimiento de la relación de correspondencia con el ESTF en el modo normal es obligatorio, y el mantenimiento de la relación de correspondencia con el ESTF en el modo X.410-1984 es facultativo.

   Nota – Una realización que sea conforme solamente con la relación de correspondencia obligatoria de la Norma ISO 10021-6 no será capaz de interfuncionar con realizaciones de la Recomendación X.411 (1984) del CCITT, ni con realizaciones que sean conformes solamente con la relación de correspondencia obligatoria de la Recomendación X.419 (1988) del CCITT, y viceversa.
3) En la Recomendación X.419 del CCITT, hay requisitos para el mantenimiento de servicios de capa inferior (véase el § 11.3.4). En la Norma 10021-6 de la ISO estos requisitos se omiten.

Recomendación X.420

SISTEMAS DE TRATAMIENTO DE MENSAJES: SISTEMA DE MENSAJERÍA INTERPERSONAL[1)]

(Málaga-Torremolinos, 1984; modificada en Melbourne, 1988)

El establecimiento en diversos países de servicios telemáticos y servicios de mensajes con almacenamiento y retransmisión controlados por computador, y asociados a redes públicas de datos, crea la necesidad de establecer normas que faciliten el intercambio internacional de mensajes entre los abonados a estos servicios.

El CCITT,

considerando

(a) la necesidad de sistemas de tratamiento de mensajes;

(b) la necesidad de transferir y almacenar mensajes de diferentes tipos;

(c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;

(d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones especificadas por el CCITT;

(e) que las Recomendaciones de la serie X.500 definen los sistemas de guía;

(f) que los sistemas de tratamiento de mensajes se definen en la serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419;

(g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

(1) que el intercambio de objetos de información abstractos que los usuarios intercambian en mensajería interpersonal se defina como se indica en la sección 2;

(2) que el servicio abstracto ofrecido a usuarios en mensajería interpersonal se defina como se indica en la sección 3;

(3) que la manera de proporcionar el servicio abstracto sea la especificada en la sección 4.

ÍNDICE

SECCIÓN 1 – *Introducción*

0 *Introducción*

1 *Campo de aplicación*

2 *Referencias*

3 *Definiciones*

4 *Abreviaturas*

5 *Convenios*

5.1 NSA.1

5.2 Grado

5.3 Términos

[1)] La Recomendación X.420 y la norma 10021-7 ISO [Information Processing Systems – Text Communication – MOTIS – Interpersonal Messaging System] se elaboraron en estrecha colaboración y están técnicamente alineadas, salvo en lo relativo a las diferencias indicadas en el anexo M.

SECCIÓN 2 – *Objetos de información abstracta*

6 *Visión de conjunto*

7 *Mensajes interpersonales*

7.1 Tipos de componentes del campo de encabezamiento
7.2 Campos de encabezamiento
7.3 Tipos de parte de cuerpo

8 *Notificaciones interpersonales*

8.1 Campos comunes
8.2 Campos de no recepción
8.3 Campos de recepción

SECCIÓN 3 – Definición de servicio abstracto

9 *Visión de conjunto*

10 *Tipos de objetos primarios*

10.1 Usuario de sistema de mensajería interpersonal
10.2 Sistema de mensajería interpersonal

11 *Tipos de puertos primarios*

11.1 Generación
11.2 Recepción
11.3 Gestión

12 *Operaciones abstractas*

12.1 Operaciones abstractas de generación
12.2 Operaciones abstractas de recepción
12.3 Operaciones abstractas de gestión

13 *Errores abstractos*

13.1 Error de abono
13.2 Destinatario especificado indebidamente

14 *Otras capacidades*

SECCIÓN 4 – *Provisión del servicio abstracto*

15 *Visión de conjunto*

16 *Tipos de objetos secundarios*

16.1 Agente de usuario del sistema de mensajería interpersonal
16.2 Dispositivo de almacenamiento de mensajes del sistema de mensajería interpersonal
16.3 Agente telemático
16.4 Unidad de acceso télex
16.5 Unidad de acceso a entrega física
16.6 Sistema de transferencia de mensajes

17 *Tipos de puertos secundarios*

17.1 Depósito
17.2 Entrega
17.3 Extracción
17.4 Administración
17.5 Importación
17.6 Exportación

18 *Operación de agente de usuario*

18.1 Variables de estado
18.2 Ejecución de operaciones de generación
18.3 Ejecución de operaciones de gestión
18.4 Invocación de operaciones de recepción
18.5 Procedimientos internos

19 *Operaciones de almacenamiento de mensajes*

19.1 Creación de objetos de información
19.2 Mantenimiento de atributos
19.3 Notificación de no recepción
19.4 Retransmisión automática

20 *Contenido de mensajes*

20.1 Contenido
20.2 Tipo de contenido
20.3 Longitud de contenido
20.4 Tipos de información codificada

21 *Realización de puertos*

22 *Conformidad*

22.1 Relación generación-recepción
22.2 Requisitos de enunciados de conformidad
22.3 Requisitos estáticos
22.4 Requisitos dinámicos

Anexo A – Ampliaciones del encabezamiento
Anexo B – Tipos de parte de cuerpo ampliado
Anexo C – Atributos del almacenamiento de mensajes
Anexo D – Definición de referencia de identificadores de objeto
Anexo E – Definición de referencia de objetos de información abstractos
Anexo F – Definición de referencia de objetos funcionales
Anexo G – Definición de referencia de servicio abstracto
Anexo H – Definición de referencia de ampliaciones de encabezamiento
Anexo I – Definición de referencia de tipos de parte de cuerpo ampliado
Anexo J – Definición de referencia de atributos de almacenamiento de mensajes
Anexo K – Definición de referencia de límites superiores
Anexo L – Sustentación del servicio de mensajería interpersonal
Anexo M – Diferencias entre la Recomendación del CCITT y la Norma de la ISO
Anexo N – Resumen de las modificaciones de la Recomendación del CCITT de 1984

SECCIÓN 1 – INTRODUCCIÓN

0 Introducción

Esta Recomendación forma parte de un conjunto de Recomendaciones sobre tratamiento de mensajes. El conjunto completo proporciona un bosquejo general para un sistema de tratamiento de mensajes (STM) realizado por un número cualquiera de sistemas abiertos cooperantes.

El STM tiene por finalidad permitir a los usuarios intercambiar mensajes sobre una base de almacenamiento y retransmisión. Un mensaje depositado por cuenta de un usuario, el originador, es transportado por el sistema de transferencia de mensajes (STRM) y entregado posteriormente a agentes de uno o más usuarios adicionales, los destinatarios. Un usuario es asistido en la preparación, el almacenamiento y la representación de mensajes por un agente de usuario (AU). Facultativamente, es asistido en el almacenamiento de mensajes por un dispositivo de almacenamiento de mensajes (AM). El STRM comprende un número de agentes de transferencia de mensajes (ATM) que, colectivamente, realizan la función de transferencia de mensajes por almacenamiento y retransmisión.

Esta Recomendación define la aplicación tratamiento de mensajes denominada *mensajería interpersonal*, especificando en el proceso el tipo de contenido de mensajes y los procedimientos asociados conocidos por *P2*.

El texto de esta Recomendación está sujeto al acuerdo mutuo entre el CCITT y la ISO. La especificación ISO/CEI correspondiente es la ISO 10021-7.

1 Campo de aplicación

Esta Recomendación define la **mensajería interpersonal**, que es una forma de tratamiento de mensajes prevista para la correspondencia comercial o privada entre personas.

Esta Recomendación forma parte de una serie de Recomendaciones sobre tratamiento de mensajes. La Recomendación X.402 constituye la introducción a la serie mencionada e identifica otros documentos de la misma.

La base y fundamento arquitecturales del tratamiento de mensajes se define en otras Recomendaciones. La Recomendación identifica también estos otros documentos.

Esta Recomendación está organizada como sigue. La sección 1 es la introducción. La sección 2 define las clases de objetos de información intercambiados en la mensajería interpersonal. La sección 3 define el servicio abstracto asociado. La sección 4 especifica la forma de proporcionarlo. Los anexos contienen información suplementaria importante.

Los requisitos para la conformidad con esta Recomendación se indican en el § 22.

2 Referencias

En esta Recomendación se cita la Recomendación X.402, muchos de los documentos citados en ésta, y los indicados a continuación.

Norma ISO 639.2	Code for the representation of names of languages.
Recomendación T.4	Normalización de los aparatos facsímil del grupo 3 para la transmisión de documentos.
Recomendación T.30	Procedimientos de transmisión de documentos por facsímil por la red telefónica general conmutada.
Recomendación T.100	Intercambio de información internacional para el videotex interactivo.
Recomendación T.101	Interfuncionamiento internacional de servicios videotex.
Recomendación T.330	Acceso telemático al SMIP.
Recomendación X.420 (1984)	Sistemas de tratamiento de mensajes: capa de agente de usuario del servicio de mensajería interpersonal.
	Guía del realizador de la serie X.400, versión 6, 6 de noviembre de 1987.

3 Definiciones

Para los fines de esta Recomendación, son aplicables las definiciones de la Recomendación X.402.

4 Abreviaturas

Para los fines de esta Recomendación, son aplicables las abreviaturas de la Recomendación X.402.

5 Convenios

Esta Recomendación utiliza los convenios descriptivos identificados a continuación.

5.1 *NSA.1*

Esta Recomendación utiliza, para los fines indicados, los siguientes convenios descriptivos basados en la notación de sintaxis abstracta uno (NSA.1):

a) para definir los objetos de información de mensajería interpersonal, y otros tipos de datos y valores de todas clases, la propia NSA.1;

b) para definir los objetos funcionales de mensajería interpersonal, las macros OBJECT y REFINE de la Recomendación X.407;

c) para definir el servicio abstracto de mensajería interpersonal, las macros PORT y ABSTRACT-OPERATION y ABSTRACT-ERROR de la Recomendación X.407;

d) para definir las *ampliaciones de encabezamiento*, la macro HEADING-EXTENSION del § 7.2.17;

e) para definir *tipos de parte de cuerpo ampliada*, la macro EXTENDED-BODY-PART-TYPE del § 7.3.12;

f) para definir atributos AM, la macro ATTRIBUTE de la Recomendación X.500.

Los diversos usos de la notación NSA.1 se recapitulan en el cuadro 1/X.420. Con las dos excepciones que pueden verse fácilmente en el cuadro, la NSA.1, cuando se utiliza, aparece dos veces, una vez en el cuerpo de la Recomendación para facilitar la exposición y una segunda vez, en una forma bastante redundante, en un anexo, con fines de referencia.

CUADRO 1/X.420

Usos de la notación ASN.1

Asunto	Exposición	Referencia
Identificadores de objeto	–	anexo D
Objetos de información abstractos	Sección 2	anexo E
Objetos funcionales	§ 10, 11, 16	anexo F
Servicio abstracto	§ 12-13	anexo G
Ampliaciones del encabezamiento	anexo A	anexo H
Tipos de parte de cuerpo ampliada	anexo B	anexo I
Atributos de almacenamiento de mensajes	anexo C	anexo J
Límites superiores	–	anexo K

Si aparecen diferencias entre la NSA.1 utilizada en la exposición y la indicada en la referencia, se indica un error de especificación.

Obsérvese que los rótulos NSA.1 están implícitos en todo el módulo NSA.1 definido en el anexo; el módulo es definitivo a ese respecto.

Nota 1 – El uso de NSA.1 para describir una clase o una información no implica, por sí mismo, que esa información se transporta entre dos sistemas abiertos. El hecho de que la información, en virtud de su descripción en NSA.1 y de las reglas de codificación básicas de la NSA.1, tenga una sintaxis de transferencia concreta puede no tener ninguna importancia. La información transportada realmente entre sistemas se designa como tal por su inclusión en un protocolo de aplicación.

Nota 2 – El uso de las macros ABSTRACT-OPERATION y ASTRACT-ERROR, derivada de las macros correspondientemente denominadas de operaciones a distancia, no implica que las operaciones y los errores abstractos sean invocados y comunicados a través de la frontera entre sistemas abiertos. El hecho de que las operaciones y los errores abstractos, en virtud de su descripción mediante estas macros y con una especificación adicional mínima, podrían ser en efecto invocadas a través de SOD, no tiene ninguna importancia en el presente contexto.

5.2 *Grado*

Esta Recomendación utiliza el concepto de grado desarrollado en la Recomendación X.402.

5.3 *Términos*

En la presente Recomendación, los términos se escriben en **negrita** cuando son definidos, y en *cursiva* cuando se hace referencia a los mismos antes de su definición, sin resaltarlos en todas las demás ocasiones.

Los términos que son nombres propios se escriben (en el texto inglés) con mayúsculas, no así los términos genéricos.

SECCIÓN 2 – OBJETOS DE INFORMACIÓN ABSTRACTA

6 Visión de conjunto

Esta sección describe abstractamente los objetos de información que los usuarios intercambian en mensajería interpersonal. Son de dos clases: *mensajes interpersonales (MIP)* y *notificaciones interpersonales (NIP).* Una notificación interpersonal acusa la recepción, por un usuario, de un mensaje interpersonal.

```
InformationObject ::= CHOICE {
        ipm [0] IPM,
        ipn [1] IPN }
```

Esta sección trata los siguientes puntos:

a) Mensajes interpersonales.

b) Notificaciones interpersonales.

Nota 1 – La utilización, en toda esta sección, de palabras tales como «originador» y «destinatario» presupone el hecho de que los *MIP* y las *NIP* son transportados entre usuarios como el contenido de mensajes (véase el § 20). Estas palabras, por tanto, se refieren a los papeles que desempeñan los usuarios y las LD en esas transferencias.

Nota 2 – Un *MIP* puede aparecer (véase § 7.3.8) en el *cuerpo* de otro *MIP* que a su vez es transportado como el contenido de un mensaje. Las palabras «originador» y «destinatario» deberán entenderse en el contexto del transporte de un *MIP* como el contenido (completo) de un mensaje, y no un componente del *cuerpo* de otro *MIP* transportado.

Nota 3 – Un *MIP* o *NIP* hace diversas aserciones sobre su propia transferencia (por ejemplo, sobre quién origina el mensaje que lo contiene). Además, una *NIP* hace aserciones sobre la transferencia del *MIP* al que ella responde. No se verifica ninguna de estas aserciones.

7 Mensajes interpersonales

Un **mensaje interpersonal (MIP)** es un miembro de la clase primaria de objeto de información transportado entre usuarios en mensajería interpersonal.

```
IPM ::= SEQUENCE {
        heading     Heading,
        body        Body }
```

Tiene los siguientes componentes:

a) **Encabezamiento**: Conjunto de **campos de encabezamiento** (o **campos**), cada uno de los cuales es un elemento de información que da una característica del MIP (por ejemplo, su importancia).

b) **Cuerpo**: Secuencia de **partes de cuerpo**, cada una de las cuales es un objeto de información que el MIP deberá transportar entre usuarios (por ejemplo, un documento).

```
Body ::= SEQUENCE OF BodyPart
```

La estructura de un MIP se representa en la figura 1/X.420.

Este punto define y describe los tipos de componentes más importantes del campo de encabezamiento y define los campos de encabezamiento y los tipos de parte de cuerpo.

Nota – Un MIP puede asimilarse a una nota comercial. En efecto, los términos «Encabezamiento» y «Cuerpo» evocan esa analogía.

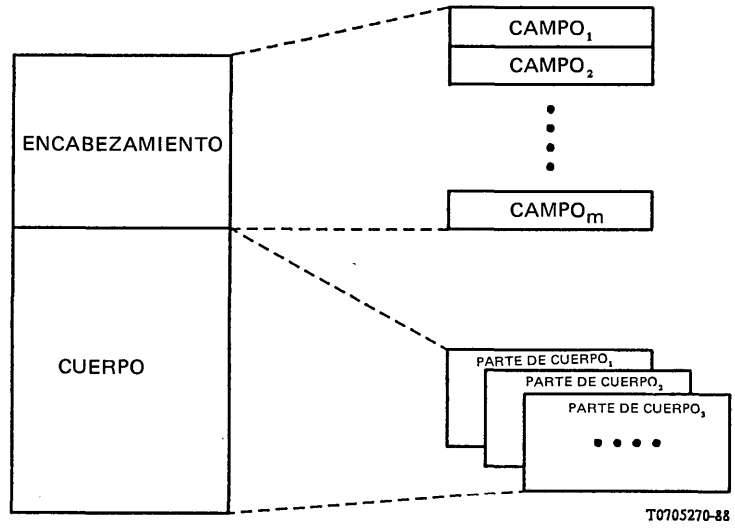


FIGURA 1/X.420

Mensaje interpersonal

7.1 *Tipos de componentes del campo de encabezamiento*

En el encabezamiento figuran elementos de información de varias clases. A continuación se definen y se describen estos tipos de componente de campo de encabezamiento-*identificador de MIP*, *especificador de destinatario*, y *descriptor O/D*.

7.1.1 *Identificador de MIP*

Un **identificador de MIP** es un elemento de información que identifica de manera única e inequívoca a un MIP, distinguiéndolo de todos los demás MIP que sean enviados por un usuario cualquiera.

```
IPMIdentifier ::= [APPLICATION 11] SET {
        user                        ORAddress OPTIONAL,
        user-relative-identifier    LocalIPMIdentifier }
```

Un identificador de MIP tiene los siguientes componentes:

a) **Usuario** (F): Identifica el usuario que origina el MIP. Una de las direcciones O/D de usuario. Se desaconseja la omisión de este componente.

b) **Identificador relativo al usuario** (O): Identifica de manera única e inequívoca el MIP, distinguiéndolo de todos los demás MIP que origina el usuario identificado por el componente usuario. Es una cadena imprimible de cero a un número prescrito de caracteres (véase el anexo K). Se desaconseja una longitud cero.

```
Local IPMIdentifier ::= PrintableString
    (SIZE (0. .ub-local-ipm-identifier))
```

Nota – El «11» en el identificador de MIP es el único rótulo de la NSA.1 empleado a nivel de la aplicación que es asignado por esta Recomendación.

7.1.2 *Especificador de destinatario*

Un **especificador de destinatario** es un elemento de información que describe un destinatario (preferido) de un MIP y que puede hacerle ciertas peticiones.

```
RecipientSpecifier ::= SET {
        recipient                [0]  ORDescriptor,
        notification-requests    [1]  NotificationRequests DEFAULT { },
        reply-requested          [2]  BOOLEAN DEFAULT FALSE }
```

Un especificador de destinatario tiene los siguientes componentes:

a) **Destinatario** (O): Identifica el destinatario preferido en cuestión. Un *descriptor O/D.*

Si el componente *peticiones de notificación* o *respuesta solicitada* hace una petición del destinatario preferido, estará presente el componente *nombre formal* del *descriptor O/D* antes mencionado.

b) **Peticiones de notificación** (D sin valores): Puede hacer ciertas peticiones del destinatario preferido, señalado por el componente destinatario.

```
NotificationRequests ::= BIT STRING {
    rn              (0),
    nrn             (1),
    ipm-return      (2) }
```

Este componente puede tomar simultáneamente cualesquiera de los valores que siguen, con la excepción de que el valor *rn* no debe seleccionarse a menos que se haya elegido el valor *nrn*:

i) *rn* (nr): Se solicita una *notificación de recepción* en circunstancias prescritas en el § 8.

ii) *nrn* (nnr): Se solicita una *notificación de no recepción* en las circunstancias prescritas en el § 8.

iii) *ipm-return* (devolución de MIP): Se solicita que se devuelva el MIP en cualquier *notificación de no recepción.*

c) **Respuesta solicitada** (D falso): Indica si se solicita o no una respuesta del destinatario preferido designado por el componente destinatario. Es un booleano.

Una **respuesta** es un MIP enviado en respuesta a otro. Un usuario puede responder a un MIP aunque no se haya pedido una respuesta y, en efecto, incluso si él no figura entre los destinatarios preferidos del MIP. Además, un usuario al que se le ha pedido una respuesta, puede dejar de responder.

7.1.3 *Descriptor O/D*

Un **descriptor O/D** es un elemento de información que identifica un usuario o LD.

```
ORDescriptor ::= SET {
    formal-name                 ORName OPTIONAL,
    Free-form-name          [0] FreeFormName OPTIONAL,
    telephone-number        [1] telephoneNumber OPTIONAL }
```

Un descriptor O/D tiene los siguientes componentes:

a) **Nombre formal** (C): Identifica al usuario o LD en cuestión. Es uno de sus nombres O/D.

Este componente condicional estará presente si se satisfacen uno o más de los criterios que se indican a continuación (pero puede también estar presente en el caso contrario):

i) El componente *nombre de forma libre* está ausente.

ii) El descriptor O/D aparece en el campo de encabezamiento *destinatarios de respuesta.*

iii) El descriptor O/D es el componente destinatario de un especificador de destinatario, y se satisfacen las condiciones indicadas en el apartado a) del § 7.1.2.

b) **Nombre de forma libre** (F): Identifica al usuario o LD en cuestión. Es una cadena teletex constituida por cero a un número prescrito de caracteres (véase el anexo K), tomados del subjuego gráfico del juego de caracteres de cadena teletex. Se desaconseja una longitud cero.

```
FreeFormName ::= TeletexString (SIZE (0. .ub-free-form-name))
```

c) **Número de teléfono** (F): Da el número de teléfono del usuario o LD en cuestión. Es una cadena imprimible de cero a un número prescrito de caracteres (véae el anexo K), tomados del subjuego gráfico del juego de caracteres de cadena imprimible. Se desaconseja una longitud cero.

```
TelephoneNumber ::= PrintableString (SIZE (0. .ub-telephone-number))
```

Nota – Pueden aparecer uno o más descriptores O/D en cada uno de los siguientes campos de encabezamiento: originador, usuarios autorizantes, destinatarios primarios, destinatarios de copia, destinatarios de copia ciega, y destinatarios de respuesta. Además, puede aparecer un descriptor O/D en los siguientes campos de notificación (véase el § 8): Originador de NIP y destinatario preferido de MIP.

7.2 *Campos de encabezamiento*

Los campos que pueden aparecer en el encabezamiento de un MIP son los definidos y descritos a continuación.

```
Heading ::= SET {
        this-IPM                    ThisIPMField,
        originator                  [0] OriginatorField OPTIONAL,
        authorizing-users           [1] AuthorizingUsersField OPTIONAL,
        primary-recipients          [2] PrimaryRecipientsField DEFAULT {},
        copy-recipients             [3] CopyRecipientsField DEFAULT {},
        blind-copy-recipients       [4] BlindCopyRecipientsField OPTIONAL,
        replied-to-IPM              [5] RepliedToIPMField OPTIONAL,
        obsoleted-IPMs              [6] ObsoletedIPMsField DEFAULT {},
        related-IPMs                [7] RelatedIPMsField DEFAULT {},
        subject                     [8] EXPLICIT SubjectField OPTIONAL,
        expiry-time                 [9] ExpiryTimeField OPTIONAL,
        reply-time                  [10] ReplyTimeField OPTIONAL,
        reply-recipients            [11] ReplyRecipientsField OPTIONAL,
        importance                  [12] ImportanceField DEFAULT normal,
        sensitivity                 [13] SensitivityField OPTIONAL,
        auto-forwarded              [14] AutoForwardedField DEFAULT FALSE,
        extensions                  [15] ExtensionsField DEFAULT {}}
```

Algunos campos tienen componentes siendo por tanto compuestos, y no indivisibles. Un componente de un campo se denomina **subcampo**.

7.2.1 *Este MIP*

El campo de encabezamiento **este MIP** (O) identifica el MIP. Comprende un identificador de MIP.

ThisIPMField ::= IPMIdentifier

7.2.2 *Originador*

El campo de encabezamiento **originador** (F) identifica el originador del MIP. Comprende un descriptor O/D.

OriginatorField ::= ORDescriptor

7.2.3 *Usuarios autorizantes*

El campo de encabezamiento **usuarios autorizantes** (C) identifica a los cero o más usuarios que son los *usuarios autorizantes* del MIP. Comprende una secuencia de subcampos, siendo cada uno de ellos un descriptor O/D, uno para cada uno de esos usuarios.

AuthorizingUsersField ::= SEQUENCE OF AuthorizingUsersSubfield

AuthorizingUsersSubfield ::= ORDescriptor

Un **usuario autorizante** es un usuario que, sea individualmente o en concierto con otros, autoriza la originación de un MIP. La palabra «autoriza» utilizada anteriormente no se define con precisión en esta Recomendación; su significado se lo dan los usuarios.

Este campo condicional estará presente únicamente si los usuarios autorizantes son otros distintos del originador del MIP.

Nota – Supóngase, por ejemplo, que un director da instrucciones a su secretario(a) para que origine un MIP en su nombre. En este caso, el(la) secretario(a), que es el originador del MIP, podría considerar que el director es el usuario autorizante.

7.2.4 *Destinatarios primarios*

El campo de encabezamiento **destinatarios primarios** (D sin subcampos, es decir, elementos) identifica a los cero o más usuarios y LD que son los «destinatarios primarios» del MIP. Identifica también las respuestas que los usuarios autorizantes solicitan de cada uno de esos usuarios y de cada miembro de esas LD. Comprende una secuencia de subcampos, cada uno de los cuales es un especificador de destinatario, uno para cada destinatario primario.

PrimaryRecipientsField ::= SEQUENCE OF PrimaryRecipientsSubfield

PrimaryRecipientsSubfield ::= RecipientSpecifier

La frase «destinatarios primarios» utilizada anteriormente no está definida con precisión en esta Recomendación; su significado se lo dan los usuarios.

Nota – Los destinatarios primarios, por ejemplo, pudieran ser los usuarios y las LD, cuyos miembros se espera actúen sobre el MIP.

7.2.5 *Destinatarios de copia*

El campo de encabezamiento **destinatarios de copia** (D sin subcampos, es decir, elementos) identifica a los cero o más usuarios y LD que son los «destinatarios de copia» del MIP. Identifica también las respuestas que los usuarios autorizantes solicitan de cada uno de esos usuarios y de cada miembro de esas LD. Comprende una secuencia de subcampos, cada uno de los cuales es un especificador de destinatario, uno para cada destinatario de copia.

CopyRecipientsField ::= SEQUENCE OF CopyRecipientsSubfield

CopyRecipientsSubfield ::= RecipientSpecifier

La frase «destinatarios de copia» no está definida con precisión en esta Recomendación; su significado se lo dan los usuarios.

Nota – Los destinatarios de copia, por ejemplo, podrían ser los usuarios a los cuales se transfiere el MIP para información, o las LD a cuyos miembros se transfiere el MIP para información.

7.2.6 *Destinatarios de copia ciega*

El campo de encabezamiento **destinatarios de copia ciega** (C) identifica a los cero o más usuarios y LD que son los «destinatarios» de copia *ciega* previstos del MIP. Identifica también las respuestas que los usuarios autorizantes solicitan de cada uno de esos usuarios y de cada miembro de esas LD. Comprende una secuencia de subcampos siendo cada uno de ellos un especificador de destinatario, uno para cada destinatario de copia *ciega.*

BlindCopyRecipientsField ::= SEQUENCE OF BlindCopyRecipientsSubfield

BlindCopyRecipientsSubfield ::= RecipientSpecifier

La frase «destinatarios de copia» que aparece anteriormente tiene el mismo significado que en el § 7.2.5. Un destinatario de copia **ciega** es un destinatario cuyo rol no se revela a los destinatarios primarios ni a los de copia.

En el caso de un MIP previsto para un destinatario de copia ciega, este campo condicional estará presente e identificará a ese usuario o LD. El que deba o no identificar también a los otros destinatarios de copia ciega es un asunto local. En el caso de un MIP previsto para un destinatario primario o un destinatario de copia, este campo estará ausente o no identificará ningún usuario ni LD.

7.2.7 *MIP contestado*

El campo de encabezamiento **MIP contestado** (C) identifica al MIP al cual responde el presente MIP. Comprende un identificador de MIP.

RepliedToIPMField ::= IPMIdentifier

Este campo condicional estará presente únicamente si el MIP es una respuesta.

Nota – En el contexto de *retransmisión*, debe distinguirse cuidadosamente entre el *MIP retransmisor* y el *MIP retransmitido.* Este campo debe identificar a cuál de estos dos MIP corresponde la respuesta.

7.2.8 *MIP obsoletos*

El campo de encabezamiento **MIP obsoletos** (D sin subcampos, es decir, elementos) identifica a los cero o más MIP que los usuarios autorizantes del presente MIP consideran obsoletos por este MIP. Comprende una secuencia de subcampos, siendo cada uno de ellos un identificador de MIP, uno para cada MIP.

ObsoletedIPMsField ::= SEQUENCE OF obsoletedIPMSubfield

ObsoletedIPMsSubfield ::= IPMIdentifier

Nota – En el contexto de *retransmisión*, debe tenerse cuidado de distinguir entre el *MIP retransmisor* y el *MIP retransmitido.* Este campo debe identificar cuál de estos dos MIP se hace obsoleto por el presente MIP.

7.2.9 *MIP relacionados*

El campo de encabezamiento **MIP relacionados** (D sin subcampos, es decir, elementos) identifica a los cero o más MIP que el usuario autorizante del presente MIP considera relacionados con este MIP. Comprende una secuencia de subcampos, cada uno de los cuales es un identificador de MIP, uno para cada MIP.

RelatedIPMsField ::= SEQUENCE OF RelatedIPMsSubfield

RelatedIPMsSubfield ::= IPMIdentifier

La palabra «relacionados», utilizada anteriormente, no está definida con precisión en esta Recomendación; su significado se lo dan los usuarios.

Nota 1 – Un MIP relacionado podría ser, por ejemplo, uno examinado en el cuerpo del MIP presente.

Nota 2 – En el contexto de *retransmisión*, debe distinguirse cuidadosamente entre el *MIP retransmisor* y el *MIP retransmitido*. Este campo debe identificar cuál de estos dos MIP está relacionado con el presente MIP.

7.2.10 *Asunto*

El campo de encabezamiento **asunto** (F) identifica el asunto del MIP. Es una cadena teletex de cero a un número prescrito de caracteres (véase el anexo K), tomados del subjuego gráfico del juego de caracteres de cadena teletex. Se desaconseja una longitud cero.

SubjectField ::= TeletexString (SIZE (0. .ub-subject-field))

7.2.11 *Hora de expiración*

El campo de encabezamiento **hora de expiración** (F) identifica cuándo los usuarios autorizantes consideran que el MIP pierde su validez. Comprende una fecha y una hora.

ExpiryTimeField ::= Time

7.2.12 *Hora de respuesta*

El campo de encabezamiento **hora de respuesta** (F) identifica el momento hasta el cual los usuarios autorizantes solicitan (pero no exigen) que se originen las eventuales respuestas al presente MIP. Comprende una fecha y una hora.

ReplyTimeField ::= Time

7.2.13 *Destinatarios de respuesta*

El campo de encabezamiento **destinatarios de respuesta** (C) identifica a los cero o más usuarios y LD a los cuales los usuarios autorizantes piden (pero no les exigen) que estén entre los destinatarios preferidos de las eventuales respuestas al presente MIP. Comprende una secuencia de subcampos, cada uno de los cuales es un descriptor O/D, uno para cada usuario o LD.

ReplyRecipientsField ::= SEQUENCE OF ReplyRecipientsSubfield

ReplyRecipientsSubfield ::= ORDescriptor

Este campo condicional estará presente únicamente si los destinatarios de respuesta deseados no son el originador del presente MIP.

Nota – Si este campo está presente e identifica a varios usuarios y LD el originador puede incluirse él mismo entre ellos. Si opta por no hacerlo, no se le considerará entre los destinatarios de copia deseados.

7.2.14 *Importancia*

El campo de encabezamiento **importancia** (D *normal*) identifica la importancia que los usuarios autorizantes atribuyen al MIP. Puede adoptar uno de los siguientes valores: *baja*, *normal*, o *alta*.

```
ImportanceField ::= ENUMERATED {
        low         (0),
        normal      (1),
        high        (2) }
```

Los valores indicados más arriba no están definidos en esta Recomendación; su significado se los dan los usuarios.

7.2.15 *Sensibilidad*

El campo de encabezamiento **sensibilidad** (C) identifica la sensibilidad que los usuarios autorizantes atribuyen al MIP.

```
SensitivityField ::= ENUMERATED {
        personal                (1),
        private                 (2),
        company-confidential    (3) }
```

Este campo puede adoptar uno de los siguientes valores:

a) *personal*: El MIP es transportado a los destinatarios preferidos en su carácter de individuos, y no en el de sus capacidades profesionales.

b) *privado*: El MIP debe transportarse a los destinatarios preferidos, y no a otros.

c) *confidencial de empresa*: El MIP contiene información que sólo debe tratarse de acuerdo con procedimientos especiales de la empresa.

Este campo condicional estará presente únicamente si el MIP es sensible.

7.2.16 *Retransmitido automáticamente*

El campo de encabezamiento **retransmitido automáticamente** (D *falso*) indica si el MIP es o no el resultado de *retransmisión automática*. Es un booleano.

```
AutoForwardedField ::= BOOLEAN
```

7.2.17 *Ampliaciones*

El campo de encabezamiento **ampliaciones** (D no *ampliaciones*, es decir, marcas) transporta una información que no esta contenida en ningún otro campo de encabezamiento. Comprende un conjunto de cero o más **ampliaciones de encabezamiento** (o **ampliaciones**), cada una de las cuales transporta un elemento de esa información.

```
ExtensionsField ::= SET OF HeadingExtension

HeadingExtension ::= SEQUENCE {
        type        OBJECT IDENTIFIER,
        value       ANY DEFINED BY type DEFAULT NULL NULL }
```

Cada ampliación tiene los siguientes componentes:

a) **Tipo** (O): Identifica la semántica y restringe la sintaxis abstracta del componente *valor*. Es un identificador de objeto.

b) **Valor** (D nulo): Elemento de información cuya sintaxis abstracta sólo está restringida por el componente tipo. Es un Any.

Los componentes tipo de todas las ampliaciones del campo ampliaciones deberán ser diferentes unos de otros. No es necesario que cada ampliación definida aparezca en el campo.

Todas las ampliaciones se definen en el anexo A. Así, cada componente tipo de la ampliación tendrá uno de los valores indicados en ese anexo. Una ampliación cuyo componente tipo tenga otro valor deberá ser ignorada.

Toda ampliación se define por medio de la siguiente macro.

```
HEADING-EXTENSION MACRO ::=
BEGIN
        TYPE   NOTATION ::= "VALUE" type | empty
        VALUE  NOTATION ::= value (VALUE OBJECT IDENTIFIER)

END
```

Un caso de notación de tipo de la macro identifica el tipo de datos al cual estará circunscrito el componente valor de la ampliación. Si no se identifica explícitamente ningún tipo, se supone nulo.

Un caso de notación de valor de la macro identifica el identificador de objeto que aparecerá como el componente tipo de la amplicación.

Nota – En futuras versiones de esta Recomendación se podrán definir ampliaciones adicionales. Además, es probable que, en las futuras versiones, se añada información sólo por medio de este campo.

7.3 *Tipos de parte de cuerpo*

A continuación se describen y definen los tipos de parte de cuerpo que pueden aparecer en el cuerpo de un MIP.

```
BodyPart ::= CHOICE {
        ia5-text                [0]  IA5TextBodyPart,
        voice                   [2]  VoiceBodyPart,
        g3-facsimile            [3]  G3FacsimileBodyPart,
        g4-class1               [4]  G4Class1BodyPart,
        teletex                 [5]  TeletexBodyPart,
        videotex                [6]  VideotexBodyPart,
        encrypted               [8]  EncryptedBodyPart,
        message                 [9]  MessageBodyPart,
        mixed-mode              [11] MixedModeBodyPart,
        bilaterally-defined     [14] BilaterallyDefinedBodyPart,
        nationally-defined      [7]  NationallyDefinedBodyPart,
        externally-defined      [15] ExternallyDefinedBodyPart }
```

Las partes de cuerpo de algunos tipos definidos más adelante tienen dos componentes: *parámetros* y *datos*. El componente **parámetro** (O) comprende una secuencia de elementos de información que describen el objeto de información representado por la parte de cuerpo y que típicamente son parámetros de formato y de control. El componente **datos** (O) es el objeto de información propiamente dicho.

Nota 1 – En la Recomendación X.420 (1984), los rótulos específicos del contexto 1 y 10 indican partes de cuerpo telex y documento formateable simple, respectivamente, que ya no están definidas. Por tanto, en la parte de cuerpo se evita el empleo de estos rótulos.

Nota 2 – En ciertas circunstancias, un MIP puede experimentar una conversión en su tránsito entre los usuarios. Tal suceso de transferencia puede alterar un tipo de parte de cuerpo.

7.3.1 *Texto AI5*

Una parte de cuerpo **texto AI5** representa texto construido con caracteres del AI5. Tiene componentes parámetros y datos.

```
IA5TextBodyPart ::= SEQUENCE {
        parameters              IA5TextParameters,
        data                    IA5TextData }

IA5TextParameters ::= SET {
        repertoire  [0] Repertoire DEFAULT ia5 }

IA5TextData ::= IA5String
```

El componente parámetros comprende los siguientes parámetros:

a) **Repertorio** (D*AI5*): Identifica el juego de caracteres a que está limitado el componente Datos.

```
Repertoire ::= ENUMERATED {
        ita2  (2),
        ia5   (5) }
```

Este parámetro puede adoptar uno cualquiera de los siguientes valores:

i) *ATI2*: El componente datos estará limitado al juego de caracteres del ATI2 (es decir telex).

ii) *AI5*: El componente datos puede tomar caracteres del juego completo de caracteres del AI5.

El componente datos es el texto, una cadena AI5. Puede contener líneas de cualquier longitud. Siempre que se reproduzca este componente (por ejemplo, en una pantalla o en una impresora para un usuario), deberá presentarse la totalidad del texto (y no una parte del mismo; por ejemplo, las líneas podrán dividirse de modo que continúen en el renglón siguiente, pero no podrán truncarse).

Nota – Muchos terminales tienen una longitud de línea máxima de 80 caracteres. En consecuencia, las líneas cuya longitud no sea superior a ésta probablemente se presenten satisfactoriamente (por ejemplo, lo más probable es que no serán divididas).

7.3.2 *Voz*

Una parte de cuerpo **voz** representa conversación. Tiene componentes parámetros y datos.

```
VoiceBodyPart ::= SEQUENCE {
        parameters              VoiceParameters,
        data                    VoiceData }

VoiceParameters ::= SET -- para ulterior estudio

VoiceData ::= BIT STRING -- para ulterior estudio
```

Los parámetros de tal parte de cuerpo, y la técnica de codificación de la conversación digitalizada que esos parámetros pudieran identificar y parametrizar serán objeto de ulterior estudio.

El componente datos es la conversación, una cadena de bits.

7.3.3 *Facsímil G3*

Una parte de cuerpo **facsímil G3** representa imágenes facsímil del grupo 3. Tiene componentes parámetros y datos.

```
G3FacsimileBodyPart ::= SEQUENCE {
        parameters              G3FacsimileParameters,
        data                    G3FacsimileData }

G3FacsimileParameters ::= SET {
        number-of-pages         [0]  INTEGER OPTIONAL,
        non-basic-parameters    [1]  G3FascimileNonBasicParameters OPTIONAL }

G3FacsimileData ::= SEQUENCE OF BIT STRING
```

El componente parámetros comprende los siguientes parámetros:

a) **Número-de-páginas** (F): Identifica el número de páginas de datos facsímil del grupo 3 presentes en el componente datos. Es un entero no negativo.

b) **Parámetros-no-básicos** (C): Identifica los parámetros no básicos (PNB) para el facsímil del grupo 3 que caracterizan al componente datos. Es un descriptor de PNB G3.

   Este parámetro condicional estará presente si el cuerpo contiene dos o más partes de cuerpo facsímil G3 (pero puede también estar presente en otro caso).

El componente datos lo forman las imágenes facsímil, que son una secuencia de cadenas de bits, cada una de las cuales codifica una sola página de datos facsímil del grupo 3, como se especifica en las Recomendaciones T.4 y T.30.

Nota 1 – El componente número-de-páginas identifica el número de elementos en la secuencia que constituye el componente datos y es por tanto redundante.

Nota 2 – Si el cuerpo comprende una sola de estas partes de cuerpo, sus PNB pueden (pero no están obligados a) ser transportados por medio de la envolvente del mensaje que contiene el MIP.

7.3.4 *G4 Clase 1*

Una parte de cuerpo **G4 Clase 1** representa un documento en forma final del género que puede ser procesado por terminales facsímil del grupo 4 clase 1. Comprende una secuencia de elementos de protocolo que describen la estructura de la disposición del documento.

```
G4Class1BodyPart ::= SEQUENCE OF ProtocolElement
```

7.3.5 *Teletex*

Una parte de cuerpo **teletex** representa un documento teletex. Tiene componentes parámetros y datos.

```
TeletexBodyPart ::= SEQUENCE {
        parameters              TeletexParameters,
        data                    TeletexData }

TeletexParameters ::= SET {
        number-of-pages         [0]  INTEGER OPTIONAL,
        telex-compatible        [1]  BOOLEAN DEFAULT FALSE,
        non-basic-parameters    [2]  TeletexNonBasicParameters OPTIONAL }

TeletexData ::= SEQUENCE OF TeletexString
```

El componente parámetros comprende los siguientes parámetros:

a) **Número-de-páginas** (F): Identifica el número de páginas del texto teletex presentes en el componente datos. Es un entero no negativo.

b) **Compatible-telex** (D*falso*): Indica si el documento en el componente datos es o no compatible con el telex. Es un booleano.

   Si este parámetro tiene el valor *verdadero* (*true*), cada cadena teletex en el componente datos estará limitada al juego de caracteres del AIT2. Ninguna línea tendrá una longitud superior a 69 caracteres.

c) **Parámetros-no-básicos** (C): Identifica los PNB para teletex que caracterizan el componente datos. Es un descriptor PNB teletex.

Este parámetro condicional estará presente si el cuerpo contiene dos o más partes de cuerpo teletex (pero puede también estar presente en otro caso).

El componente datos es el documento, una Secuencia de cadenas teletex, cada una de las cuales codifica una de sus páginas.

Nota 1 – El componente número-de-páginas identifica el número de elementos en la secuencia que constituye el componente datos, y es por tanto redundante.

Nota 2 – Si el cuerpo comprende una sola parte de cuerpo, sus PNB pueden (pero no tienen necesariamente que) ser transportados por medio del sobre del mensaje que contiene el MIP.

7.3.6 *Videotex*

Una parte de cuerpo **videotex** representa datos videotex. Tiene componentes parámetros y datos.

```
VideotexBodyPart ::= SEQUENCE {
        parameters          VideotexParameters,
        data                VideotexData }

VideotexParameters ::= SET {
        syntax              [0] VideotexSyntax OPTIONAL }

VideotexData ::= VideotexString
```

El componente parámetro comprende los siguientes parámetros:

a) **Sintaxis** (F): Identifica la sintaxis del componente datos. Cuando no hay parámetros, se considera que la sintaxis no está especificada.

```
VideotexSyntex ::= INTEGER {
        ids                 (0),
        data-syntax1        (1),
        data-syntax2        (2),
        data-syntax3        (3) }
```

Este parámetro puede adoptar uno de los siguientes valores, cada uno de los cuales designa una de las sintaxis videotex definidas en las Recomendaciones T.100 y T.101:

i) *sdi*: Sintaxis de datos de interfuncionamiento (sintaxis SDI).

ii) *sintaxis-de-datos1*: Sintaxis de datos 1.

iii) *sintaxis-de-datos2*: Sintaxis de datos 2.

iv) *sintaxis-de-datos3*: Sintaxis de datos 3.

El componente datos está constituido por los datos videotex, que constituyen una cadena videotex. Se ajustará a la sintaxis videotex designada por el parámetro sintaxis.

7.3.7 *Cifrado*

Una parte de cuerpo **cifrado** representa el resultado de cifrar una parte de cuerpo de un tipo definido por esta Recomendación. Tiene componentes parámetros y datos.

```
EncryptedBodyPart ::= SEQUENCE {
        parameters          EncryptedParameters,
        data                EncryptedData }

EncryptedParameters ::= SET -- para ulterior estudio

EncryptedData ::= BIT STRING -- para ulterior estudio
```

Los parámetros de esta parte de cuerpo, y la técnica de cifrado que estos parámetros pudieran identificar y parametrizar, quedan para ulterior estudio.

El componente datos es la parte de cuerpo cifrada, formada por una cadena de bits. Los bits de la cadena cifrarán un valor de datos del tipo BodyPart (NSA.1) codificado de acuerdo con las reglas básicas de codificación de la Recomendación X.209.

7.3.8 *Mensaje*

Una parte de cuerpo **mensaje** representa un MIP y, facultativamente, su sobre de entrega. Tiene componentes parámetros y datos.

```
MessageBodyPart ::= SEQUENCE {
        parameters          MessageParameters,
        data                MessageData }

MessageParameters ::= SET {
        delivery-time       [0] MessageDeliveryTime OPTIONAL,
        delivery-envelope   [1] OtherMessageDeliveryFields OPTIONAL }

MessageData ::= IPM
```

El componente parámetros comprende los siguientes parámetros.

a) **Hora-de-entrega** (F): Fecha y hora en que fue entregado el MIP. Se desaconseja la presencia de este componente estando ausente el componente sobre de entrega.

b) **Sobre-de-entrega** (F): Los demás campos de entrega de mensaje del MIP. Se desaconseja la presencia de este componente en ausencia del componente hora-de-entrega.

El componente datos es el MIP.

La inclusión de un MIP dentro de otro como se describe en el presente punto se denomina **retransmisión** de ese MIP. El MIP englobante se denomina **MIP retransmisor**, el MIP englobado se denomina el **MIP retransmitido**.

Nota 1 – La posible inclusión en el futuro de identificador de mensaje en el componente parámetros queda para ulterior estudio. Su omisión presente proporciona la compatibilidad con la Recomendación X.420 (1984).

Nota 2 – No se verifica el que el MIP y el sobre de entrega contemplado de una parte de cuerpo mensaje sean, en todo sentido, genuinos.

7.3.9 *Modo mixto*

Una parte de cuerpo **modo mixto** representa un documento en forma final de género que puede ser procesado por terminales teletex modo mixto y terminales facsímil del grupo 4, clases 2 y 3. Está constituida por una secuencia de elementos de protocolo que describen la estructura de disposición del documento.

```
MixedModeBodyPart ::= SEQUENCE OF ProtocolElement
```

7.3.10 *Definida bilateralmente*

Una parte de cuerpo **definida bilateralmente** representa un objeto de información cuya semántica y sintaxis abstracta son convenidas bilateralmente por el originador y todos los destinatarios potenciales del MIP. Está constituida por una cadena de octetos.

```
BilaterallyDefinedBodyPart ::= OCTET STRING
```

Nota – Se desaconseja el uso de este tipo de parte de cuerpo. Ella antedata el tipo de parte de cuerpo definido externamente y se mantiene con miras a la compatibilidad descendente con la Recomendación X.420 (1984). El tipo de parte de cuerpo definido externamente proporciona las mismas capacidades, y otras más, y se prefiere su uso, por ejemplo, porque en el mismo se distingue claramente entre las partes de cuerpo definidas por una comunidad de usuarios y las definidas por otra.

7.3.11 *Definida nacionalmente*

Una parte de cuerpo **definida nacionalmente** representa un objeto de información cuya semántica y sintaxis abstracta están definidas nacionalmente por un país cuya identidad está convenida bilateralmente por el originador y todos los destinatarios potenciales del MIP. Está constituida por un tipo Any.

```
NationallyDefinedBodyPart ::= ANY
```

Nota 1 – Este tipo de parte de cuerpo está destinado a ser utilizado en comunicación dentro de un mismo país, siendo el país en cuestión, implícitamente el del originador y el de todos los destinatarios potenciales.

Nota 2 – Se desaconseja la utilización de este tipo de parte de cuerpo. Ella antedata el tipo de parte de cuerpo definido externamente y se mantiene con miras a la compatibilidad descendente con la Recomendación X.420 (1984). El tipo de parte de cuerpo definido externamente proporciona las mismas capacidades, y otras más, y su uso se prefiere, por ejemplo, porque en el mismo distingue claramente entre las partes de cuerpo definidas por un país y las definidas por otro.

7.3.12 *Definida externamente*

Una parte de cuerpo **definida externamente** representa un objeto de información cuya semántica y sintaxis abstracta son designadas por un identificador de objeto transportado en la parte de cuerpo. Tiene componentes parámetros y datos.

```
ExternallyDefinedBodyPart ::= SEQUENCE {
        parameters          [0] ExternallyDefinedParameters OPTIONAL,
        data                    ExternallyDefinedData }

ExternallyDefinedParameters ::= EXTERNAL

ExternallyDefinedData ::= EXTERNAL
```

Los componentes parámetros y datos son externos (véase el § 32 de la Recomendación X.208). Sus componentes referencia-directa deben estar presentes, y sus componentes referencia-indirecta y descriptor-de-valor-de-datos estarán ausentes.

Sobre la base del tipo de parte de cuerpo definida externamente, todos los tipos de parte de cuerpo se dividen en las dos importantes clases siguientes:

a) **básico**: contiene cualquier tipo de parte de cuerpo, excepto definida externamente. Se designa por un entero (un rótulo NSA.1 específico del contexto).

   Todos los tipos de parte de cuerpo básicos se definen en esta Recomendación.

b) **ampliado**: contiene el tipo de parte de cuerpo definida externamente, limitado a uno cualquiera de los valores del componente referencia-directa del componente datos de tal parte de cuerpo. Se designa por un identificador de Objeto.

   Algunos (pero no necesariamente todos) los tipos de parte de cuerpo ampliado se definen en el anexo B de esta Recomendación.

Cada tipo de parte de cuerpo ampliado que define esta Recomendación está definido por medio de la siguiente macro. Cada tipo de parte de cuerpo ampliado definido en otro lugar deberá también ser definido.

```
EXTENDED-BODY-PART-TYPE MACRO ::=
BEGIN
        TYPE   NOTATION ::= Parameters Data
        VALUE  NOTATION ::= value (VALUE OBJECT IDENTIFIER)

        Parameters          ::= "PARAMETERS" type "IDENTIFIED" "BY" value (OBJECT
                                IDENTIFIER) | empty
        Data                ::= "DATA" type

END
```

Un caso de notación de tipo de la macro define, por medio de su cláusula PARÁMETROS, el tipo del valor de datos que es representado por el componente parámetros del tal parte de cuerpo (definida externamente) (un tipo externo) y el identificador de objeto que aparece en el componente referencia-directa de este componente de parámetros. La omisión del componente de parámetros va implicada por la omisión de esta cláusula. Un caso de notación del tipo define también, por medio de su cláusula DATOS, el tipo del valor de datos representado por el componente datos de tal parte de cuerpo (un tipo externo).

Un caso de la notación de valor de la macro define el identificador de objeto que aparece como el componente referencia-directa del componente datos de tal parte de cuerpo (definida externamente). El identificador de objeto identifica las reglas de codificación para la parte de cuerpo. Aquellas partes de cuerpo cuyos tipos están definidos en esta Recomendación se codificarán utilizando las reglas básicas de codificación de NSA.1.

Nota 1 – Este tipo de parte de cuerpo permite el intercambio de objetos de información de todas clases, cada uno de los cuales está identificado de manera inequívoca y única. Esta identificación se basa en el componente referencia-directa mencionado anteriormente, que es un identificador de objeto. Los identificadores de objeto se obtienen fácilmente, por ejemplo, por los organismos nacionales y organizaciones privadas.

Nota 2 – Si una parte de cuerpo definida externamente posee un componente parámetros, el identificador de objeto de su componente referencia-directa se asigna al mismo tiempo y por la misma autoridad denominadora que la del componente de referencia-directa del componente datos.

Nota 3 – Al igual que las partes de cuerpo de otros tipos, una parte de cuerpo definida externamente puede ser objeto de una conversión. Sin embargo, la especificación del algoritmos de conversión pueden estar fuera del ámbito de la Recomendación X.408 del CCITT.

Nota 4 – Los tipos básicos de parte de cuerpo existen por razones puramente históricas, antedatando el tipo de parte de cuerpo definida externamente.

8 Notificaciones interpersonales

Una **notificación interpersonal (NIP)** es un miembro de una clase secundaria de objetos de información transportado entre usuarios en mensajería interpersonal.

```
IPN ::= SET{
        -- common-fields -- COMPONENTS OF CommonFields,
        choice [0] CHOICE{
            non-receipt-fields      [0] NonReceiptFields,
            receipt-fields          [1] ReceiptFields}}
```

Una NIP puede adoptar una de las formas siguientes:

a) **notificación-de-no-recepción (NNR)**: NIP que informa al originador de un MIP que dicho mensaje no se recibirá, no se aceptará o se recibirá con retardo.

NRN ::= IPN -- *con campos-de-no-recepción elegidos*

b) **notificación de recepción (NR)**: NIP que informa al originador de un MIP que éste ha sido recibido, o que se espera y está dispuesta su futura recepción.

RN ::= IPN -- *con campos-de-recepción elegidos*

El MIP al que se refiere una NIP se denomina **MIP asunto**. Sólo un AU al que se entrega efectivamente el MIP asunto originará una NIP relacionada con dicho MIP, y originará, como máximo, una tal NIP que deberá ser transportada al originador del MIP asunto.

Un destinatario efectivo deberá originar una NIP solamente de acuerdo con el componente peticiones de notificación del *especificador de destinatario asunto.* El **especificador de destinatario asunto** es el especificador de destinatario en el encabezamiento del MIP asunto, como resultado del cual se entrega a ese usuario el MIP asunto.

Se determina el especificador de destinatario asunto examinando las secuencias de especificadores de destinatario que constituyen los campos de encabezamiento destinatarios primarios, destinatarios de copia y destinatarios de copia ciega del MIP asunto. Los campos se examinan en el orden en que son mencionados en el párrafo anterior. Dentro de cada campo, los especificadores se examinan en el orden en que allí aparecen. El especificador de destinatario asunto es el primero encontrado cuyo componente destinatario tiene como valor un descriptor O/D cuyo componente nombre formal está presente y tiene como valor, bien un nombre O/D del destinatario preferido, como resultado del cual el MIP asunto fue entregado al usuario a cuyo nombre se efectuó el examen, o bien, si el usuario recibe el MIP por figurar en una LD, un nombre O/D que aparece en la historia de ampliación de la LD del mensaje (véase el § 8.3.1.1.1.7 de la Recomendación X.411).

Una NIP consta de un conjunto de elementos de información denominados **campos de notificación** (o **campos**), cada uno de los cuales es de una de las clases siguientes:

a) **campo común**: Campo de notificación aplicable a las NNR y las NR.

b) **campo de no recepción**: Campo de notificación aplicable a las NNR solamente.

c) **campo de recepción**: Campo de recepción aplicable a las NR solamente.

La estructura de una NIP se describe en la figura 2/X.420.

A continuación se definen y describen los campos, de cada una de las clases mencionadas, que puedan aparecer en una NIP.

8.1 *Campos comunes*

A continuación se definen y describen los campos comunes:

```
CommonFields ::= SET{
        subject-ipm                 SubjectIPMField,
        ipn-originator          [1] IPNOriginatorField OPTIONAL,
        ipm-preferred-recipient [2] IPMPreferredRecipientField OPTIONAL,
        conversion-eits             ConversionEITsField OPTIONAL}
```

8.1.1 *MIP asunto*

El campo común **MIP asunto** (O) identifica el MIP asunto. Consta de un identificador de MIP.

SubjectIPMField ::= IPMIdentifier

8.1.2 *Originador de NIP*

El campo común **originador de NIP** (F) identifica el originador de la NIP. Consta de un descriptor O/D.

IPNOriginatorField ::= ORDescriptor

Si el originador de la NIP es un destinatario preferido del MIP asunto, el descriptor O/D antes mencionado deberá ser exactamente el que es el valor del componente destinatario del especificador del destinatario asunto.

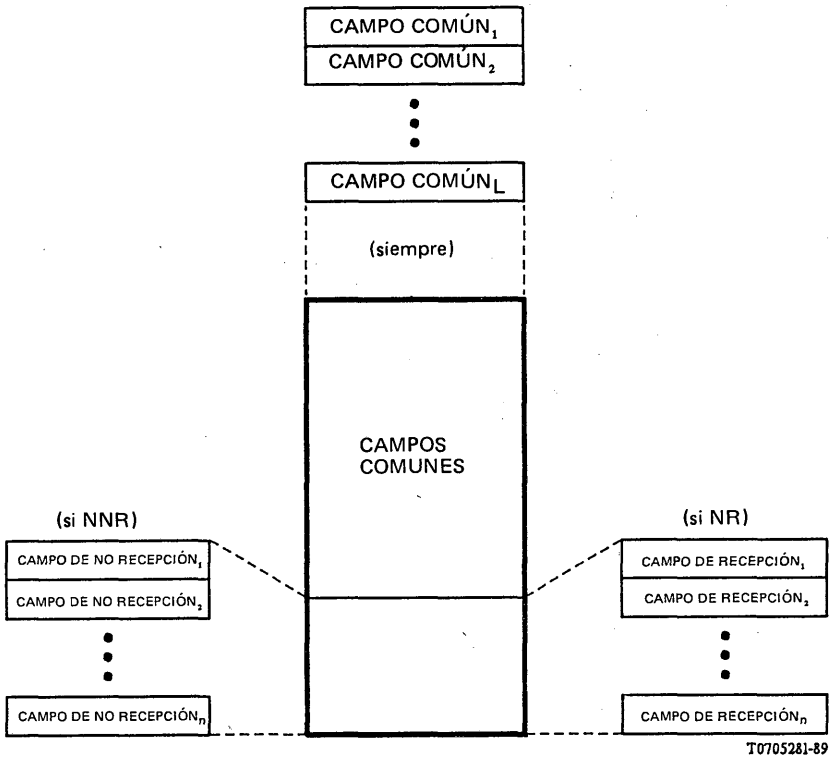


FIGURA 2/X.420

Notificación interpersonal

8.1.3 *Destinatario preferido de MIP*

El campo común **destinatario preferido de MIP** (C) identifica el destinatario preferido del MIP asunto que da lugar a su entrega al originador de la NIP (que será un destinatario alternativo, miembro de una LD o sustituto). Consta de un descriptor O/D.

IPMPreferredRecipientField ::= ORDescriptor

El descriptor O/D mencionado será exactamente el que es el valor del componente destinatario del especificador de destinatario asunto.

Este campo condicional estará presente si y sólo si identificase a un usuario que no fuese el originador de la NIP o una LD.

8.1.4 *TIC de conversión*

El campo común **TIC de conversión** (C) identifica los TIC del MIP asunto al efectuarse la entrega al originador de la NIP. Consta de un descriptor de TIC.

ConversionEITsField ::= EncodedInformationTypes

Este campo condicional estará presente si y sólo si el MIP estaba sujeto a una conversión para entrega del originador de la NIP.

8.2 *Campos de no recepción*

A continuación se definen y describen los campos de no recepción:

```
NonReceiptFields ::= SET{
        non-receipt-reason      [0]  NonReceiptReasonField,
        discard-reason          [1]  DiscardReasonField OPTIONAL,
        auto-forward-comment    [2]  AutoForwardCommentField OPTIONAL,
        returned-ipm            [3]  ReturnedIPMField OPTIONAL}
```

8.2.1 *Motivo de no recepción*

El campo de no recepción **motivo de no recepción** (O) indica el motivo por el cual el originador de la NNR no ha recibido el MIP asunto (aunque se le haya entregado).

```
NonReceiptReasonField ::= ENUMERATED {
        ipm-discarded           (0),
        ipm-auto-forwarded      (1) }
```

Este campo puede adoptar uno de los siguientes valores:

a) *mip-descartado*: El MIP fue descartado. Este caso es objeto de una explicación ulterior por el campo motivo de descarte.

b) *mip-retransmitido-automáticamente*: El MIP fue retransmitido automáticamente. Este caso es objeto de una explicación ulterior por el campo *comentario de retransmisión automática.*

8.2.2 *Motivo de descarte*

El campo de no recepción **motivo de descarte** (C) indica el motivo por el cual fue descartado el MIP asunto (después de su entrega al originador de la NNR y antes de su recepción).

```
DiscardReasonField ::= ENUMERATED {
        ipm-expired                     (0),
        ipm-obsoleted                   (1),
        user-subscription-terminated    (2) }
```

Este campo puede adoptar uno de los siguientes valores:

a) *mix-expirado*: Estaba en vigor descarte automático, los MIP expirados se descartaban, y llegó el tiempo identificado por el campo de encabezamiento hora de expiración del MIP asunto.

b) *mip-obsoleto*: Estaba en vigor descarte automático, los MIP obsoletos se estaban descartando, y el campo de encabezamiento MIP absoletos de otro MIP, entregado al originador de las NNR, identificó el MIP asunto.

c) *terminado-el-abono-del-usuario*: El abono a mensajería interpersonal del originador de la NNR ha terminado.

Este campo condicional estará presente únicamente si el campo motivo de no recepción tiene el valor *mip-descartado.*

8.2.3 *Comentario de retransmisión automática*

El campo de no recepción **comentario de retransmisión automática** (C) es una información suministrada previamente con esta finalidad por el originador de la NNR. Consta de una cadena imprimible de cero a un número prescrito de caracteres (véase el anexo K), tomados del juego de caracteres de cadena imprimible. Se desaconseja una longitud de cero.

```
AutoForwardCommentField ::= AutoForwardComment

AutoForwardComment ::= PrintableString
        (SIZE (0. .ub-auto-forward-comment)
```

El valor de este campo será exactamente el argumento del comentario de retransmisión automática de la operación abstracta *cambio retransmisión automática*, como resultado de la cual fue retransmitido automáticamente el MIP.

Este campo condicional estará presente únicamente si el campo motivo de no recepción tiene el valor *mip-retransmitido automáticamente* y se ha suministrado el argumento mencionado del comentario de retransmisión automática.

8.2.4 *MIP devuelto*

El campo de no recepción **MIP devuelto** (C) es precisamente el MIP asunto.

```
ReturnedIPMField ::= IPM
```

Este campo condicional estará presente únicamente si *devolución-mip* se encuentra entre los valores del componente peticiones de notificación del especificador de destinatario asunto y el MIP asunto no está sujeto a conversión para su entrega al originador de la NNR.

8.3 *Campos de recepción*

A continuación se definen y describen los campos de recepción:

```
ReceiptFields ::= SET {
        receipt-time            [0]  ReceiptTimeField,
        acknowledgment-mode     [1]  AcknowledgmentModeField DEFAULT manual,
        suppl-receipt-info      [2]  SupplReceiptInfoField DEFAULT"" }
```

8.3.1 *Hora de recepción*

El campo de recepción **hora de recepción** (O) identifica el momento en que el originador de la NR recibió el MIP asunto. Comprende una fecha y una hora.

```
ReceiptTimeField ::= Time
```

8.3.2 *Modo acuse de recibo*

El campo de recepción **modo acuse de recibo** (D *manual*) identifica el modo según el cual se originó la NR.

```
AcknowledgmentModeField ::= ENUMERATED {
        manual      (0),
        automatic   (1) }
```

Este campo puede adoptar uno de los valores siguientes:

a) *manual*: La NR fue originada por medio de la operación abstracta *generación NR.*

b) *automático*: La NR fue originada como resultado de *acuse automático de recibo.*

8.3.3 *Información de recepción suplementaria*

El campo de recepción **información de recepción suplementaria** (F) proporciona información suplementaria sobre la recepción del MIP asunto por el originador de la NR. Comprende una cadena imprimible de cero a un número prescrito de caracteres (véase la Recomendación X.411), tomados del juego de caracteres de cadena imprimible.

```
SupplReceiptInfoField ::= SupplementaryInformation
```

SECCIÓN 3 – DEFINICIÓN DE SERVICIO ABSTRACTO

9 Visión de conjunto

Esta sección define el servicio abstracto que caracteriza la mensajería interpersonal, y describe el entorno en el cual este servicio se proporciona y utiliza. Para esta definición y descripción se utilizan los convenios de definición de servicio abstracto de la Recomendación X.407.

Esta sección trata de los siguientes puntos:

a) Tipos de objetos primarios.

b) Tipos de puertos primarios.

c) Operaciones abstractas.

d) Errores abstractos.

e) Otras capacidades.

10 Tipos de objetos primarios

El entorno en que tiene lugar la mensajería interpersonal puede modelarse como un objeto abstracto que en lo sucesivo se denominará el **entorno de mensajería interpersonal (EMIP).**

```
ipme OBJECT
        ::= id-ot-ipme
```

El EMIP, cuando es redefinido (es decir, cuando se efectúa su descomposición funcional), puede considerarse que comprende objetos menores que interactúan por medio de puertos.

```
ipme-refinement REFINE ipme AS
        ipms
            origination   [S] PAIRED WITH ipms-user
            reception     [S] PAIRED WITH ipms-user
            management    [S] PAIRED WITH ipms-user
        ipms-user-RECURRING
        ::= id-ref-primary
```

Los objetos menores se denominan **objetos primarios** de mensajería interpersonal. Incluyen un objeto central único, el *sistema de mensajería interpersonal (SMIP)* y numerosos objetos periféricos denominados *usuarios de sistema de mensajería interpersonal (usuarios SMIP).*

La estructura del EMIP se describe en la figura 3/X.420.

A continuación se definen y describen los tipos de objetos primarios. Los tipos de puertos a través de los cuales interactúan los tipos de objeto primario se examinan en el § 11.

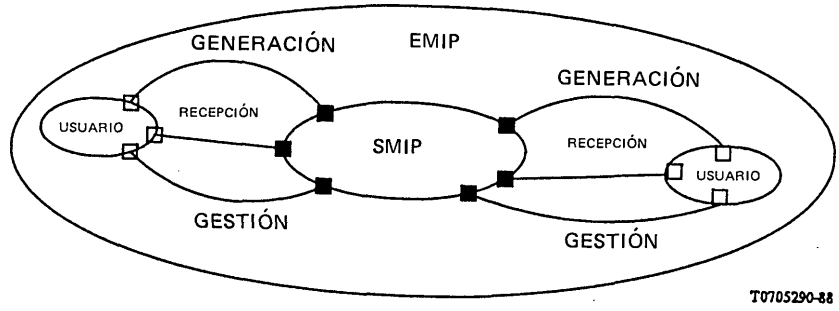


FIGURA 3/X.420

Entorno de mensajería interpersonal

10.1 *Usuario de sistema de mensajería interpersonal*

Un **usuario de sistema de mensajería interpersonal (usuario SMIP)** es un usuario que interviene en mensajería interpersonal. Un usuario SMIP origina, recibe, u origina y recibe, objetos de información de los tipos definidos en la sección dos.

```
ipms-user OBJECT
        PORTS {
            origination   [C],
            reception     [C],
            management    [C] }
        ::= id-ot-ipms-user
```

El EMIP comprende cualquier número de usuarios SMIP.

Nota 1 – Como sugiere su nombre, la mensajería interpersonal es típicamente una actividad de personas. Por esa razón, en esta Recomendación se utilizan pronombres personales (por ejemplo, «él») para hacer referencia a usuarios SMIP. Sin embargo, esta práctica no tiene por objeto la exclusión de otros usos, no típicos de la mensajería interpersonal, en los cuales los usuarios SMIP no son personas.

Nota 2 – Por razones de brevedad, en la parte restante de esta Recomendación, el término «usuario» se emplea con el significado de «usuario SMIP».

10.2 *Sistema de mensajería interpersonal*

El **sistema de mensajería interpersonal (SMIP)** es el objeto por medio del cual todos los usuarios comunican unos con otros en mensajería interpersonal.

```
ipms OBJECT
        PORTS {
            origination   [S],
            reception     [S],
            management    [S] }
        ::= id-ot-ipms
```

El EMIP comprende exactamente un SMIP.

11 Tipos de puertos primarios

Los objetos primarios de la mensajería interpersonal están unidos entre sí, e interactúan unos con otros por medio de puertos. Estos puertos, que son suministrados por el SMIP, se denominan **puertos primarios** de mensajería interpersonal. Son de los tres tipos definidos más adelante.

Nota – En el § 16, el SMIP se descompone en objetos aún menores, entre los cuales está el sistema de transferencia de mensajes (STRM). Este hecho se ha tenido previamente en cuenta en la presente sección por la inclusión de ciertas capacidades de STRM en el servicio abstracto SMIP.

11.1 *Generación*

Un **puerto de generación** es el medio por el cual un solo usuario transfiere al SMIP mensajes que contienen objetos de información de los tipos definidos en la sección dos. A través de ese puerto, el usuario genera *mensajes interpersonales* y *notificaciones de recepción.* Además, a través de tal puerto, el usuario puede generar sondas.

El SMIP suministra un puerto de originación para cada usuario (con excepción de los usados indirectos servidos por UAEF; véase el § 16.5).

11.2 *Recepción*

Un **puerto de recepción** es el medio por el cual el SMIP transporta a un usuario simple mensajes que contienen objetos de información de los tipos definidos en la sección dos. A través de este puerto el usuario puede recibir *mensajes interpersonales* y *notificaciones interpersonales.* Además, a través de tal puerto el usuario puede recibir informes.

El SMIP suministra un puerto de recepción a cada usuario.

11.3 *Gestión*

Un **puerto de gestión** es el medio por el cual un usuario simple cambia información relativa a sí mismo, que figura en un fichero del SMIP. Por medio de tal puerto el usuario activa y desactiva *descarte automático, acuse automático de recibo* y *retransmisión automática.*

El SMIP proporciona un puerto de gestión para cada usuario (con excepción de los usuarios indirectos servidos por UAEF; véase el § 16.5).

12 Operaciones abstractas

El **servicio abstracto SMIP** es el conjunto de capacidades que el SMIP proporciona a cada usuario por medio de un puerto de generación, un puerto de recepción y un puerto de gestión. Esas capacidades son modeladas con operaciones abstractas, que, cuando son invocadas, pueden encontrar errores abstractos.

A continuación se definen y describen las operaciones abstractas disponibles en los puertos de generación, recepción y gestión, respectivamente. Los errores abstractos que dichas operaciones pueden provocar se tratan en el § 13.

Nota 1 – El servicio abstracto SMIP no comprende operaciones abstractas de vinculación ni operaciones abstractas de desvinculación.

Nota 2 – El SMIP auténtica (es decir, establece la identidad de) el usuario típico antes de ofrecerle el servicio abstracto SMIP. Por este medio puede verificar, por ejemplo, que el usuario es un abonado SMIP. La autenticación, cuando se requiera, es implícita (y no explícita) en la definición del servicio abstracto SMIP.

Nota 3 – La finalidad de la definición del servicio abstracto SMIP no es la de prescribir los interfaces de usuarios de realizaciones de porciones del SMIP, sino la de aclarar el significado y el uso que se desea hacer de los objetos de información descritos en la sección dos. Un interfaz de usuario no necesita proporcionar instrucciones en correspondencia biunívoca con las operaciones abstractas del servicio, ni siquiera dividir la labor entre el usuario y el SMIP, como lo hace el servicio.

Nota 4 – En el § 16, el SMIP se descompone en objetos entre los cuales se encuentra el STRM. En este punto, se refleja este hecho por la inclusión de diversos elementos de información definidos por el STRM, en el servicio abstracto SMIP.

12.1 *Operaciones abstractas de realizaciones*

Las operaciones abstractas disponibles en el puerto de generación son invocadas por el usuario y efectuadas por el SMIP.

```
origination PORT
        CONSUMER INVOKES{
            OriginateProbe,
            OriginateIPM,
            OriginateRN }
        ::= id-pt-origination
```

12.1.1 *Generación sonda*

La operación abstracta **generación sonda** genera una sonda con relación a (una clase de) mensajes cuyo contenido está constituido por MIP.

```
OriginateProbe ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] ProbeSubmissionEnvelope,
            content   [1] IPM}
        RESULT SET{
            submission-identifier     [0] ProbeSubmissionIdentifier,
            submission-time           [1] ProbeSubmissionTime}
        ERRORS{
            SubscriptionError,
            RecipientImproperlySpecified}
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre de depósito de sonda, cuya composición está definida por el servicio abstracto STRM. El AU proporciona todos los componentes del sobre, excepto los siguientes que son suministrados por el usuario:

   i) Las opciones deseadas para cada mensaje (es decir, los indicadores y las ampliaciones para cada mensaje).

   ii) Los nombres O/D de los destinatarios preferidos y las opciones por cada destinatario (es decir, petición de informe del originador, conversión explícita, y ampliaciones) deseadas para cada uno.

b) **Contenido** (O): Caso de la clase de MIP cuya entregabilidad se sondea.

Esta operación abstracta tiene los siguientes resultados:

1) **Identificador de depósito** (O): Identificador de depósito de sonda que el STRM asigna a la sonda.

2) **Hora de depósito** (O): Fecha y hora en que la sonda fue depositada directamente.

12.1.2 *Generación MIP*

La operación abstracta **generación MIP** origina un mensaje cuyo contenido es un MIP.

```
OriginateIPM ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] MessageSubmissionEnvelope,
            content   [1] IPM}
        RESULT SET{
            submission-identifier     [0] MessageSubmissionIdentifier,
            submission-time           [1] MessageSubmissionTime}
        ERRORS{
            SubscriptionError,
            RecipientImproperlySpecified}
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre depósito de mensaje, cuya constitución está definida por el servicio abstracto STRM. El AU suministra todos los componentes de sobre salvo los siguientes, que son proporcionados por el usuario:

   i) Las opciones deseadas para cada mensaje (es decir, prioridad, indicadores para cada mensaje, hora de entrega diferida, y ampliaciones).

   ii) Los nombres O/D de los destinatarios preferidos y las opciones para cada destinatario (es decir, petición de informe de originador, conversión explícita, y ampliaciones) deseadas para cada uno.

b) **Contenido** (O): El MIP que se está originando. Su campo de encabezamiento de reenvío automático deberá estar ausente o tener el valor *falso.*

Esta operación abstracta tiene los siguientes resultados:

1) **Identificador de depósito** (O): Identificador de depósito de mensaje que el STRM asigna al depósito.

2) **Hora de depósito** (O): Fecha y hora en que el mensaje fue depositado directamente.

12.1.3 *Generación NR*

Operación abstracta **generación NR** cuyo contenido es una NR.

```
OriginateRN ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] MessageSubmissionEnvelope,
            content   [1] RN }
        RESULT SET{
            submission-identifier     [0] MessageSubmissionIdentifier,
            submission-time           [1] MessageSubmissionTime }
        ERRORS{
            SubscriptionError,
            RecipientImproperlySpecified }
```

Una NR será generada solamente por un destinatario efectivo del MIP asunto con relación al cual se ha solicitado una NR por medio del componente peticiones de notificación del especificador del destinatario asunto del MIP.

El usuario no deberá haber originado previamente una RN en respuesta al MIP asunto, por medio de la presente operación abstracta o un acuse automático de recibo.

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre de depósito de mensaje, cuya constitución está definida por el servicio abstracto STRM. El AU suministra todos los componentes de sobre salvo los siguientes, que son proporcionados por el usuario:

   i) Las opciones deseadas para cada mensaje (es decir, prioridad, indicadores para cada mensaje, y ampliaciones). Deberá prohibirse la conversión implícita, la prioridad será la del MIP asunto.

   ii) Los nombres O/D de los destinatarios preferidos y opciones para cada destinatario (es decir, conversión explícita y ampliaciones) deseadas, para cada uno. No se solicitarán informes.

b) **Contenido** (O): La RN que se está originando.

Esta operación abstracta tiene los siguientes resultados:

1) **Identificador de depósito** (O): El identificador de depósito de mensaje lo asigna el STRM al depósito.

2) **Hora de depósito** (O): Fecha y hora en que el mensaje fue depositado directamente.

12.2 *Operaciones abstractas de recepción*

Las operaciones abstractas disponibles en un puerto de recepción son invocadas por el SMIP y efectuadas por el usuario.

```
reception PORT
        SUPPLIER INVOKES{
            ReceiveReport,
            ReceiveIPM,
            ReceiveRN,
            ReceiveNRN }
        ::= id-pt-reception
```

Nota 1 – Por haberse definido abstractamente, el SMIP no proporciona el almacenamiento de los mensajes recibidos, pues el hecho de que lo proporcione, o de que no lo proporcione, para un determinado usuario no influye en forma alguna en la capacidad del usuario para comunicar con otros usuarios. En consecuencia el suministro de almacenamiento es un asunto local.

Nota 2 – Por estas consideraciones, la operación abstracta *recepción MIP*, por ejemplo, expele un MIP del SMIP porque su finalidad es aclarar el significado del paso de transferencia de recepción. En cambio, las capacidades de un usuario al que se proporciona el almacenamiento de los mensajes recibidos podría incluir una instrucción «visualización MIP» que permitiera al usuario visualizar el MIP entregado (y quizás ya recibido) cuyo identificador de MIP él especifica, y que le permita proceder de esta manera todas las veces que desee, introduciendo repetidamente la instrucción. La primera, pero no las ulteriores utilizaciones de la instrucción para visualizar un determinado MIP, representa la realización concreta de la operación abstracta de recepción MIP en tal realización.

12.2.1 *Recepción informe*

La operación abstracta **recepción informe** recibe un informe.

```
ReceiveReport ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope                [0] ReportDeliveryEnvelope,
            undelivered-object      [1] InformationObject OPTIONAL}
        RESULT
        ERRORS {}
```

El informe recibido puede estar relacionado con uno de los siguientes puntos originado previamente por los destinatarios del informe:

a) Una sonda referente a un mensaje cuyo contenido era un MIP, que fue originado con la operación abstracta generación sonda.

b) Un mensaje cuyo contenido era una NNR, que fue originado como resultado de un descarte automático o una retransmisión automática.

c) Un mensaje cuyo contenido era una NR, que fue originado con la operación abstracta generación NR o por *acuse de recibo automático.*

d) Un mensaje cuyo contenido era un MIP, que fue originado con la operación abstracta generación MIP o por *retransmisión automática.*

Esta operación abstracta tiene los siguientes argumentos:

1) **Sobre** (O): Sobre de entrega de informe, cuya composición está definida por el servicio abstracto STRM.

2) **Objeto no entregado** (C): Contenido del mensaje sobre cuyo estado se está informando. Es un MIP o una NIP.

   Si el informe fue provocado por una invocación anterior de la operación abstracta generación sonda, este argumento condicional estará ausente. Si el informe fue provocado por una invocación anterior de la operación abstracta generación MIP, el argumento estará presente si y sólo si se solicitó devolución del contenido. En otro caso (es decir, si el informe fue provocado por una NIP) el argumento estará ausente.

Esta operación abstracta no tiene resultados.

12.2.2 *Recepción MIP*

La operación abstracta **recepción MIP** recibe un mensaje cuyo contenido es un MIP.

```
ReceiveIPM ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] MessageDeliveryEnvelope,
            content   [1] IPM}
        RESULT
        ERRORS {}
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre de entrega del mensaje.

b) **Contenido** (O): MIP que es el contenido del mensaje.

Esta operación abstracta no tiene resultados.

12.2.3 *Recepción NR*

La operación abstracta **recepción NR** recibe un mensaje cuyo contenido es una NR. La NR es provocada por un MIP generado con la operación abstracta generación MIP.

```
ReceiveRN ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] MessageDeliveryEnvelope,
            content   [1] RN}
        RESULT
        ERRORS {}
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre de entrega del mensaje.

b) **Contenido** (O): NR que es el contenido del mensaje.

Esta operación abstracta no tiene resultados.

12.2.4 *Recepción NNR*

La operación abstracta **recepción NNR** recibe un mensaje cuyo contenido es una NNR. La NNR es provocada por un MIP originado con la operación abstracta generación MIP.

```
ReceiveNRN ::= ABSTRACT-OPERATION
        ARGUMENT SET{
            envelope  [0] MessageDeliveryEnvelope,
            content   [1] NNR }
        RESULT
        ERRORS {}
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Sobre** (O): Sobre de entrega del mensaje.

b) **Contenido** (O): NNR que es el contenido del mensaje.

Esta operación abstracta no tiene resultados.

12.3 *Operaciones abstractas de gestión*

Las operaciones abstractas disponibles en un puerto de gestión son invocadas por el usuario y ejecutadas por el SMIP.

```
management PORT
        CONSUMER INVOKES {
            ChangeAutoDiscard,
            ChangeAutoAcknowledgment,
            ChangeAutoForwarding }
        ::= id-pt-management
```

12.3.1 *Cambio descarte automático*

La operación abstracta **cambio descarte automático** activa o desactiva el **descarte automático**, es decir, el descarte automático por el SMIP de MIP expirados u obsoletos, entregados al usuario, pero aún no recibidos por éste.

```
ChangeAutoDiscard; ::= ABSTRACT-OPERATION
        ARGUMENT SET {
            auto-discard-expired-IPMs      [0] BOOLEAN,
            auto-discard-obsolete-IPMs     [1] BOOLEAN }
        RESULT
        ERRORS {}
```

Cuando el SMIP descarta automáticamente un MIP, origina una NNR a nombre del usuario únicamente si se había solicitado del mismo una de estas notificaciones por medio del componente peticiones de notificación del especificador de destinatario asunto.

Esta operación abstracta tiene los siguientes argumentos:

a) **Descarte automático de MIP expirados** (O): Independientemente de que los MIP expirados deban ser o no descartados automáticamente. Es un booleano.

b) **Descarte automático de MIP obsoletos** (O): Independientemente de que los MIP obsoletos sean o no descartados automáticamete. Es un booleano.

Esta operación abstracta no tiene resultados.

12.3.2 *Cambio acuse de recibo automático*

La operación abstracta **cambio acuse de recibo automático** activa o desactiva **acuse de recibo automático**, la generación automática de NR por el SMIP en nombre del usuario. Esta generación se produce al entregarse los MIP que solicitan NR del usuario por medio de los componentes peticiones de notificación de sus especificadores de destinatario asunto.

```
ChangeAutoAcknowledgment ::= ABSTRACT-OPERATION
        ARGUMENT SET {
            auto-acknowledge-IPMs                [0] BOOLEAN,
            auto-acknowledge-suppl-receipt-info  [1]
            SupplementaryInformation OPTIONAL }
RESULT
ERRORS {
        SubscriptionError }
```

Esta operación abstracta tiene los siguientes argumentos:

a) **Acuse de recibo automático de MIP** (O): Independientemente de que acuse o no recibo automáticamente de los MIP. Es un booleano.

b) **Información de recepción suplementaria de acuse de recibo automático** (C): Campo de información de recepción suplementaria de cada NR provocada por un acuse de recibo automático.

   Este argumento condicional estará presente únicamente si el argumento de los MIP con acuse de recibo automático tiene el valor *verdadero.*

Esta operación abstracta no tiene resultados.

12.3.3 *Cambio retransmisión automática*

La operación abstracta **cambio retransmisión automática** activa o desactiva la **retransmisión automática**, retransmisión automática de MIP por el SMIP a usuarios o LD especificadas previamente. Esta retransmisión se produce al entregarse los MIP.

```
ChangeAutoForwarding ::= ABSTRACT-OPERATION
        ARGUMENT SET {
            auto-forward-IPMs          [0] BOOLEAN,
            auto-forward-recipients    [1] SEQUENCE OF ORName OPTIONAL,
            auto-forward-heading       [2] Heading OPTIONAL,
            auto-forward-comment       [3] AutoForwardComment OPTIONAL }
RESULT
ERRORS {
        SubscriptionError,
        RecipientImproperlySpecified }
```

El cuerpo de cada MIP, originado por el SMIP como resultado de una retransmisión automática comprende una sola parte de cuerpo de tipo mensaje. El contenido del mensaje representado por la parte de cuerpo es el MIP retransmitido.

Cuando el SMIP retransmite automáticamente un MIP, origina una NNR en nombre del usuario si y sólo si se había solicitado de él tal notificación por medio del componente peticiones de notificación del especificador del destinatario asunto.

Esta operación abstracta tiene los siguientes argumentos:

a) **MIPs de retransmisión automático** (O): Independientemente o no de que los MIP deban ser reenviados automáticamente. Es un booleano.

b) **Destinatarios de retransmisión automática** (C): Los usuarios o LD a los cuales deben retransmitirse los MIP. Es una secuencia de nombres O/D.

   Este argumento condicional estará presente únicamente si el argumento de los MIP de retransmisión automática tiene el valor *verdadero.*

c) **Encabezamiento de retransmisión automática** (C): Encabezamiento que ha de utilizarse para cada retransmisión de MIP. El campo de encabezamiento retransmitido automáticamente deberá tener el valor *verdadero.*

   Este argumento condicional estará presente únicamente si el argumento MIP de retransmisión automática tiene el valor *verdadero.*

d) **Comentario de retransmisión automática** (C): Valor que ha de suministrarse como el campo de no recepción comentario de retransmisión automática de cada NNR transportada al originador de un MIP retransmitido automáticamente.

   Este argumento condicional estará presente únicamente si el argumento de los MIP retransmisión automática tiene el argumento *verdadero.*

Esta operación abstracta no tiene resultados.

Nota – Esta operación abstracta está prevista para definir la esencia de la retransmisión automática, y no para impedir que se ofrezcan capacidades de retransmisión automática más sofisticadas; por ejemplo, como las de un AM.

13 Errores abstractos

Los errores abstractos que pueden ser informados en respuesta a la invocación de las operaciones abstractas disponibles en los puertos de generación, recepción y gestión se definen y describen a continuación o como parte de la definición del servicio abstracto STRM.

Nota – El conjunto de errores abstractos representados más adelante tiene una finalidad ilustrativa, y no es exhaustivo.

13.1 *Error de abono*

El error abstracto **error de abono** notifica que el usuario no está abonado a uno o más de los elementos de servicio implícitos en su invocación de la operación abstracta cuya ejecución ha sido abortada.

```
SubscriptionError ::= ABSTRACT-ERROR
        PARAMETER SET {
            problem  [0] SubscriptionProblem }
```

Este error abstracto tiene los siguientes parámetros:

a) **Problema** (O): Problema referente al abono, con el cual se ha tropezado.

```
SubscriptionProblem ::= ENUMERATED {
        ipms-eos-not-subscribed(0),
        mts-eos-not-subscribed (1) }
```

Este parámetro puede adoptar uno de los siguientes valores:

i) *eds-SMIP-no-abonado* : Elemento de servicio SMIP no abonado.

ii) *eds-STRM-no-abonado* : Elemento de servicio STRM no abonado.

13.2 *Destinatario especificado indebidamente*

El error abstracto **destinatario indebidamente especificado** notifica que no son válidos uno o más de los nombres O/D suministrados como argumentos o como componentes de los argumentos de la operación abstracta cuya ejecución ha sido abortada.

Este error abstracto está definido por el servicio abstracto STRM.

14 Otras capacidades

Además de las capacidades comprendidas en el servicio abstracto SMIP, definidas anteriormente, el SMIP extenderá transparentemente a cada usuario las capacidades del AM y del STRM identificadas más adelante. (La enumeración de estas capacidades anticipan necesariamente el hecho, indicado en el § 16, de que los AM y el STRM se encuentran entre las partes componentes de los SMIP.)

Se proporcionarán las siguientes capacidades adicionales:

a) *Depósito* : Capacidades del puerto de depósito de los AM o de los STRM no incluidos en el servicio abstracto SMIP, por ejemplo, la posibilidad de anular la entrega de un mensaje generado anteriormente cuyo contenido es un MIP (pero no una NR), si se seleccionó entrega diferida.

b) *Entrega* : Capacidades del cuerpo de entrega de los STRM no comprendidas en el servicio abstracto SMIP, por ejemplo, la posibilidad de controlar temporalmente las clases de objetos de información que el STRM transporta al AU del usuario.

c) *Administración* : Capacidades del puerto de administración de los AM o los STRM.

d) *Extracción* : Capacidades del puerto de extracción de los AM.

Además de lo anteriormente expresado y como asunto local, los SMIP pueden proporcionar a los usuarios capacidades adicionales que no están definidas o no están limitadas por esta Recomendación. Entre estas capacidades están las de la guía.

Nota – Las capacidades requeridas a que se refiere este punto están excluidas de la definición formal del servicio abstracto SMIP por razones puramente pragmáticas, en particular, porque su inclusión reproducía en gran parte, e innecesariamente, las definiciones de las operaciones abstractas AM y STRM sobre las cuales se basan dichas capacidades.

SECCIÓN 4 – PROVISIÓN DEL SERVICIO ABSTRACTO

15 Visión de conjunto

Esta sección especifica cómo el SMIP proporciona el servicio abstracto SMIP a los usuarios.

Esta sección trata los siguientes temas:

a) Tipos de objetos secundarios.

b) Tipos de puertos secundarios.

c) Operación de agente de usuario.

d) Operaciones de almacenamiento de mensajes.

e) Contenido de mensajes.

f) Realización de puertos.

g) Conformidad.

16 Tipos de objetos secundarios

El SMIP puede describirse mediante un modelo que comprende objetos menores que interactúan entre sí por medio de puertos (adicionales).

```
ipms-refinement REFINE ipms AS
        mTS
            submission      [S]  PAIRED WITH ipms-ua, ipms-ms
            delivery        [S]  PAIRED WITH ipms-ua, ipms-ms
            administration  [S]  PAIRED WITH ipms-ua, ipms-ms
        ipms-ua RECURRING
            origination     [S]  VISIBLE
            reception       [S]  VISIBLE
            management      [S]  VISIBLE
        ipms-ms RECURRING
            submission      [S]  PAIRED WITH ipms-ua
            retrieval       [S]  PAIRED WITH ipms-ua
            administration  [S]  PAIRED WITH ipms-ua
        tlma RECURRING
            origination     [S]  VISIBLE
            reception       [S]  VISIBLE
            management      [S]  VISIBLE
        tlxau RECURRING
            origination     [S]  VISIBLE
            reception       [S]  VISIBLE
            management      [S]  VISIBLE
        pdau RECURRING
            reception       [S]  VISIBLE
        ::= id-ref-secondary
```

Estos objetos menores se denominan **objetos secundarios** de la mensajería interpersonal. Comprenden un objeto central único, el STRM, y numerosos objetos periféricos: *agentes de usuario del sistema de mensajería interpersonal (AU SMIP), dispositivos de almacenamiento de mensajes del sistema de mensajería interpersonal (AM SMIP), agentes telemáticos (ATLM), unidades de acceso télex (UATLX),* y unidades de acceso a entrega física (UAEF).

La estructura del SMIP se describe en la figura 4/X.420. Como se indica en dicha figura, los *AU SMIP, ATLM, UATLX* y *UAEF* son instrumentos por medio de los cuales el SMIP proporciona el servicio abstracto a los usuarios.

A continuación se definen y describen los tipos de objeto secundario. Los tipos de puertos por medio de los cuales interactúan dichos tipos de objetos se examinan en el § 17.

Nota 1 – La presentación anterior comprende todas las posibles interconexiones entre todos los objetos posibles. Ignora la posible ausencia de objetos de un tipo determinado (por ejemplo, UAEF) y configuraciones lógicas específicas del *AM SMIP.* Estas últimas se identifican en la Recomendación X.402.

Nota 2 – La Recomendación T.330 extiende de hecho el servicio abstracto de mensajería interpersonal mediante su definición de un puerto *misceláneo,* que no se muestra en la figura. Véase la nota en el § 16.3.

Nota 3 – El STRM abastece a los puertos de importación y exportación. Sin embargo, como esos puertos no están definidos formalmente (en la Recomendación X.411), no se incluyen en la presentación formal anterior.

16.1 *Agente de usuario del sistema de mensajería interpersonal*

Un **agente de usuario del sistema de mensajería interpersonal (AU SMIP)** es un AU diseñado para facilitar la utilización, por un solo usuario, de la mensajería interpersonal. Lo ayuda a generar, recibir, o a generar y recibir mensajes que contienen objetos de información de los tipos definidos en la sección dos.

```
ipms-ua OBJECT
        PORTS {
            origination     [S],
            reception       [S],
            management      [S],
            submission      [C],
            delivery        [C],
            retrieval       [C],
            administration  [C] }
        ::= id-ot-ipms-ua
```

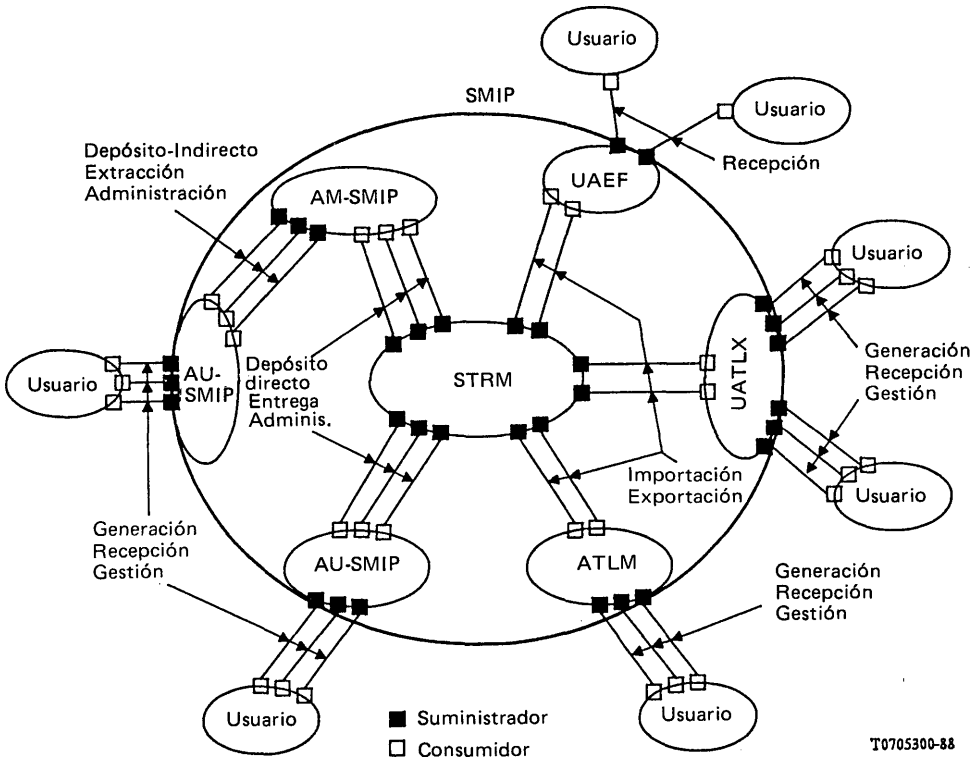


FIGURA 4/X.420

Sistema de mensajería interpersonal

El SMIP comprende un número cualquiera de AU SMIP.

Nota – Por razones de brevedad, en el resto de esta Recomendación se usa el término «AU» con el significado de «AU SMIP».

16.2 *Dispositivo de almacenamiento de mensajes del sistema de mensajería interpersonal*

Un **dispositivo de almacenamiento de mensajes del sistema de mensajería interpersonal (AM SMIP)** es un AM diseñado para facilitar la utilización por un solo usuario, de la mensajería interpersonal. Le ayuda a depositar, aceptar la entrega, o a depositar y aceptar la entrega de mensajes que contienen objetos de información de los tipos definidos en la sección dos.

```
ipms-ms OBJECT
        PORTS {
            submission      [S],
            retrieval       [S],
            administration  [S],
            submission      [C],
            delivery        [C],
            administration  [C] }
        ::= id-ot-ipms-ms
```

El SMIP comprende cualquier número de AM SMIP.

Nota – Por razones de brevedad, en el resto de esta Recomendación se utiliza el término «AM» con el significado de «AM SMIP».

16.3 *Agente telemático*

Un **agente telemático (ATLM)** es un UA que ayuda a un solo usuario indirecto a emplear la mensajería interpersonal a partir de un terminal telemático, junto con ese terminal y a la red que los une. Un ATLM ayuda al usuario a generar, recibir, o a generar y recibir mensajes que contienen objetos de información de los tipos definidos en la sección dos.

```
tlma OBJECT
        PORTS {
            origination     [S],
            reception       [S],
            management      [S],
            miscellanea     [S] }
        ::= id-ot-tlma
```

El SMIP comprende cualquier número de ATLM.

Nota 1 – Un ATLM consume puertos importación y exportación. Sin embargo, como dichos puertos no están definidos formalmente (en la Recomendación X.411), no se incluyen en la definición de ATLM mencionada anteriormente.

Nota 2 – En la Recomendación T.330 se define un puerto *misceláneo* del ATLM. Este no forma parte del servicio abstracto SMIP en su forma más general, que es el asunto de esta Recomendación. En lugar de esto, comprende capacidades disponibles solamente para un usuario ATLM. Por esta razón, no se considera ulteriormente en esta Recomendación y no se incluye en el perfeccionamiento formal del SMIP que figura en el § 16.

16.4 *Unidad de acceso télex*

Una **unidad de acceso télex (UATLX)** es una UA que ayuda a cualquier número de usuarios indirectos a utilizar la mensajería interpersonal a partir de terminales télex. Les ayuda a generar, recibir o a generar y recibir mensajes que contienen objetos de información de los tipos definidos en la sección dos.

```
tlxau OBJECT
        PORTS {
            origination     [S],
            reception       [S],
            management      [S] }
        ::= id-ot-tlxau
```

El SMIP comprende cualquier número de UATLX.

Nota – Una UATLX consume puertos de importación y exportación. Sin embargo, como dichos puertos no están definidos formalmente (en la Recomendación X.411), no se incluyen en la definición formal de UATLX mencionada anteriormente.

16.5 *Unidad de acceso a entrega física*

En el presente contexto, una unidad de acceso a entrega física (UAEF) ayuda a cualquier número de usuarios indirectos a utilizar la mensajería interpersonal por medio de un servicio de entrega física (SEF). Les ayuda a recibir (pero no a generar) mensajes que contienen objetos de información de los tipos definidos en la sección dos.

```
pdau OBJECT
        PORTS {
            reception       [S] }
        ::= id-ot-pdau
```

El SMIP comprende cualquier número de UAEF.

Nota – Una UAEF consume puertos de importación y exportación. Sin embargo, como dichos puertos no están definidos formalmente (en la Recomendación X.411), no se incluyen en la definición formal de UAEF mencionada anteriormente.

16.6 *Sistema de transferencia de mensajes*

En el presente contexto, el sistema de transferencia de mensajes (STRM) transporta objetos de información de los tipos definidos en la sección dos entre AU, AM, ATLM y UA.

El SMIP comprende un solo STRM.

17 Tipos de puertos secundarios

Los objetos secundarios de la mensajería interpersonal están unidos e interactúan entre si por medio de puertos. Estos puertos, que son proporcionados por los AM y STRM, se denominan **puertos secundarios** de mensajería interpersonal. Son de los tipos identificados más adelante.

Las capacidades incorporadas en un puerto de depósito, un puerto de extracción, y un puerto de administración constituyen el servicio abstracto AM. Estas capacidades se definen en la Recomendación X.413.

Las capacidades incorporadas en un puerto de depósito, un puerto de entrega y un puerto de administración constituyen el servicio abstracto STRM. Se definen en la Recomendación X.411.

Nota – Por medio de la operación abstracta de vinculación que vigila sus puertos, un AM o el STRM autentican típicamente otro objeto secundario antes de ofrecer sus servicios abstractos a ese objeto.

17.1 *Depósito*

En el presente contexto, un puerto de depósito es el medio por el cual un AU (directa o indirectamente) o un AS (directamente) deposita sondas relativas a, o mensajes que contienen, objetos de información de los tipos definidos en la sección dos.

Un AM proporciona un puerto de depósito a su AU.

El STRM proporciona un puerto de depósito a cada AU configurado sin un AM y a cada AM.

17.2 *Entrega*

En el presente contexto, un puerto de entrega es el medio por el cual un AU o AM acepta la entrega de informes relativos a, y mensajes que contienen, objetos de información de los tipos definidos en la sección dos.

El STRM proporciona un puerto de entrega cada AU configurado sin un AM, y a cada AM.

17.3 *Extracción*

En el presente contexto, un puerto de *extracción* es el medio por el cual un AU extrae informes relativos a, y mensajes que contienen, objetos de información de los tipos definidos en la sección dos.

Un AM proporciona un puerto de extracción a su AU.

17.4 *Administración*

En el presente contexto, un puerto de administración es el medio por el cual un AU cambia información sobre el mismo o su usuario en un fichero con el AM, o un AU, o un AM cambia tal información en un fichero con el STRM.

Un AM proporciona un puerto de administración a su AU.

El STRM proporciona un puerto de administración a cada AU configurado sin un AM y a cada AM.

17.5 *Importación*

En el presente contexto, un puerto de importación es el medio por el cual el STRM importa informes relativos a mensajes que contienen objetos de información de los tipos definidos en la sección dos.

El STRM proporciona un cuerpo de importación a cada UA (o ATLM).

17.6 *Exportación*

En el presente contexto, un puerto de exportación es el medio por el cual el STRM exporta sondas relativas a, y mensajes que contienen, objetos de información de los tipos definidos en la sección dos.

El STRM proporciona un puerto de exportación a cada UA (o ATLM).

18 Operación de agente de usuario

Un AU tiene que emplear el STRM de una manera particular con el fin de proporcionar (correctamente) el servicio abstracto de SMIP a su usuario. Si el usuario está equipado con un AM, este último contribuye a la prestación del servicio abstracto y, por tanto, está sujeto a las mismas reglas.

Son objeto de éste punto las reglas que gobiernan la operación de un AU (y un AM). La operación de un ATLM o un AU está fuera del ámbito de esta Recomendación.

Nota 1 – Se debe a razones históricas el que la Recomendación que define el servicio abstracto de SMIP especifique también la forma en que un AU (y un AM), pero no un ATLM o UA, lo proporciona.

Nota 2 – La finalidad de este punto no es imponer ni limitar innecesariamente la realización de un AU real, sino aclarar el significado y el efecto deseado del servicio abstracto SMIP.

18.1 *Variables de estado*

La operación de un AU se describe a continuación con ayuda de *variables de estado.* Una **variable de estado** es un elemento de información cuyo valor registra los resultados de las interacciones pasadas del AU con su usuario e influye en las interacciones futuras. Las variables de estado son comunes, es decir, están compartidas por los puertos de originación, recepción y gestión del AU.

El AU mantiene cada variable de estado continuamente, es decir, a través del abono del usuario al SMIP. A cada variable de estado booleana se le asigna el valor *falso* cuando comienza el abono. Los valores iniciales de otras variables de estado no tienen importancia y por eso no se especifican.

El AU cambia sus variables de estado cuando efectúa o invoca operaciones abstractas. El AU consulta esas variables para determinar cómo ha de efectuar operaciones abstractas, la forma de hacerlo y si deben invocarse y cómo dichas operaciones. Sus valores (si existen) tienen importancia para la vinculación y desvinculación de puertos.

Nota – Las variables de estado son dispositivos didácticos que no tienen por finalidad limitar innecesariamente la realización de un AU real. En particular, un AU no necesita mantener estructuras de datos al tiempo de la ejecución que corresponden a variables de estado si el comportamiento requerido del mismo puede asegurarse de otra manera.

18.2 *Ejecución de operaciones de generación*

Un AU deberá ejecutar las operaciones abstractas, que pone a disposición en su puerto de generación, como se indica a continuación. Al efectuar estas operaciones particulares, el AU no modifica ninguna de sus variables de estado.

En la ejecución de estas operaciones, el AU invoca las siguientes operaciones abstractas del servicio abstracto STRM (que, en el resto de este punto, se indicarán de una manera no calificada con respecto a su fuente):

a) depósito de sonda,

b) depósito de mensaje.

Nota – En respuesta a la invocación de estas operaciones abstractas, un AU notificará los errores abstractos según proceda. La especificación de las circunstancias precisas en las cuales deberá notificarse cada error abstracto está fuera del ámbito de esta Recomendación.

18.2.1 *Generación sonda*

Un AU ejecutará la operación abstracta generación sonda invocando depósito de sonda con los argumentos indicados más adelante y devolviendo a su usuario los resultados que también se indican más adelante.

Los argumentos de depósito sonda serán los siguientes:

a) *Sobre:* Los componentes de este argumento que constituyen los campos para cada sonda serán los siguientes; los que no se mencionen explícitamente más abajo serán como los especificados por el argumento sobre de generación sonda:

   i) *Nombre-de-originador:* Nombre O/D del usuario del AU.

   ii) *Tipo-de-contenido, longitud-de-contenido y tipos-de-información-codificada-original:* Determinados a partir del argumento contenido de generación sonda, especificado en los § 20.2 a 20.4.

   iii) *Identificador-de-contenido:* Su especificación u omisión es un asunto local.

   Los componentes de este argumento que constituyen campos para cada destinatario serán los especificados por el argumento de sobre de generación sonda.

Los resultados de generación sonda serán los siguientes:

1) *Identificador-de-depósito:* Resultado del identificador de depósito de sonda del depósito de sonda.

2) *Hora-de-depósito:* Resultado de la hora de depósito de sonda del depósito de sonda.

Nota 1 – El AU ignorará todas las propiedades del argumento contenido de generación sonda que no sean las mencionadas anteriormente.

Nota 2 – La manera en que el AU emplea el resultado de identificador de contenido del depósito de sonda es un asunto local.

18.2.2 *Generación MIP*

Un AU efectuará la operación abstracta generación MIP invocando depósito de mensaje con los argumentos indicados más adelante, y devolviendo a su usuario los resultados que también se indican más adelante.

Los argumentos de depósito de mensaje serán los siguientes:

a) *Sobre:* Los componentes de este argumento que constituyen campos para cada mensaje serán los siguientes; los que no se mencionan explícitamente se especificarán por el argumento del sobre de generación MIP:

   i) *Nombre-de-originador:* Nombre O/D del usuario del AU.

   ii) *Tipo-de-contenido y tipos-de-información-codificada-original:* Determinados a partir del argumento de contenido de generación MIP como se especifica en los § 20.2 y 20.4, respectivamente.

   iii) *Identificador-contenido:* Su especificación u omisión es un asunto local.

   Los componentes de este argumento que constituyen campos para cada destinatario serán los especificados por el argumento del sobre de generación MIP.

b) *Contenido:* Determinado a partir del argumento del contenido de generación MIP (identificado como un MIP), como se especifica en el § 20.1.

Si el campo de encabezamiento de los destinatarios de copia ciega del MIP identifica uno o más usuarios y LD, el AU invocará el depósito de mensaje repetidas veces, variando en cada ocasión el campo de encabezamiento para ajustarse a los requisitos de ocultación de información del § 7.2.6.

Los resultados de MIP serán los siguientes:

1) *Identificador-de-depósito:* Resultado del identificador de depósito de mensaje del depósito de mensaje.

2) *Hora-de-depósito:* Resultado de la hora de depósito de mensaje del depósito de mensaje.

Nota 1 – La forma en que el AU emplea el resultado del identificador de contenido del depósito de mensaje es un asunto local.

Nota 2 – La inclusión del resultado de ampliaciones del depósito de mensaje entre los resultados de generación MIP es un asunto de orden propio y queda para ulterior estudio.

18.2.3 *Generación NR*

Un AU realizará la operación abstracta generación NR invocando un depósito de mensaje con los argumentos indicados más adelante, y devolviendo a su usuario los resultados que también se indican más adelante.

Los argumentos de depósito de mensaje serán los siguientes:

a) *Sobre:* Los componentes de este argumento, que constituyen campos para cada mensaje, serán los siguientes; los que no se mencionan explícitamente más adelante serán especificados por el argumento del sobre de generación NR:

   i) *Nombre-del-originador:* Nombre O/D del usuario del AU.

   ii) *Tipo-de-contenido y tipos-de-información-codificada-original:* Determinados a partir de la NR como se especifica en los § 20.2 y 20.4, respectivamente.

   iii) *Identificador-de-contenido:* Su especificación u omisión es un asunto local.

   iv) *Hora-de-entrega-diferida:* Omitida.

   Los componentes de este argumento que constituyen campos para cada destinatario serán especificados por el argumento del sobre de generación NR.

b) *Contenido:* Determinado a partir del argumento del contenido de generación NR (identificado como una NR) como se especifica en el § 20.1.

Los resultados de generación NR serán los siguientes:

1) *Identificador-de-depósito:* Resultado del identificador-de-depósito-de-mensaje del depósito de mensaje.

2) *Hora-de-depósito:* Resultado de la hora-de-depósito-de-mensaje del depósito de mensaje.

Nota 1 – La manera en que el AU emplea el resultado del identificador de contenido del depósito de mensaje es un asunto local.

Nota 2 – La inclusión del resultado de ampliaciones del depósito de mensaje entre los resultados de generación NR es un asunto de índole propia y queda para ulterior estudio.

18.3 *Ejecución de operaciones de gestión*

Un AU ejecutará las operaciones abstractas que pone a disposición en su puerto de gestión, como se especifica más adelante. El AU modifica una o más de sus variables de estado (véase más abajo) al efectuar cada operación.

Nota – En respuesta a la invocación de estas operaciones abstractas, un AU notifica errores abstractos según proceda. La especificación de las circunstancias precisas en las cuales debe informarse cada error abstracto está fuera del ámbito de esta Recomendación.

18.3.1 *Cambio descarte automático*

Para ayudar a proporcionar esta operación abstracta, un AU mantiene las siguientes variables de estado.

a) **Descarte-automático-de-MIP-expirados**: Es un booleano que indica si el descarte automático está o no vigente para los MIP expirados.

b) **Descarte-automático-de-MIP-obsoletos**: Es un booleano que indica si el descarte automático está o no vigente para los MIP obsoletos.

Un AU ejecutará la operación abstracta cambio descarte automático registrando los valores de los argumentos de descarte automático de MIP expirados y descarte automático de MIP obsoletos en las variables de estado denominadas correspondientemente.

18.3.2 *Cambio acuse de recibo automático*

Para ayudar a proporcionar esta operación abstracta, un AU mantiene las siguientes variables de estado:

a) **Acuse-de-recibo-automático-de-MIP**: Es un booleano que indica si el acuse de recibo automático está o no vigente.

b) **Información-recepción-suplementaria-de-acuse-recibo-automático**: Campo información recepción suplementaria de cada NR provocada por acuse de recibo automático.

Un AU ejecutará la operación abstracta Cambio acuse de recibo automático registrando el valor del argumento de acuse de recibo automático de MIP en la variable de estado denominada correspondientemente. Si ese valor es *verdadero*, registrará también el valor del argumento de acuse recibo automático de recepción de información suplementaria en la variable de estado denominada correspondientemente.

18.3.3 *Cambio de retransmisión automática*

Para ayudar a proporcionar esta operación abstracta, un AU mantiene las siguientes variables de estado:

a) **MIP-con-retransmisión-automática**: Es un booleano que indica si está o no vigente la retransmisión automática.

b) **Destinatarios-de-retransmisión-automática**: Secuencia de nombre O/D que identifican los usuarios y LD a los cuales se están reenviando MIP.

c) **Encabezamiento-de-retransmisión-automática**: Encabezamiento de cada MIP retransmisora provocado por la retransmisión automática. Su campo retransmitido automáticamente tiene el valor *verdadero*.

d) **Comentario-de-retransmisión-automática**: Campo de no recepción comentario de retransmisión automática de cada NNR transportada al originador de un MIP retransmitido automáticamente.

Un AU efectuará la operación abstracta cambio retransmisión automática registrando el valor del argumento de los MIP retransmitidos automáticamente en la variable de estado denominada correspondientemente. Si ese valor es *verdadero* registrará también los valores de los argumentos de destinatarios de retransmisión automática, encabezamiento de retransmisión automática, y comentarios de retransmisión automática, en las variables de estado denominadas correspondientemente.

18.4 *Invocación de operaciones de recepción*

Un AU invocará las operaciones abstractas disponibles en su puerto de recepción como se especifica más adelante. El AU no modifica ninguna de sus variables de estado en relación con la invocación de estas operaciones.

El AU invoca estas operaciones en respuesta a la invocaciòn STRM de las siguientes operaciones abstractas del servicio abstracto STRM (las cuales, durante el resto de este punto, no serán calificadas en lo que respecta a su fuente):

a) Entrega de informe.

b) Entrega de mensaje.

Nota – Las operaciones abstractas de un puerto de recepción no notifican errores.

18.4.1 *Recepción informe*

Cuando el STRM invoca entrega de informe en un puerto de entrega del AU, el AU invocará la operación abstracta recepción informe con los siguientes argumentos:

a) *Sobre*: Argumento del sobre de entrega de informe.

b) *Objeto-no-entregado*: Determinado a partir del argumento contenido devuelto de la entrega de informe, como se especifica en el § 20.1.

Nota – Toda forma de empleo, por el AU, del componente identificador de contenido del argumento de sobre de entrega de informe es un asunto local.

18.4.2 *Recepción MIP*

Cuando el STRM invoca entrega de mensaje en un puerto de entrega del AU, y su argumento de contenido codifica un MIP como se especifica en el § 20.1, el AU invocará la operación abstracta recepción MIP con los siguientes argumentos, a condición de que el mensaje no esté sujeto a retransmisión automática, ni a descarte automático (véase el § 18.5):

a) *Sobre*: Argumento del sobre de entrega de mensaje.

b) *Contenido*: Determinado a partir del argumento del contenido de entrega de mensaje como se especifica en el § 20.1 (pero ya no será marcado como un MIP).

18.4.3 *Recepción NR*

Cuando el STR invoca entrega de mensaje en un puerto de entrega del AU, y su argumento de contenido codifica una NR como se especifica en el § 20.1, el AU invocará la operación abstracta recepción NR con los siguientes argumentos:

a) *Sobre*: Argumento del sobre de entrega de mensaje.

b) *Contenido*: Determinado a partir del argumento del contenido de entrega de mensaje como se especifica en el § 20.1 (pero ya no será marcado como una NR).

18.4.4 *Recepción NNR*

Cuando el STRM invoca entrega de mensaje en un puerto de entrega del AU, y su argumento de contenido codifica una NNR como se especifica en el § 20.1, el AU invocará la operación abstracta recepción NNR con los siguientes argumentos:

a) *Sobre*: Argumento del sobre de entrega de mensaje.

b) *Contenido*: Determinado a partir del argumento del contenido de entrega de mensaje como se especifica en el § 20.1 (pero ya no será marcado como NNR).

18.5 *Procedimientos internos*

Un AU aplicará, como se indica más adelante, los procedimientos internos de descarte automático, acuse de recido automático, y reenvío automático para dejar concluidas las operaciones abstractas disponibles en su puerto de gestión.

Los procedimientos comprenden las siguientes operaciones abstractas del servicio abstracto STRM (las cuales, en el resto de este punto, no serán calificadas con respecto a su fuente):

a) Depósito de mensaje.

b) Entrega de mensaje.

Como se deduce de lo anteriormente expuesto, en el curso de los procedimientos, el AU tiene ocasión de invocar entrega de mensaje. Su actuación sobre los resultados de esta operación abstracta es un asunto local.

El AU considerará como candidato para cada procedimiento, individualmente, cada mensaje con relación al cual se cumplan las siguientes condiciones:

a) El STRM ha transportado el mensaje al AU invocando entrega de mensaje en el puerto de entrega del AU.

b) El AU no ha transportado el mensaje al usuario invocando recepción MIP en el puerto de recepción del usuario.

c) El mensaje contiene un MIP (y no una NIP).

Nota – Con relación al anterior apartado b), el mensaje podría ser detenido en el AU, por ejemplo, como caso típico, por motivo de indisponibilidad del usuario.

18.5.1 *Descarte automático*

El AU aplicará un descarte automático a cada mensaje candidato en base a que sus respectivos contenidos cumplan las siguientes condiciones:

a) La variable de estado descarte automático de MIP expirados tiene el valor *verdadero* y han pasado la fecha y hora señaladas por el campo hora de expiración del MIP.

b) La variable de estado descarte de MIP obsoletos tiene el valor *verdadero* y otro MIP candidato identifica el MIP candidato presente por medio de su campo de encabezamiento MIP obsoletos.

El AU descartará automáticamente cada mensaje como sigue.

18.5.1.1 *Descarte de MIP*

El AU descartará el MIP a fin de que nunca se transfiera al usuario.

18.5.1.2 *Construcción de NNR*

El AU construirá una NNR si y sólo si así se le solicita por medio del componente peticiones de notificación del especificador del destinatario asunto del MIP.

La NNR tendrá los campos comunes prescritos para el acuse de recibo automático (véase el § 18.5.2.1).

La NNR tendrá los siguientes campos de recepción:

a) *Motivo de no recepción:* Valor *mip descartado.*

b) *Motivo de descarte:* Valor *mip-expirado* o *mip-obsoleto,* el que sea aplicable. Si ninguno de los dos es aplicable, se puede especificar cualquiera de ellos.

c) *Comentario de reenvío automático:* Omitido.

d) *MIP devuelto:* Si se ha solicitado la devolución del MIP por medio del componente peticiones de notificación de su especificador de destinatario asunto, y está ausente el componente tipos de información codificada convertida del argumento del sobre de entrega de mensaje, el MIP. Omitido en otro caso.

18.5.1.3 *Depósito de NNR*

El AU depositará la NNR anteriormente mencionada (si existe) invocando depósito de mensaje. El argumento de su sobre será el prescrito para acuse automático de recibo (véase el § 18.5.2.2), el argumento de su contenido se determina a partir de la NNR como se especifica en el § 20.1.

18.5.2 *Acuse de recibo automático*

El AU aplicará un acuse de recibo automático a cada mensaje candidato atendiendo a que sus contenidos respectivos cumplan las siguientes condiciones:

a) La variable de estado acuse de recibo automático tiene el valor *verdadero* y el MIP solicita una NR del usuario del AU por medio del componente peticiones de notificación del especificador de destinatario asunto del MIP.

El AU acusará recibo automáticamente de cada uno de estos mensajes de acuerdo con lo siguiente.

18.5.2.1 *Construcción de NR*

El AU construirá una NR.

La NR tendrá los siguientes campos comunes:

a) *MIP sujeto:* El campo de encabezamiento Este MIP del MIP.

b) *Originador de NIP:* Especificado u omitido como asunto local (pero, desde luego, conforme al § 8.1.2).

c) *Destinatario preferido del MIP:* El componente destinatario del especificador de destinatario asunto del MIP, a menos que su componente nombre formal sea el nombre O/D del usuario del AU, en cuyo caso deberá omitirse este campo.

d) *Conversión de TIC:* Componente tipos de información codificada convertida del argumento del sobre de entrega de mensaje.

La NR tendrá los siguientes campos de recepción:

a) *Hora de recepción:* La fecha y hora en cuestión.

b) *Modo de acuse de recibo:* El valor *automático.*

c) *Información de recepción suplementaria:* La variable de estado información de recepción suplementaria de acuse de recibo automático.

18.5.2.2 *Depósito de NR*

El AU depositará la NR mencionada anteriormente invocando depósito de mensaje con los siguientes argumentos:

a) *Sobre:* Los componentes de este argumento serán los prescritos para la realización de la operación abstracta generación NR con las siguientes excepciones:

i) *Prioridad:* Como se especifica por el argumento del sobre de entrega de mensaje.

ii) *Indicadores para cada mensaje:* Asunto local, con la salvedad de que entre los valores especificados deberá estar *conversión prohibida.*

iii) *Campos para cada destinatario:* Un campo único cuyo componente nombre de destinatario formará parte del componente nombre de originador del argumento del sobre de entrega de mensaje. No se solicitarán informes.

b) *Contenido:* Determinado a partir de la NR como se especifica en el § 20.1.

18.5.3 *Retransmisión automática*

El AU aplicará una retransmisión automática a cada mensaje candidato, si la variable de estado retransmisión MIP tiene el valor *verdadero.*

El AU retransmitirá automáticamente tal mensaje de acuerdo con lo siguiente.

18.5.3.1 *Prevención de bucles*

El AU suprimirá la retransmisión automática si y sólo si el MIP que ha de retransmitirse contiene en sí mismo un MIP retransmisor que ha sido creado previamente por el AU. Se suprimirá la retransmisión automática con independencia de que el MIP retransmisor aparezca (directamente) en la parte de cuerpo mensaje del MIP que haya de retransmitirse, o (anidado) en una parte de cuerpo mensaje del MIP que aparece en tal parte de cuerpo.

El AU considerará que ha sido él mismo quien ha creado el MIP retransmisor antes mencionado (cuyo campo de encabezamiento retransmitido automáticamente tiene el valor *verdadero*) si y sólo si el componente nombre de originador del componente parámetros del MIP concuerda con el nombre O/D del usuario del AU.

Nota – La retransmisión automática de un MIP de la clase descrita anteriormente constituirá un «bucle» autorretransmisor.

18.5.3.2 *Construcción de MIP*

El AU construirá un MIP retransmisor cuyo encabezamiento es la variable de estado encabezamiento de retransmisión automática (teniendo su campo retransmitido automáticamente el valor *verdadero*) y cuyo cuerpo comprende una sola parte de cuerpo de tipo mensaje.

La parte de cuerpo mensaje tendrá los siguientes componentes:

a) *Parámetros:* Argumento del sobre de entrega de mensaje.

b) *Datos:* MIP a retransmitir.

18.5.3.3 *Depósito de MIP*

El AU depositará el MIP que ha construido en la forma mencionada anteriormente invocando depósito de mensaje con los siguientes argumentos:

a) *Sobre:* Los componentes de este argumento serán los siguientes:

i) *Nombre de originador:* Nombre O/D del usuario del AU.

ii) *Tipo de contenido y tipos de información codificada original*: Determinados a partir del MIP como se especifica en los § 20.2 y 20.4.

iii) *Identificador de contenido:* Especificado y omitido como asunto local.

iv) *Prioridad*: Como se especifica mediante el argumento del sobre de entrega de mensaje.

v) *Indicadores para cada mensaje y ampliaciones:* Asunto local.

vi) *Hora de entrega diferida:* Omitida.

vii) *Campos para cada destinatario:* Sus componentes nombre de destinatario serán los nombres O/D que constituyen la variable de estado destinatarios de reenvío. Sus otros componentes son un asunto local.

b) *Contenido:* Determinado a partir del MIP como se especifica en el § 20.1.

18.5.3.4 *Construcción de NNR*

El AU construirá una NNR si y sólo si se le solicita por medio del componente peticiones de notificación del especificador de destinatario asunto del MIP retransmitido.

La NNR tendrá los campos comunes prescritos para efectuar el acuse de recibo automático.

La NNR tendrá los siguientes campos de recepción:

a) *Motivo de no recepción:* Valor *mip retransmitido automáticamente.*

b) *Motivo de descarte:* Omitido.

c) *Comentario de retransmisión automática:* Variable de estado comentario de reenvío automático.

d) *MIP devuelto:* Si se solicita la devolución de MIP por medio del componente peticiones de notificación de su especificador de destinatario asunto, y el componente tipos de información codificada convertida del argumento del sobre de entrega de mensaje está ausente, el MIP. Omitido en otro caso.

18.5.3.5 *Depósito de NNR*

El AU depositará la NNR mencionada anteriormente (si la hubiere), invocando depósito de mensaje. El argumento del sobre de depósito de mensaje será el prescrito para acuse de recibo automático, determinándose el argumento de su contenido a partir de la NNR especificada en el § 20.1.

19 Operaciones de almacenamiento de mensajes

Un AM deberá efectuar ciertas funciones específicas a la mensajería interpersonal para ser calificado como un AM SMIP y distinguirse de esa manera de un AM genérico. Estas funciones se tratan en el presente punto.

19.1 *Creación de objetos de información*

Un AM SMIP satisfará las siguientes exigencias relacionadas con los objetos de información que él mantiene:

a) El AM mantendrá un objeto de información separado para cada MIP o NIP (o para cada mensaje que contenga un MIP o NIP) que se le entrega.

b) El AM mantendrá como un objeto de información separado no solamente cada MIP retransmisor (o cada mensaje que contenga un tal MIP) [de acuerdo con el apartado a)] sino también cada MIP retransmitido (o mensaje que contenga un tal MIP) (recurrentemente).

c) El AM asignará números secuenciales, teniendo en cuenta primeramente la profundidad, a los mensajes en la jerarquía formada por un MIP retransmisor y sus MIP retransmitidos.

Ejemplo – Si el MIP *A* contiene los MIP *B* y *C* entre sus partes de cuerpo, y si el MIP *B* contiene los MIP *D* y *E* entre sus partes de cuerpo, los números secuenciales se asignarán a los MIP en el orden siguiente: *A*, *B*, *D*, *E*, y *C*.

19.2 *Mantenimiento de atributos*

Un AM SMIP satisfará los siguientes requisitos relacionados con los atributos del AM:

a) Para cada MIP o NIP contenido por el AM, éste admitirá los atributos del anexo C tal como están allí especificados.

b) Para cada MIP contenido en el AM, éste dará los siguientes significados a los valores definidos del atributo estado del AM:

   i) *nuevo:* No se han transportado valores de atributo al AU.

   ii) *listado:* Se ha transportado al AU al menos un valor de atributo y no ha sido transportada al menos una parte de cuerpo.

   iii) *procesado:* Todas las partes de cuerpo han sido transportadas al AU.

c) Para cada NIP contenido en el AM, éste dará los siguientes significados a los valores definidos del atributo estado del AM:

   i) *nuevo:* No se han transportado atributos al AU.

   ii) *listado:* Se ha transportado al AU al menos un valor de atributo, y se ha transportado al menos un valor de atributo distinto de MIP devuelto.

   iii) *procesado:* Todos los atributos, con la posible excepción de MIP devuelto, han sido transportados al AU.

d) El atributo estado del AM reflejará la situación antes de la invocación de una operación abstracta que modifica su valor.

e) El atributo tipo de contenido de cada MIP o NIP (o de cada mensaje que lo contenga) que se entrega al AM tendrá el valor id-mct-p2-1984 o id-mct-p2-1988 (véase el anexo D), según proceda, lo que dependerá del tipo de contenido del mensaje entregado (véase el § 20.2).

19.3 *Notificación de no recepción*

El AM, cuando descarta un MIP mientras está realizando una operación abstracta supresión, del servicio abstracto AM, depositará una NNR si así se ha solicitado y el atributo estado del AM del MIP tiene el valor *listado.*

19.4 *Retransmisión automática*

Un AM SMIP realizará la acción de retransmisión automática (Recomendación X.413) como se especifica en el § 18.5.3. Utiliza el componente otros-parámetros del argumento de registro de retransmisión automática de la operación abstracta del servicio abstracto AM. El tipo de datos del componente otros-parámetros se define de la manera siguiente:

```
Forwarded Info ::= SET{
        auto-forwarding-comment [0] AutoForwardComment OPTIONAL,
        cover-note [1] IA5TextBodyPart OPTIONAL,
        this-ipm-prefix [2] PrintableString (SIZE
        (1..ub-ipm-identifier-suffix)) OPTIONAL}
```

Además, el AM cumplirá los siguientes requisitos:

a) Depositará una NNR, incluso si deja una copia del MIP retransmitido.

b) Tomará el campo comentario de reenvío de la NNR, si existe, extrayéndolo del componente otros-parámetros.

c) Tomará la nota-de cubierta, si existe, que deberá incluirse junto con el MIP retransmitido, extrayéndolo del componente otros-parámetros.

d) Prefijará el componente identificador relativo al usuario del campo este MIP del encabezamiento del MIP reenviante con este-prefijo-mip, si existe.

Nota – Un AM (SMIP) no efectúa descartes automáticos ni acuses de recibo automáticos, siendo las posibles excepciones un asunto local.

19.5 *Retransmisión manual*

Un AM SMIP soportará la retransmisión manual de un mensaje utilizando la ampliación de petición-retransmisión de la Recomendación X.413, como se especifica en el § 6.6. El usuario de AM SMIP puede someter un MIP, incluyendo encabezamiento y cuerpo, utilizando la operación de depósito de mensaje, e identificar un mensaje que ya está en el AM y ha de combinarse con un cuerpo de mensaje depositado, para su retransmisión al (o a los) destinatarios del mensaje, utilizando la ampliación de petición-retransmisión.

El cuerpo de mensaje depositado y el mensaje retransmitido se combinan insertando el mensaje retransmitido, como una parte de cuerpo de mensaje en el cuerpo de mensaje depositado.

20 Contenido de mensajes

Como ya se ha visto, diversos objetos secundarios (por ejemplo, AU) tienen ocasión de transportar los objetos de información descritos en la sección dos como contenidos de mensajes, y también de transportar sondas relativas a tales mensajes. Este punto especifica de manera precisa cómo deben hacerlo.

Las reglas que gobiernan la transmisión de esos mensajes y sondas, así como la semántica y la sintaxis abstracta y de transferencia de su contenido, se denominan **protocolo de mensajería interpersonal (P2).**

Nota – El nombre, «P2», refleja el hecho histórico de que éste fue el segundo protocolo de tratamiento de mensajes que se desarrolló.

20.1 *Contenido*

Un objeto secundario que deposita un mensaje que contiene un MIP o una NIP suministrará como los octetos de la cadena de octetos que constituye el contenido del mensaje, el resultado de codificar objeto de información (InformationObject) de la sección dos de acuerdo con las reglas básicas de codificación de la Recomendación X.209.

20.2 *Tipo de contenido*

Un objeto secundario que deposita un mensaje que contiene un MIP o una NIP seleccionará su tipo de contenido de la manera siguiente.

Si el MIP o la NIP cumple todas las limitaciones, se especificará el entero 2:

i) El encabezamiento (de un MIP) está desprovisto del campo ampliaciones.

ii) El cuerpo (de un MIP) está desprovisto de partes de cuerpo definido externamente.

iii) El elemento parámetros de toda parte de cuerpo videotex: ... (de un MIP) está desprovisto de miembro de sintaxis.

iv) Cada componente del MIP o de la NIP que es un valor de un tipo de datos definido como parte del servicio abstracto STRM cumple las limitaciones de la Recomendación X.411 (1984).

Los tipos en cuestión son los listados en la cláusula IMPORTS del módulo NSA.1 definido en el anexo E. Las restricciones en cuestión se detallan en un anexo de la Recomendación X.419.

v) El elemento datos de toda parte de cuerpo mensaje (de un MIP) cumple estas mismas limitaciones (en forma recurrente).

En otro caso, se especificará el entero 22.

Nota 1 – El protocolo de contenido de mensaje designado (aquí) por el entero 2 es idéntico al especificado por la Recomendación X.420 (1984) (aclarada por la versión 6 de la Recomendación *Guía del realizador de las Recomendaciones de la serie X.400*), con excepción del tipo de parte de cuerpo documento formatizable simple, definido en esta última, que se ha omitido en la primera.

Nota 2 – Se aconseja el uso del entero 2, mencionado anteriormente, con preferencia al entero 22, para facilitar el interfuncionamiento entre sistemas conformes a esta Recomendación y sistemas conformes (solamente) a la Recomendación X.420 (1984).

El STRM no hace conversiones entre protocolos de contenido de mensaje. Por tanto, no hace conversiones entre el P2 definido en esta Recomendación solamente (y señalado por el entero 22) y el P2 definido por esta Recomendación y por la Recomendación X.420 (1984) (y señalado por el entero 2).

20.3 *Longitud de contenido*

Un objeto secundario que presenta una sonda relativa a un mensaje que contiene un MIP o una NIP especificará como longitud del contenido de mensaje el tamaño en octetos de la codificación del caso en cuestión del objeto de información (InformationObject) de la sección dos (elección de un MIP o una NIP) cuando se siguen las reglas básicas de codificación de la Recomendación X.209. Si esas reglas permiten varias codificaciones (por ejemplo, la primitiva y la construida) de ese objeto de información (InformationObject), la longitud de contenido puede reflejar cualquiera de las dos.

20.4 *Tipos de información codificada*

Un objeto secundario que deposita un mensaje que contiene un MIP o una NIP especificará los tipos de información codificada (TIC) y los parámetros no básicos (PNB) de los mensajes de la manera siguiente.

En el caso de una NIP, los TIC básicos serán *no especificado.*

En el caso de un MIP, los TIC básicos y los PNB se especificarán de acuerdo con las reglas siguientes:

a) *Partes de cuerpo múltiples:* Los TIC básicos (si existen) y los PNB (si existen) del mensaje comprenderán la unión lógica de los TIC básicos y los PNB de las partes de cuerpo individuales del MIP, respectivamente.

b) *Parte de cuerpo mensaje retransmitido:* Los TIC básicos (si existen) y los PNB (si existen) de una parte de cuerpo mensaje serán los mismos del mensaje retransmitido.

c) *Parte de cuerpo definido externamente:* Una parte de cuerpo definido externamente cuyo tipo ampliado corresponde a un tipo básico (véase el anexo B) se tratará de manera prescrita para el tipo básico.

Cualquier otro tipo de parte de cuerpo ampliado se tratará como sigue. Si al tipo corresponden uno o más TIC definidos externamente, serán especificados. De no ser así, se indicará TIC *no definido.* En cualquiera de los dos casos, no se especificará ningún PNB.

d) *Parte de cuerpo básico:* Los TIC básicos (si existen) y los PNB (si existen) de una parte de cuerpo individual de un tipo que no sea mensaje ni definido externamente dependerán del tipo de parte de cuerpo especificado en el cuadro 2/X.420. Un tipo de parte de cuerpo para el cual el cuadro no especifica TIC básicos no provocará el establecimiento de bits en la cadena de bits de los TIC básicos.

e) *Parte de cuerpo cifrado:* El efecto de una parte de cuerpo cifrado en los TIC básicos y los PNB que deben especificarse será objeto de ulterior estudio.

CUADRO 2/X.420

TIC básicos y PNB en mensajería interpersonal

Tipo de parte de cuerpo	TIC básico	PNB
Texto AI5	Texto AI5	–
Voz	Voz	–
Facsímil G3	Facsímil G3	Facsímil G3
G4 clase 1	G4 clase 1	G4 clase 1/Modo mixto
Teletex	Teletex	Teletex
Videotex	Videotex	–
Cifrado	–	–
Mensaje	(véase texto)	(véase texto)
Modo mixto	Modo mixto	G4 clase 1/Modo mixto
Definido bilateralmente	No definido	–
Definido nacionalmente	No definido	–
Definido externamente	(véase texto)	(véase texto)

21 Realización de puertos

En la Recomendación X.419 se especifica la manera en que un AM o el STRM realiza concretamente los puertos secundarios que proporciona.

La forma en que un AU, ATLM, o UA realiza concretamente los puertos primarios que proporciona está fuera del ámbito de esta Recomendación.

Nota 1 – Un interfaz de usuario de AU es un asunto local. Es posible una gran diversidad de interfaces que comprenden por ejemplo gran variedad de dispositivos de entrada/salida.

Nota 2 – Una realización, por el ATLM, de sus puertos primarios se especifica, en parte, en la Recomendación T.330 del CCITT.

Nota 3 – Una UA proporciona sus puertos primarios por medio del sistema de comunicación particular a que da acceso esa UA.

22 Conformidad

A continuación se indican los requisitos que debe satisfacer un objeto secundario (excluido el STRM) y su realizador cuando éste anuncia que el objeto secundario es conforme a esta Recomendación. Cierto número de requisitos de conformidad distinguen entre *sustentar en la generación y sustentar en la recepción.*

22.1 *Relación generación-recepción*

Se dice que un AU, ATLM, o UA **sustentan en la generación** un determinado campo de encabezamiento, ampliación de encabezamiento, tipo de parte de cuerpo básico, o tipo de parte de cuerpo ampliado, únicamente si acepta, conserva y emite, exactamente como se prescribe en esta Recomendación, ese determinado campo de encabezamiento o ampliación, o partes de cuerpo de ese tipo determinado básico o ampliado, en todo momento que un usuario lo invoque para transportar un MIP que los contenga, al STRM o al AM del usuario (este último solamente en el caso de un AU).

Se dirá que un AU, ATLM o UA **sustenta en recepción** un determinado campo de encabezamiento, ampliación de encabezamiento, tipo de parte de cuerpo básico, o tipo de parte de cuerpo ampliado, únicamente si acepta, conserva, y emite, exactamente como prescribe esta Recomendación, ese determinado campo de encabezamiento o ampliación, partes de cuerpo de ese tipo determinado básico o ampliado, en todo momento que el STRM o un AM de usuario (este último solamente en el caso de un AU) lo invoque para transportar al usuario un MIP que los contenga.

Nota – De hecho, una UADP no sustenta nada en generación porque ella no es el suministrador del puerto de generación.

22.2 *Requisitos de los enunciados de conformidad*

El realizador de un AU SMIP, AM SMIP, ATLM, o UA enunciará lo siguiente. Para cada uno de los puntos indicados a continuación deberá hacer enunciados separados relativos a la conformidad en la generación y la conformidad en recepción:

a) Los campos de encabezamiento y las ampliaciones de encabezamiento para los cuales anuncia conformidad.

b) Los tipos de parte de cuerpo básico y ampliado para los cuales anuncia conformidad.

c) En el caso de un AU SMIP o AM SMIP, los atributos de AM específicos o la mensajería interpersonal para los cuales anuncia conformidad.

22.3 *Requisitos estáticos*

Un AU SMIP, AM SMIP, ATLM, o UA satisfarán los siguientes requisitos estáticos:

a) Un AU SMIP, AM SMIP, ATLM o UA establecerá los campos de encabezamiento y las ampliaciones de encabezamiento, y los tipos de parte de cuerpo básico y ampliado para los cuales se anuncia conformidad.

b) Un AU SMIP o AM SMIP sustentará los atributos de AM específicos a la mensajería interpersonal para los cuales se anuncia conformidad, pero incluirá como mínimo los designados como obligatorios en el anexo C.

c) Un AU SMIP, AM SMIP, ATLM o UA realizará concretamente sus puertos abstractos como se especifica en el § 21.

d) Un AU SMIP o AM SMIP deberá poder depositar y aceptar la entrega de mensajes de los dos tipos de contenido indicados en el § 20.2. Un ATLM o UA deberá poder importar y exportar tales mensajes.

22.4 *Requisitos dinámicos*

Un AU SMIP, AM SMIP, ATLM o UA satisfarán los siguientes requisitos dinámicos:

a) Un AU SMIP o AM SMIP seguirá las reglas de operación especificadas en el § 18 ó 19, respectivamente.

b) Un AU SMIP, AM SMIP, ATLM o UA depositará y aceptará la entrega de mensajes cuyo contenido sea el especificado en el § 20.

c) Un AU SMIP, AM SMIP, ATLM o UA inscribirá en el STRM su capacidad para aceptar entregas de mensajes de los dos tipos de contenido indicados en el § 20.2.

ANEXO A

(a la Recomendación X.420)

Ampliaciones del encabezamiento

Este anexo forma parte integrante de la Recomendación.

Este anexo define todas las ampliaciones de encabezamiento (actualmente definidas).

A.1 *Copia incompleta*

La ampliación de encabezamiento **copia incompleta**, por su presencia, indica que una o más partes de cuerpo o campos de encabezamiento están ausentes del cuerpo del MIP (el caso presente del MIP). La ampliación comprende un nulo (por defecto).

```
Incomplete-copy HEADING EXTENSION
        ::= id-hex-incomplete copy
```

Si esta ampliación está ausente del campo de ampliaciones, se considerará que todas las partes de cuerpo están presentes.

A.2 *Idiomas*

La ampliación de encabezamiento **idiomas** identifica los idiomas utilizados en la composición del campo de encabezamiento asunto y cuerpo del MIP. La ampliación comprende un conjunto de cero o más cadenas imprimibles, siendo cada una de ellas uno de los códigos de idioma de dos caracteres identificados en ISO 639.2.

```
languages HEADING-EXTENSION
        VALUE SET OF Language
        ::= id-hex-languages

Language ::= PrintableString (SIZE (2..2))
```

Si esta ampliación está ausente del campo de encabezamiento ampliaciones o no se indica ningún idioma, los idiomas deberán considerarse no especificados.

ANEXO B

(a la Recomendación X.420)

Tipos de parte de cuerpo ampliado

Este anexo forma parte integrante de esta Recomendación.

Para cada tipo de parte de cuerpo básico, esta Recomendación define como sigue un tipo de parte de cuerpo ampliado.

```
ia5-text-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  IA5TextParameters IDENTIFIED BY id-ep-ia5-text
        DATA        IA5TextData
        ::= id-et-ia5-text

voice-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  VoiceParameters IDENTIFIED BY id-ep-voice
        DATA        VoiceData
        ::= id-et-voice

g3-facsimile-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  G3FacsimileParameters IDENTIFIED BY id-ep-g3-facsimile
        DATA        G3FacsimileData
        ::= id-et-g3-facsimile

g4-class1-body-part EXTENDED-BODY-PART-TYPE
        DATA        G4Class1BodyPart
        ::= id-et-g4-class1

teletex-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  TeletexParameters IDENTIFIED BY id-ep-teletex
        DATA        TeletexData
        ::= id-et-teletex

videotex-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  VideotexParameters IDENTIFIED BY id-ep-videotex
        DATA        VideotexData
        ::= id-et-videotex

encrypted-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  EncryptedParameters IDENTIFIED BY id-ep-encrypted
        DATA        EncryptedData
        ::= id-et-encrypted

message-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  MessageParameters IDENTIFIED BY id-ep-message
        DATA        MessageData
        ::= id-et-message
```

```
mixed-mode-body-part EXTENDED-BODY-PART-TYPE
        DATA            MixedModeBodyPart
        ::= id-et-mixed-mode

bilaterally-defined-body-part EXTENDED-BODY-PART-TYPE
        DATA            BilaterallyDefinedBodyPart
        ::= id-et-bilaterally-defined

nationally-defined-body-part EXTENDED-BODY-PART-TYPE
        DATA            NationallyDefinedBodyPart
        ::= id-et-nationally-defined
```

ANEXO C

(a la Recomendación X.420)

Atributos del almacenamiento de mensajes

Este anexo forma parte integrante de esta Recomendación.

Como se ha descrito en la Recomendación X.413, un AM mantiene y proporciona acceso a ciertos atributos (por ejemplo, la importancia) de cada objeto de información contenido en el mismo. Un atributo comprende un tipo y, según el tipo de que se trate, uno o más valores. Los atributos que pueden adoptar varios valores simultáneamente (pertenecientes todos ellos a un solo objeto) se denominan atributos de múltiples valores (o multivaluados) y los que sólo pueden adoptar un valor se denominan atributos de un solo valor (o univaluados). Algunos atributos corresponden a objetos de información de todas clases, y otros objetos de información de ciertas clases (por ejemplo, los de la sección 2).

Este anexo define los atributos de AM específicos de la mensajería interpersonal.

Todos los atributos definidos en este anexo, con excepción de los que corresponden a los tipos de parte de cuerpo ampliado (que no pueden enumerarse: véase el § C.3.6) se enumeran en la primera columna del cuadro C-1/X.420. En este cuadro se indica su presencia en una inscripción de mensaje entregado. Ninguno de ellos aparece en una inscripción de informe entregado ni en una inscripción de contenido devuelto. En cuanto a los símbolos utilizados en el cuadro, véase la Recomendación X.413.

C.1 *Atributos de resumen*

Algunos atributos resumen un objeto de información de mensajería interpersonal. Estos atributos se definen y describen a continuación.

C.1.1 *Tipo de inscripción de MIP*

El atributo **tipo de inscripción MIP** identifica un tipo de objeto de información.

```
ipm-entry-type ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMEntryType
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-sat-ipm-entry-type

IPMEntryType ::= ENUMERATED {
        ipm(0),
        rn(1),
        nrn(2) }
```

Este atributo puede adoptar uno de los siguientes valores:

a) *mip:* El objeto de información es un MIP.

b) *nr:* El objeto de información es una NR.

c) *nnr:* El objeto de información es una NNR.

Un AM que admite este atributo lo mantendrá para un objeto de información contenido en el mismo si y solo si ese objeto es un mensaje cuyo contenido es un MIP o un NIP.

CUADRO C-1/X.420

Resumen de los atributos AM

Atributo	V	L	P MIP	P NNR	P NR	L	S
Modo acuse de recibo	S	F	–	–	O	Y	Y
Usuarios autorizantes	M	F	C	–	–	Y	N
Comentario de retransmisión automática	S	F	–	C	–	Y	N
Retransmitido automáticamente	S	F	C	–	–	Y	Y
Partes de cuerpo definido bilateralmente	M	F	C	–	–	N	N
Destinatarios de copia ciega	M	F	C	–	–	Y	N
Cuerpo	S	O	O	–	–	N	N
TIC para conversión	M	F	–	C	C	Y	N
Destinatarios de copia	M	F	C	–	–	Y	N
Motivo de descarte	S	F	–	C	–	Y	Y
Partes de cuerpo cifrado	M	F	C	–	–	N	N
Datos cifrados	M	F	C	–	–	N	N
Parámetros cifrados	M	F	C	–	–	N	N
Hora de expiración	S	F	C	–	–	Y	Y
Tipos de parte de cuerpo ampliado	M	F	C	–	–	Y	Y
Partes de cuerpo facsímil G3	M	F	C	–	–	N	N
Datos facsímil G3	M	F	C	–	–	N	N
Parámetros facsímil G3	M	F	C	–	–	N	N
Partes de cuerpo G4 clase 1	M	F	C	–	–	N	N
Encabezamiento	S	M	O	–	–	N	N
Partes de cuerpo de texto AI5	M	F	C	–	–	N	N
Datos de texto AI5	M	F	C	–	–	N	N
Parámetros de texto AI5	M	F	C	–	–	N	N
Importancia	S	F	C	–	–	Y	Y
Copia incompleta	S	F	C	–	–	Y	N
Tipo de inscripción de MIP	S	O	O	O	O	Y	Y
Destinatario preferido de MIP	S	F	–	C	C	Y	N
Sinopsis de MIP	S	F	O	–	–	N	N
Originador de MIP	S	F	–	C	C	Y	N
Idiomas	M	F	C	–	–	Y	N
Partes de cuerpo de mensaje	M	F	C	–	–	N	N
Datos de mensaje	M	F	C	–	–	N	N
Parámetros de mensaje	M	F	C	–	–	N	N
Partes de cuerpo de modo mixto	M	F	C	–	–	N	N
Partes de cuerpo definido nacionalmente	M	F	C	–	–	N	N
Motivo de no recepción	S	F	–	O	–	Y	Y
Solicitantes de NNR	M	F	C	–	–	Y	N
MIP obsoletos	M	F	C	–	–	Y	N
Originador	S	F	C	–	–	Y	N

CUADRO C-1/X.420 *(cont.)*

Atributo	V	L	P MIP	P NNR	P NR	L	S
Destinatarios primarios	M	F	C	–	–	Y	N
Hora de recepción	S	F	–	–	O	Y	N
MIP conexos	M	F	C	–	–	Y	N
MIP constestado	S	F	C	–	–	Y	N
Destinatarios de respuesta	M	F	C	–	–	Y	N
Solicitantes de respuesta	M	F	C	–	–	Y	N
Hora de respuesta	S	F	C	–	–	Y	N
MIP devuelto	S	F	–	C	–	Y	N
Solicitantes NR	M	F	C	–	–	Y	N
Sensibilidad	S	F	C	–	–	Y	Y
Asunto	S	F	C	–	–	Y	N
MIP asunto	S	O	–	O	O	Y	N
Información de recepción suplementaria	S	F	–	–	C	Y	N
Partes de cuerpo teletex	M	F	C	–	–	N	N
Datos teletex	M	F	C	–	–	N	N
Parámetros teletex	M	F	C	–	–	N	N
Este MIP	S	O	O	–	–	Y	N
Partes de cuerpo videotex	M	F	C	–	–	N	N
Datos videotex	M	F	C	–	–	N	N
Parámetros videotex	M	F	C	–	–	N	N
Partes de cuerpo voz	M	F	C	–	–	N	N
Datos de voz	M	F	C	–	–	N	N
Parámetros de voz	M	F	C	–	–	N	N

V Uni/multivaluado

L Nivel de sustentación por AM y AU de acceso

P Presencia en la inscripción de mensaje entregado

L Disponible para lista, alerta

S Disponible para resumen

Nota – En este cuadro, en las columnas bajo el epígrafe L y P: O significa obligatorio *(mandatory)* y F significa facultativo *(optional)*.

C.1.2 *Sinopsis de MIP*

El atributo **sinopsis de MIP** da la estructura, características, tamaño y estado de procesamiento de un MIP para la granularidad de partes de cuerpo individuales.

```
ipm-synopsis ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMSynopsis
        SINGLE VALUE
        ::= id-sat-ipm-synopsis
```

La sinopsis de un MIP consta de una sinopsis de cada una de sus partes de cuerpo. Las sinopsis aparecen en el mismo orden que las partes de cuerpo.

```
IPMSynopsis ::= SEQUENCE OF BodyPartSynopsis
```

La sinopsis de una parte de cuerpo adopta una de dos formas, lo que depende de que la parte de cuerpo sea del tipo mensaje. Esto permite a la sinopsis de un MIP retransmisor abarcar las partes de cuerpo de cada MIP retransmitido (recurrentemente), así como las del propio MIP retransmisor.

```
BodyPartSynopsis ::= CHOICE {
        message         [0] MessageBodyPartSynopsis
        non-message     [1] NonMessageBodyPartSynopsis }

MessageBodyPartSynopsis ::= SEQUENCE {
        number          [0] SequenceNumber,
        synopsis        [1] IPMSynopsis }

NonMessageBodyPartSynopsis ::= SEQUENCE {
        type            [0] OBJECT IDENTIFIER,
        parameters      [1] ExternallyDefinedParameters,
        size            [2] INTEGER,
        processed       [3] BOOLEAN DEFAULT FALSE }
```

La sinopsis de una parte de cuerpo de mensaje tiene los siguientes componentes:

a) **Número** (O): Número secuencial que el AM asigna a la inscripción representada por la parte de cuerpo mensaje.

b) **Sinopsis** (O): Sinopsis del MIP que forma el contenido del mensaje representado por la parte de cuerpo.

La sinopsis de una parte de cuerpo de un tipo diferente de mensaje tiene los siguientes componentes. A los fines de esta sinopsis, se considera que la parte de cuerpo es del tipo definido externamente, independientemente (véase el anexo B) de que sea o no transportada al AM:

a) **Tipo** (O): Parte de cuerpo de tipo ampliado, es decir, el componente referencia directa del componente datos de la parte de cuerpo. Es un identificador de objeto.

b) **Parámetros** (O): Parámetros de formato y de control de la parte de cuerpo, es decir, el componente parámetros de la parte de cuerpo. Es un cualquiera (Any).

c) **Tamaño** (O): Tamaño en octetos de la codificación de componente codificación del componente datos de la parte de cuerpo, cuando se siguen las reglas básicas de codificación de la Recomendación X.209. Si esas reglas permiten varias codificaciones (por ejemplo, la primitiva y la construida) del componente, el tamaño puede reflejar cualquiera de ellas. Es un entero.

d) **Procesado** (D *falso*): Indicación de si la parte de cuerpo ha sido o no transportada al AU por medio de la operación abstracta listado o captura del AM. Es un booleano.

Un AM que admite este atributo deberá mantenerlo para un objeto de información contenido por el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP.

Nota – Como consecuencia de su variabilidad el valor del componente tamaño debe considerarse solamente como una estimación del tamaño de la parte de cuerpo.

C.2 *Atributos del encabezamiento*

Del encabezamiento de un MIP se derivan algunos atributos los cuales se definen y describen a continuación.

C.2.1 *Encabezamiento*

El abributo **encabezamiento** es el encabezamiento (completo) de un MIP.

```
heading ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Heading
        SINGLE VALUE
        ::= id-hat-heading
```

Un AM que admite este atributo lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP.

C.2.2 *Análisis del encabezamiento*

Algunos atributos tienen como valores descriptores O/D seleccionados después de un análisis del encabezamiento. Dichos valores identifican destinatarios «primarios», «de copia», y «de copia ciega» de un MIP con relación al cual se ha solicitado una NR, NNR, o respuesta.

```
rn-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-rn-requestors
```

```
nrn-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-nrn-requestors

reply-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-reply-requestors
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo encabezamiento solicita, de al menos un usuario o LD, un NR, NNR o respuesta, respectivamente. Mantendrá un valor de atributo para cada especificador de destinatario en el campo de destinatarios primarios, de copia, o de copia ciega del MIP, campo cuyo componente peticiones de notificación incluye el valor nr (en el caso del primer atributo) o nnr (en el caso del segundo), o cuyo componente respuesta solicitada significa, por su presencia o ausencia, que se ha solicitado una respuesta (en el caso del tercero). El valor será el componente destinatario del especificador de destinatario.

C.2.3 *Campos del encabezamiento*

Algunos atributos llevan los nombres de campos de encabezamiento y tienen estos campos como sus valores. Para la ordenación de los atributos de hora de expiración y hora de respuesta se sigue el orden cronológico creciente.

```
this-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX This IPMField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-this-ipm

originator ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OriginatorField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-originator

replied-to-IPM ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RepliedToIPMField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-replied-to-IPM

subject ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-hat-subject

expiry-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ExpiryTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-hat-expiry-time

reply-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReplyTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-hat-reply-time

importance ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ImportanceField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-importance
```

```
sensitivity ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SensitivityField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-sensitivity

auto-forwarded ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AutoForwardedField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-auto-forwarded
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo encabezamiento contiene el campo cuyo nombre lleva el atributo.

C.2.4 *Subcampos del encabezamiento*

Algunos atributos llevan los nombres de campos de encabezamiento y tienen como valores subcampos de esos campos.

```
authorizing-users ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AuthorizingUsersSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-authorizing-users

primary-recipients; ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX PrimaryRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-primary-recipients

copy-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX CopyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-copy-recipients

blind-copy-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX BlindCopyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-blind-copy-recipients

obsoleted-IPMs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ObsoletedIPMsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-obsoleted-IPMs

related-IPMs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RelatedIPMsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-related-IPMs

reply-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReplyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-reply-recipients
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo encabezamiento contiene el campo cuyo nombre lleva el atributo. Mantendrá un valor de atributo para cada subcampo.

C.2.5 *Ampliaciones del encabezamiento*

Algunos atributos llevan los nombres de ampliaciones de encabezamiento y tienen como valores los valores de estas ampliaciones o una parte de los mismos.

```
incomplete-copy ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX incompleteCopyExtensionValue
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-incomplete-copy

languages ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Language
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-languages
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo encabezamiento contiene la ampliación cuyo nombre lleva el atributo. En el caso de los atributos de idioma, el AM mantendrá un valor de atributo para cada idioma identificado por la ampliación.

C.3 *Atributos de cuerpo*

Algunos atributos se derivan del cuerpo de un MIP. Estos atributos se definen y describen a continuación.

C.3.1 *Cuerpo*

El atributo **cuerpo** es el cuerpo (completo) de un MIP.

```
body ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Body
        SINGLE VALUE
        ::= id-bat-body
```

Un AM que admite este atributo lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP.

C.3.2 *Partes de cuerpo básico*

Algunos atributos llevan los nombres de tipos de parte de cuerpo básico y tienen como valores, con una excepción, tales parte de cuerpo.

Un AM contiene cada MIP retransmitido (es decir, cada parte de cuerpo mensaje) como un objeto de información por su propio derecho, separado del MIP retransmisor. Ese objeto de información, por supuesto, es un mensaje cuyo contenido es un MIP. El atributo partes de cuerpo de mensaje, que se indica más adelante, tiene por tanto como valores la secuencia de números que el AM asigna a esos mensajes.

```
ia5-text-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IA5TextBodyPart
        MULTI VALUE
        ::= id-bat-ia5-text-body-parts

voice-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VoiceBodyPart
        MULTI VALUE
        ::= id-bat-voice-body-parts

g3-facsimile-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G3FacsimileBodyPart
        MULTI VALUE
        ::= id-bat-g3-facsimile-body-parts

g4-class1-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G4Class1BodyPart
        MULTI VALUE
        ::= id-bat-g4-class1-body-parts

teletex-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX TeletexBodyPart
        MULTI VALUE
        ::= id-bat-teletex-body-parts
```

videotex-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX VideotexBodyPart
MULTI VALUE
::= id-bat-videotex-body-parts

encrypted-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX EncryptedBodyPart
MULTI VALUE
::= id-bat-encrypted-body-parts

message-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX SequenceNumber
MULTI VALUE
::= id-bat-message-body-parts

mixed-mode-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX MixedModeBodyPart
MULTI VALUE
::= id-bat-mixed-mode-body-parts

bilaterally-defined-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX BilaterallyDefinedBodyPart
MULTI VALUE
::= id-bat-bilaterally-defined-body-parts

nationally-defined-body-parts ATTRIBUTE
WITH ATTRIBUTE-SYNTAX NationallyDefinedBodyPart
MULTI VALUE
::= id-bat-nationally-defined-body-parts

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo cuerpo contiene una o más partes de cuerpo del tipo cuyo nombre lleva el atributo. Mantendrá un valor de atributo para cada una de esas partes de cuerpo.

C.3.3 *Componentes de parámetros de parte de cuerpo básico*

Algunos atributos llevan los nombres de tipos de parte de cuerpo básico y tienen como valores los componentes parámetros de esas partes de cuerpo.

ia5-text-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX IA5TextParameters
MULTI VALUE
::= id-bat-ia5-text-parameters

voice-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX VoiceParameters
MULTI VALUE
::= id-bat-voice-parameters

g3-facsimile-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX G3FacsimileParameters
MULTI VALUE
::= id-bat-g3-facsimile-parameters

teletex-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX TeletexParameters
MULTI VALUE
::= id-bat-teletex-parameters

videotex-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX VideotexParameters
MULTI VALUE
::= id-bat-videotex-parameters

encrypted-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX EncryptedParameters
MULTI VALUE
::= id-bat-encrypted-parameters

message-parameters ATTRIBUTE
WITH ATTRIBUTE-SYNTAX MessageParameters
MULTI VALUE
::= id-bat-message-parameters

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si el objeto es un mensaje cuyo contenido es un MIP cuyo cuerpo contiene una o más partes de cuerpo del tipo cuyo nombre lleva el atributo. Mantendrá un valor de atributo para cada una de esas partes de cuerpo.

C.3.4 *Componentes de datos de parte de cuerpo básico*

Algunos atributos llevan los nombres de tipos de parte de cuerpo básico y tienen como valores componentes datos de esas partes de cuerpo.

```
ia5-text-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IA5TextData
        MULTI VALUE
        ::= id-bat-ia5-text-data

voice-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VoiceData
        MULTI VALUE
        ::= id-bat-voice-data

g3-facsimile-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G3FacsimileData
        MULTI VALUE
        ::= id-bat-g3-facsimile-data

teletex-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX TeletexData
        MULTI VALUE
        ::= id-bat-teletex-data

videotex-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VideotexData
        MULTI VALUE
        ::= id-bat-videotex-data

encrypted-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EncryptedData
        MULTI VALUE
        ::= id-bat-encrypted-data

message-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageData
        MULTI VALUE
        ::= id-bat-message-data
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP cuyo cuerpo contiene una o más partes de cuerpo del tipo cuyo nombre lleva el atributo. Mantendrá un valor de atributo para cada una de esas partes de cuerpo.

C.3.5 *Tipos de partes de cuerpo ampliado*

El atributo **tipos de parte de cuerpo ampliado** identifica los tipos de parte de cuerpo ampliado representados en un MIP.

```
extended-body-part-types ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OBJECT IDENTIFIER
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-bat-extended-body-part-types
```

Un AM que admite este atributo lo mantendrá para un objeto de información contenido en el mismo, si y solo si el objeto es un mensaje cuyo contenido es un MIP cuyo cuerpo contiene uno o más partes de cuerpo definido externamente. Mantendrá un valor de atributo para cada tipo presente. El valor designará el tipo como se especifica en el § 7.3.12.

Nota – Cada valor de este atributo corresponde a uno de los atributos descritos en el § C.3.6.

C.3.6 *Partes de cuerpo ampliado*

Algunos atributos, no denominados, tienen como sus valores los componentes codificación (véase el § 7.3.12) de los externos NSA.1 que constituyen los componentes datos de partes de cuerpo definido externamente.

A cada tipo de parte de cuerpo ampliado corresponden dos atributos. El primer atributo es designado por el identificador de objeto que es el componente referencia directa (véase también aquí el § 7.3.12) del externo que constituye el componente datos de una parte de cuerpo de ese tipo. El contenido de este primer atributo es dicho componente datos. El segundo atributo es designado por el identificador de objeto que es el componente referencia directa del externo que constituye el componente parámetros de una parte de cuerpo de ese tipo. El contenido de este segundo atributo es dicho componente parámetros.

Un AM que admite una de estas parte de cuerpo mantendrá ambos atributos para un objeto de información contenido en el mismo, si y solo si el objeto es un mensaje cuyo contenido es un MIP cuyo cuerpo contiene una o más partes de cuerpo del tipo que corresponde a ese atributo. Mantendrá un valor de cada atributo para cada una de esas partes de cuerpo.

Nota 1 – Los atributos de parte de cuerpo ampliado no pueden enumerarse en la práctica, pues los tipos de parte de cuerpo ampliado no pueden enumerarse entonces.

Nota 2 – El atributo tipos de parte de cuerpo ampliado (véase el § C.3.5) determina los atributos de parte de cuerpo ampliado para un MIP determinado.

C.4 *Atributos de notificación*

Algunos atributos se derivan de una NIP. Estos atributos se definen y describen a continuación.

C.4.1 *Campos comunes*

Algunos atributos llevan los nombres de campos comunes y tienen esos campos como valores.

```
subject-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectIPMField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-subject-ipm

ipn-originator ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPNOriginatorField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-ipn-originator

ipm-preferred-recipient ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMPreferredRecipientField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-ipm-preferred-recipient

conversion-eits ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EITs
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-nat-conversion-eits
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es un MIP que contiene el campo cuyo nombre lleva el atributo.

C.4.2 *Campos de no recepción*

Algunos atributos llevan los nombres de campos de no recepción y tienen esos campos como valores.

```
non-receipt-reason ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX NonReceiptReasonField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-non-receipt-reason
```

```
discard-reason ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DiscardReasonField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-discard-reason

auto-forward-comment ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AutoForwardCommentField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-auto-forward-comment

returned-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReturnedIPMField
        SINGLE VALUE
        ::= id-nat-returned-ipm
```

Un AM que admite uno de estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es una NNR que contiene el campo cuyo nombre lleva el atributo.

C.4.3 *Campos de recepción*

Algunos atributos llevan los nombres de campos de recepción y tienen esos nombres como valores. Para la ordenación del atributo hora de recepción se sigue el orden cronológico creciente.

```
receipt-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReceiptTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-nat-receipt-time

acknowledgment-mode ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AcknowledgmentModeField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-acknowledgment-mode

suppl-receipt-info ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SupplReceiptInfoField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-suppl-receipt-info
```

Un AM que admite estos atributos lo mantendrá para un objeto de información contenido en el mismo, si y solo si ese objeto es un mensaje cuyo contenido es una NR que contiene el campo cuyo nombre lleva el atributo.

ANEXO D

(a la Recomendación X.420)

Definición de referencia de indicadores de objeto

Este anexo forma parte integrante de esta Recomendación.

El anexo define, con fines de referencia, diversos identificadores de objeto mencionados en módulos NSA.1 de anexos subsiguientes. Utiliza NSA.1.

Todos los identificadores de objeto asignados por esta Recomendación figuran como tales en este anexo. El anexo es definitivo con respecto a todos ellos, salvo los que corresponden a módulos NSA.1 y a la aplicación SMIP propiamente dicha. Las asignaciones definitivas para los primeros vienen dadas en los propios módulos; otras referencias a los mismos se dan en cláusulas IMPORT. Los últimos son fijos.

```
IPMObjectIdentifiers {joint-iso-ccitt
        mhs-motis(6) modules(0) object-identifiers(0)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo

IMPORTS -- nada --;

ID ::= OBJECT IDENTIFIER


-- Mensajería Interpersonal (no definitivo)

id-ipms ID ::= {joint-iso-ccitt mhs-motis(6) ipms(1)} -- no definitivo


-- Categorías

id-mod  ID ::= {id-ipms 0} --  módulos; no definitivos
id-ot   ID ::= {id-ipms 1} --  tipos de objeto
id-pt   ID ::= {id-ipms 2} --  tipos de puerto
id-ref  ID ::= {id-ipms 3} --  perfeccionamientos
id-et   ID ::= {id-ipms 4} --  tipos de parte de cuerpo ampliado
id-hex  ID ::= {id-ipms 5} --  ampliaciones de encabezamiento
id-sat  ID ::= {id-ipms 6} --  atributos de resumen
id-hat  ID ::= {id-ipms 7} --  atributos de encabezamiento
id-bat  ID ::= {id-ipms 8} --  atributos de cuerpo
id-nat  ID ::= {id-ipms 9} --  atributos de notificación
id-mct  ID ::= {id-ipms 10} -- tipos de contenido de mensaje
id-ep   ID ::= {id-ipms 11} -- parámetros de parte de cuerpo ampliado


-- Módulos

id-mod-object-identifiers          ID ::= {id-mod 0} -- no definitivo
id-mod-functional-objects          ID ::= {id-mod 1} -- no definitivo
id-mod-information-objects         ID ::= {id-mod 2} -- no definitivo
id-mod-abstract-service            ID ::= {id-mod 3} -- no definitivo
id-mod-heading-extensions          ID ::= {id-mod 6} -- no definitivo
id-mod-extended-body-part-types    ID ::= {id-mod 7} -- no definitivo
id-mod-message-store-attributes    ID ::= {id-mod 8} -- no definitivo
id-mod-upper-bounds                ID ::= {id-mod 10} -- no definitivo


-- Tipos de objeto

id-ot-ipme                         ID ::= {id-ot 0}
id-ot-ipms-user                    ID ::= {id-ot 1}
id-ot-ipms                         ID ::= {id-ot 2}
id-ot-ipms-ua                      ID ::= {id-ot 3}
id-ot-ipms-ms                      ID ::= {id-ot 4}
id-ot-tlma                         ID ::= {id-ot 5}
id-ot-tlxau                        ID ::= {id-ot 6}
id-ot-pdau                         ID ::= {id-ot 7}


-- Tipos de puerto

id-pt-origination                  ID ::= {id-pt 0}
id-pt-reception                    ID ::= {id-pt 1}
id-pt-management                   ID ::= {id-pt 2}
```

-- *Perfeccionamientos*

```
id-ref-primary                  ID ::= { id-ref 0 }
id-ref-secondary                ID ::= { id-ref 1 }
```

-- *Tipos de parte de cuerpo ampliado*

```
id-et-ia5-text                  ID ::= { id-et 0 }
id-et-voice                     ID ::= { id-et 1 }
id-et-g3-facsimile              ID ::= { id-et 2 }
id-et-g4-classe1                ID ::= { id-et 3 }
id-et-teletex                   ID ::= { id-et 4 }
id-et-videotex                  ID ::= { id-et 5 }
id-et-encrypted                 ID ::= { id-et 6 }
id-et-message                   ID ::= { id-et 7 }
id-et-mixed-mode                ID ::= { id-et 8 }
id-et-bilaterally-defined       ID ::= { id-et 9 }
id-et-nationally-defined        ID ::= { id-et 10 }
```

-- *Ampliaciones de encabezamiento*

```
id-hex-incomplete-copy          ID ::= { id-hex 0 }
id-hex-languages                ID ::= { id-hex 1 }
```

-- *Atributos de resumen*

```
id-sat-ipm-entry-type           ID ::= { id-sat 0 }
id-sat-ipm-synopsis             ID ::= { id-sat 1 }
```

-- *Atributos de encabezamiento*

```
id-hat-heading                  ID ::= { id-hat 0 }
id-hat-this-ipm                 ID ::= { id-hat 1 }
id-hat-originator               ID ::= { id-hat 2 }
id-hat-replied-to-IPM           ID ::= { id-hat 3 }
id-hat-subject                  ID ::= { id-hat 4 }
id-hat-expiry-time              ID ::= { id-hat 5 }
id-hat-reply-time               ID ::= { id-hat 6 }
id-hat-importance               ID ::= { id-hat 7 }
id-hat-sensitivity              ID ::= { id-hat 8 }
id-hat-auto-forwarded           ID ::= { id-hat 9 }
id-hat-authorizing-users        ID ::= { id-hat 10 }
id-hat-primary-recipients       ID ::= { id-hat 11 }
id-hat-copy-recipients          ID ::= { id-hat 12 }
id-hat-blind-copy-recipients    ID ::= { id-hat 13 }
id-hat-obsoleted-IPMs           ID ::= { id-hat 14 }
id-hat-related-IPMs             ID ::= { id-hat 15 }
id-hat-reply-recipients         ID ::= { id-hat 16 }
id-hat-incomplete-copy          ID ::= { id-hat 17 }
id-hat-languages                ID ::= { id-hat 18 }
id-hat-rn-requestors            ID ::= { id-hat 19 }
id-hat-nrn-requestors           ID ::= { id-hat 20 }
id-hat-reply-requestors         ID ::= { id-hat 21 }
```

-- *Atributos de cuerpo*

```
id-bat-body                          ID ::= {id-bat 0}
id-bat-ia5-text-body-parts           ID ::= {id-bat 1}
id-bat-voice-body-parts              ID ::= {id-bat 2}
id-bat-g3-facsimile-body-parts       ID ::= {id-bat 3}
id-bat-g4-class1-body-parts          ID ::= {id-bat 4}
id-bat-teletex-body-parts            ID ::= {id-bat 5}
id-bat-videotex-body-parts           ID ::= {id-bat 6}
id-bat-encrypted-body-parts          ID ::= {id-bat 7}
id-bat-message-body-parts            ID ::= {id-bat 8}
id-bat-mixed-mode-body-parts         ID ::= {id-bat 9}
id-bat-bilaterally-defined-body-parts ID ::= {id-bat 10}
id-bat-nationally-defined-body-parts ID ::= {id-bat 11}
id-bat-extended-body-part-types      ID ::= {id-bat 12}
id-bat-ia5-text-parameters           ID ::= {id-bat 13}
id-bat-voice-parameters              ID ::= {id-bat 14}
id-bat-g3-facsimile-parameters       ID ::= {id-bat 15}
id-bat-teletex-parameters            ID ::= {id-bat 16}
id-bat-videotex-parameters           ID ::= {id-bat 17}
id-bat-encrypted-parameters          ID ::= {id-bat 18}
id-bat-message-parameters            ID ::= {id-bat 19}
id-bat-ia5-text-data                 ID ::= {id-bat 20}
id-bat-voice-data                    ID ::= {id-bat 21}
id-bat-g3-facsimile-data             ID ::= {id-bat 22}
id-bat-teletex-data                  ID ::= {id-bat 23}
id-bat-videotex-data                 ID ::= {id-bat 24}
id-bat-encrypted-data                ID ::= {id-bat 25}
id-bat-message-data                  ID ::= {id-bat 26}
```

-- *Atributos de notificación*

```
id-nat-subject-ipm                   ID ::= {id-nat 0}
id-nat-ipn-originator                ID ::= {id-nat 1}
id-nat-ipm-preferred-recipient       ID ::= {id-nat 2}
id-nat-conversion-eits               ID ::= {id-nat 3}
id-nat-non-receipt-reason            ID ::= {id-nat 4}
id-nat-discard-reason                ID ::= {id-nat 5}
id-nat-auto-forward-comment          ID ::= {id-nat 6}
id-nat-returned-ipm                  ID ::= {id-nat 7}
id-nat-receipt-time                  ID ::= {id-nat 8}
id-nat-acknowledgment-mode           ID ::= {id-nat 9}
id-nat-suppl-receipt-info            ID ::= {id-nat 10}
```

-- *Tipos de contenido de mensaje (para uso por AM solamente)*

```
id-mct-p2-1984 ID ::= {id-mct 0} -- P2 1984
id-mct-p2-1988 ID ::= {id-mct 1} -- P2 1988
```

-- *Parámetros de parte de cuerpo ampliado*

```
id-ep-ia5-text                       ID ::= {id-ep 0}
id-ep-voice                          ID ::= {id-ep 1}
id-ep-g3-facsimile                   ID ::= {id-ep 2}
id-ep-teletex                        ID ::= {id-ep 4}
id-ep-videotex                       ID ::= {id-ep 5}
id-ep-encrypted                      ID ::= {id-ep 6}
id-ep-message                        ID ::= {id-ep 7}
```

END -- *of IPMSObjectIdentifiers*

ANEXO E

(a la Recomendación X.420)

Definición de referencia de objetos de información abstractos

Este anexo forma parte integrante de esta Recomendación.

Este anexo, que es un suplemento de la sección dos, define con fines de referencia los objetos de información abstractos de mensajería interpersonal.

```
IPMSInformationObjects {joint-iso-ccitt
    mhs-motis(6) ipms(1) modules(0) information-objects(2)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo

IMPORTS
    -- Límites superiores SMIP

        ub-auto-forward-comment, ub-free-form-name, ub-ipm-identifier-suffix,
        ub-local-ipm-identifier, ub-subject-field, ub-telephone-number
        ----
        FROM IPMSUpperBounds {joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) upper-bounds(10)}

    -- TAMD

        ProtocolElement
        ----
        FROM dTAM

    -- Servicio abstracto STRM

        EncodedInformationTypes, G3FacsimileNonBasicParameters,
        MessageDeliveryTime, ORAddress, ORName,
        OtherMessageDeliveryFields, SupplementaryInformation,
        TeletexNonBasicParameters,
        ----
        FROM MTSAbstractService {joint-iso-ccitt
            mhs-motis(6) mts(3) modules(0) mts-abstract-service(1)};

Time ::= UTCTime


-- Objeto de información

InformationObject ::= CHOICE {
    ipm     [0] IPM,
    ipn     [1] IPN}


-- MIP

IPM ::= SEQUENCE {
    heading     Heading,
    body        Body}
```

```
--Encabezamiento

Heading ::= SET{
        this-IPM                    ThisIPMField,
        originator                  [0] OriginatorField OPTIONAL,
        authorizing-users           [1] AuthorizingUsersField OPTIONAL,
        primary-recipients          [2] PrimaryRecipientsField DEFAULT {},
        copy-recipients             [3] CopyRecipientsField DEFAULT {},
        blind-copy-recipients       [4] BlindCopyRecipientsField OPTIONAL,
        replied-to-IPM              [5] RepliedToIPMField OPTIONAL,
        obsoleted-IPMs              [6] ObsoletedIPMsField DEFAULT {},
        related-IPMs                [7] RelatedIPMsField DEFAULT {},
        subject                     [8] EXPLICIT SubjectField OPTIONAL,
        expiry-time                 [9] ExpiryTimeField OPTIONAL,
        reply-time                  [10] ReplyTimeField OPTIONAL,
        reply-recipients            [11] ReplyRecipientsField OPTIONAL,
        importance                  [12] ImportanceField DEFAULT normal,
        sensitivity                 [13] SensitivityField OPTIONAL,
        auto-forwarded              [14] AutoForwardedField DEFAULT FALSE,
        extensions                  [15] ExtensionsField DEFAULT {}}


-- Tipos de componente de encabezamiento

IPMIdentifier ::= [APPLICATION 11] SET{
        user                        ORAdress OPTIONAL
        user-relative-identifier    LocalIPMIdentifier}

LocalIPMIdentifier ::= PrintableString
        (SIZE (0. .ub-local-ipm-identifier))

RecipientSpecifier ::= SET{
        recipient                   [0] ORDescriptor,
        notification-requests       [1] NotificationRequests DEFAULT {},
        reply-requested             [2] BOOLEAN DEFAULT FALSE}

NotificationRequests ::= BIT STRING{
        rn(0),
        nrn(1),
        ipm-return(2)}

ORDescriptor ::= SET{
        formal-name                 ORName OPTIONAL,
        free-form-name              [0] FreeFormName OPTIONAL,
        telephone-number            [1] TelephoneNumber OPTIONAL}

FreeFormName ::= TeletexString (SIZE (0. .ub-free-form-name))

TelephoneNumber ::= PrintableString (SIZE (0. .ub-telephone-number))


-- Campo de encabezamiento este MIP

ThisIPMField ::= IPMIdentifier


-- Campo de encabezamiento originador

OriginatorField ::= ORDescriptor


-- Campo de encabezamiento usuarios autorizantes

AuthorizingUsersField ::= SEQUENCE OF AuthorizingUsersSubfield

AuthorizingUsersSubField ::= ORDescriptor
```

```
-- Campo de encabezamiento destinatarios primarios
PrimaryRecipientsField ::= SEQUENCE OF PrimaryRecipientsSubfield
PrimaryRecipientsSubfield ::= RecipientSpecifier

-- Campo de encabezamiento destinatarios de copia
CopyRecipientsField ::= SEQUENCE OF CopyRecipientsSubfield
CopyRecipientsField ::= RecipientsSpecifier

-- Campo de encabezamiento destinatarios de copia ciega
BlindCopyRecipientsField ::= SEQUENCE OF BlindCopyRecipientsSubfield
BlindCopyRecipientsField ::= RecipientsSpecifier

-- Campo de encabezamiento MIP contestado
RepliedToIPMField ::= IPMIdentifier

-- Campo de encabezamiento MIP obsoleto
ObsoletedIPMsField ::= SEQUENCE OF ObsoletedIPMsSubfield
ObsoletedIPMsSubfield ::= IPMIdentifier

-- Campo de encabezamiento MIP conexos
RelatedIPMsField ::= SEQUENCE OF RelatedIPMsSubfield
RelatedIPMsSubfield ::= IPMIdentifier

-- Campo de encabezamiento asunto
SubjectField ::= TeletexString (SIZE (0. .ub-subject-field))

-- Campo de encabezamiento hora de expiración
ExpiryTimeField ::= Time

-- Campo de encabezamiento hora de respuesta
ReplyTimeField ::= Time

-- Campo de encabezamiento destinatarios de respuesta
ReplyRecipientsField ::= SEQUENCE OF ReplyRecipientsSubfield
ReplyRecipientsSubfield ::= ORDescriptor

-- Campo de encabezamiento importancia
ImportanceField ::= ENUMERATED {
        low             (0),
        normal          (1),
        high            (2) }
```

```
-- Campo de encabezamiento sensibilidad

SensitivityField ::= ENUMERATED {
        personal                    (1),
        private                     (2),
        company-confidential        (3) }


-- Campo de encabezamiento retransmitido automáticamente

AutoForwardedField ::= BOOLEAN


-- Campo de encabezamiento ampliaciones

ExtensionsField ::= SET OF HeadingExtension

HeadingExtension ::= SEQUENCE {
        type    OBJECT IDENTIFIER,
        value   ANY DEFINED BY type DEFAULT NULL NULL }

HEADING-EXTENSION MACRO ::=
BEGIN
                TYPE NOTATION   ::= "VALUE" type | empty
                VALUE NOTATION  ::= value (VALUE OBJECT IDENTIFIER)

END


-- Cuerpo

Body ::= SEQUENCE OF BodyPart

BodyPart ::= CHOICE {
        ia5-text                [0]  IA5TextBodyPart,
        voice                   [2]  VoiceBodyPart,
        g3-facsimile            [3]  G3FacsimileBodyPart,
        g4-class1               [4]  G4Class1BodyPart,
        teletex                 [5]  TeletexBodyPart,
        videotex                [6]  VideotextBodyPart,
        encrypted               [8]  EncryptedBodyPart,
        message                 [9]  MessageBodyPart,
        mixed-mode              [11] MixedModeBodyPart,
        bilaterally-defined     [14] BilaterallyDefinedBodyPart,
        nationally-defined      [7]  NationallyDefinedBodyPart,
        externally-defined      [15] ExternallyDefinedBodyPart }


-- Parte de cuerpo texto AI5

IA5TextBodyPart ::= SEQUENCE {
        parameters      IA5TextParameters,
        data            IA5TextData }

IA5TextParameters ::= SET {
        repertoire      [0] Repertoire DEFAULT ia5 }

IA5TextData ::= IA5String

Repertoire ::= ENUMERATED {
        ita2(2),
        ia5 (5) }


-- Parte de cuerpo voz

VoiceBodyPart ::= SEQUENCE {
        parameters      Voiceparameters,
        data            VoiceData }
```

```
VoiceParameters ::= SET -- para ulterior estudio
VoiceData ::= BIT STRING -- para ulterior estudio

-- Parte de cuerpo facsímil G3
G3FacsimileBodyPart ::= SEQUENCE {
        parameters      G3FacsimileParameters,
        data            G3FacsimileData }
G3FacsimileParameters ::= SET {
        number-of-pages         [0]  INTEGER OPTIONAL,
        non-basic-parameters    [1]  G3FacsimileNonBasicParameters OPTIONAL }
G3FacsimileData ::= SEQUENCE OF BIT STRING

-- Partes de cuerpo G4 clase 1 y modo mixto
G4Class1BodyPart ::= SEQUENCE OF ProtocolElement
MixedModeBodyPart ::= SEQUENCE OF ProtocolElement

-- Partes de cuerpo teletex
TeletexBodyPart ::= SEQUENCE {
        parameters      TeletexParameters,
        data            TeletexData }
TeletexParameters ::= SET {
        number-of-pages         [0]  INTEGER OPTIONAL,
        telex-compatible        [1]  BOOLEAN DEFAULT FALSE,
        non-basic-parameters    [2]  TeletexNonBasicParameters OPTIONAL }
TeletexData ::= SEQUENCE OF TeletexString

-- Parte de cuerpo videotex
VideotexBodyPart ::= SEQUENCE {
        parameters      VideotexParameters,
        data            VideotexData }
VideotexParameters ::= SET {
        syntax          [0] VideotexSyntax OPTIONAL }
VideotexSyntax ::= INTEGER {
        ids                     (0),
        data-syntax1            (1),
        data-syntax2            (2),
        data-syntax3            (3) }
VideotexData ::= VideotexString

-- Parte de cuerpo cifrado
EncryptedBodyPart ::= SEQUENCE {
        parameters      EncryptedParameters,
        data            EncryptedData }
EncryptedParameters ::= SET -- para ulterior estudio
EncryptedData ::= BIT STRING -- para ulterior estudio

-- Parte de cuerpo mensaje
MessageBodyPart ::= SEQUENCE {
        parameters      MessageParameters,
        data            MessageData }
```

```
MessageParameters ::= SET{
        delivery-time           [0]  MessageDeliveryTime OPTIONAL,
        delivery-envelope       [1]  OtherMessageDeliveryFields OPTIONAL}

MessageData ::= IPM


-- Parte de cuerpo definido bilateralmente

BilaterallyDefinedBodyPart ::= OCTET STRING


-- Parte de cuerpo definido nacionalmente

NationallyDefinedBodyPart ::= ANY


-- Parte de cuerpo definido externamente

ExternallyDefinedBodyPart ::= SEQUENCE{
        parameters [0] ExternallyDefinedParameters OPTIONAL,
        data           ExternallyDefinedData}

ExternallyDefinedParameters ::= EXTERNAL

ExternallyDefinedData ::= EXTERNAL

EXTENDED-BODY-PART-TYPE MACRO ::=
BEGIN
        TYPE NOTATION           ::= Parameters Data
        VALUE NOTATION          ::= value (VALUE OBJECT IDENTIFIER)

        Parameters              ::= "PARAMETERS" type "IDENTIFIED" "BY" value (OBJECT
                                    IDENTIFIER) | empty
        Data                    ::= "DATA" type

END

-- NIP

IPN ::= SET{
        -- common-fields -- COMPONENTS OF CommonFields,
        choice [0] CHOICE{
                non-receipt-fields      [0] NonReceiptFields,
                receipt-fields          [1] ReceiptFields}}

RN ::= IPN -- con campos de recepción elegidos

NRN ::= IPN -- con campos de no recepción elegidos

CommonFields ::= SET{
        subject-ipm                 SubjectIPMField,
        ipn-originator          [1] IPNOriginatorField OPTIONAL,
        ipm-preferred-recipient [2] IPMPreferredRecipientField OPTIONAL,
        conversion-eits             ConversionEITsField OPTIONAL}

NonReceiptFields ::= SET{
        non-receipt-reason      [0] NonReceiptReasonField,
        discard-reason          [1] DiscardReasonField OPTIONAL,
        auto-forward-comment    [2] AutoForwardCommentField OPTIONAL,
        returned-ipm            [3] ReturnedIPMField OPTIONAL}

ReceiptFields ::= SET{
        receipt-time            [0] ReceiptTimeField,
        acknowledgment-mode     [1] AcknowledgmentModeField DEFAULT manual,
        suppl-receipt-info      [2] SupplReceiptInfoField DEFAULT " "}


-- Campos comunes

SubjectIPMField ::= IPMIdentifier

IPNOriginatorField ::= ORDescriptor

IPMPreferredRecipientField ::= ORDescriptor

ConversionEITsField ::= EncodedInformationTypes
```

```
-- Campos de no recepción

NonReceiptReasonField ::= ENUMERATED {
        ipm-discarded           (0),
        ipm-auto-forwarded      (1) }

DiscardReasonField ::= ENUMERATED {
        ipm-expired                     (0),
        ipm-obsoleted                   (1),
        user-subscription-terminated    (2) }

AutoForwardCommentField ::= AutoForwardComment

AutoForwardComment ::= PrintableString
        (SIZE (0. .ub-auto-forward-comment))

ReturnedIPMField ::= IPM


-- Campos de recepción

ReceiptTimeField ::= Time

AcknowledgmentModeField ::= ENUMERATED {
        manual          (0),
        automatic       (1) }

SupplReceiptInfoField ::= SupplementaryInformation


-- Realización de almacenamiento de mensajes

ForwardedInfo ::= SET {
        auto-forwarding-comment [0]
                AutoForwardComment OPTIONAL,
        cover-note [1]
                IA5TextBody Part OPTIONAL,
        this-ipm-prefix [2]
                PrintableString (SIZE (1. .ub-ipm-identifier-suffix))
                    OPTIONAL }

END  -- de ObjetosdeInformación SMIP
```

ANEXO F

(a la Recomendación X.420)

Definición de referencia de objetos funcionales

Este anexo forma parte integrante de esta Recomendación.

Este anexo que es un suplemento a los § 10, 11 y 16, define con fines de referencia los objetos funcionales de mensajería interpersonal. Utiliza las macros OBJECT y REFINE de la Recomendación X.407.

```
IPMSFunctionalObjects { joint-iso-ccitt
        mhs-motis(6) ipms(1) modules(0) functional-objects(1) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
--Prólogo
--Exporta todo

IMPORTS
        -- Servicio abstracto SMIP
                management, origination, reception
                ----
                FROM IPMSAbstractService { joint-iso-ccitt
                    mhs-motis(6) ipms(1) modules(0) abstract-service(3) }

        -- Identificadores de objeto SMIP
                id-ot-ipme, id-ot-ipms, id-ot-ipms-ms, id-ot-ipms-ua,
                id-ot-ipms-user, id-ot-pdau, id-ot-tlma, id-ot-tlxau,
                id-ref-primary, id-ref-secondary
                ----
                FROM IPMSObjectidentifiers { joint-iso-ccitt
                    mhs-motis(6) ipms(1) modules(0) object-identifiers(0) }

        -- Servicio abstracto ATLM
                miscellanea
                ----
                FROM TLMAAbsService { ccitt
                    recommendation(0) t(20) 330 tlmaabsservice(0) }

        -- Servicio abstracto AM
                retrieval
                ----
                FROM MSAbstractService { joint-iso-ccitt
                    mhs-motis(6) ms(4) modules(0) abstract-service(1) }

        -- Servicio abstracto STRM
                administration, delivery, mTs, submission
                ----
                FROM MTSAbstractService { joint-iso-ccitt
                    mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

        -- Convenios de definición del servicio abstracto
                OBJECT, REFINE
                ----
                FROM AbstractServiceNotation { joint-iso-ccitt
                    mhs-motis(6) asdc(2) modules(0) notation(1) };


-- Tipo de objeto «Raíz»

ipme OBJECT
        ::= id-ot-ipme


-- Perfeccionamiento primario

ipme-refinement REFINE ipme AS
        ipms
                origination     [S] PAIRED WITH ipms-user
                reception       [S] PAIRED WITH ipms-user
                management      [S] PAIRED WITH ipms-user
        ipms-user RECURRING
        ::= id-ref-primary


-- Tipos de objeto primario

ipms-user OBJECT
        PORTS {
                origination     [C],
                reception       [C],
                management      [C] }
        ::= id-ot-ipms-user
```

```
ipms OBJECT
        PORTS {
                origination     [S],
                reception       [S],
                management      [S] }
        ::= id-ot-ipms


-- Perfeccionamiento secundario

ipms-refinement REFINE ipms AS
        mTs
                submission      [S] PAIRED WITH ipms-ua, ipms-ms
                delivery        [S] PAIRED WITH ipms-ua, ipms-ms
                administration  [S] PAIRED WITH ipms-ua, ipms-ms
        ipms-ua RECURRING
                origination     [S] VISIBLE
                reception       [S] VISIBLE
                management      [S] VISIBLE
        ipms-ms RECURRING
                submission      [S] PAIRED WITH ipms-ua
                retrieval       [S] PAIRED WITH ipms-ua
                administration  [S] PAIRED WITH ipms-ua
        tlma RECURRING
                origination     [S] VISIBLE
                reception       [S] VISIBLE
                management      [S] VISIBLE
        tlxau RECURRING
                origination     [S] VISIBLE
                reception       [S] VISIBLE
                management      [S] VISIBLE
        pdau RECURRING
                reception       [S] VISIBLE
        ::= id-ref-secondary


-- Objetos secundarios

ipms-ua OBJECT
        PORTS {
                origination     [S],
                reception       [S],
                management      [S],
                submission      [C],
                delivery        [C],
                retrieval       [C],
                administration  [C] }
        ::= id-ot-ipms-ua

ipms-ms OBJECT
        PORTS {
                submission      [S],
                retrieval       [S],
                administration  [S],
                submission      [C],
                delivery        [C],
                administration  [C] }
        ::= id-ot-ipms-ms

tlma OBJECT
        PORTS {
                origination     [S],
                reception       [S],
                management      [S],
                miscellanea     [S] }
        ::= id-ot-tlma
```

```
tlxau OBJECT
        PORTS {
                origination     [S],
                reception       [S],
                management      [S] }
        ::= id-ot-tlxau

pdau OBJECT
        PORTS {
                reception       [S] }
        ::= id-ot-pdau

END  -- de ObjetosFuncionalesSMIP
```

ANEXO G

(a la Recomendación X.420)

Definición de referencia de servicio abstracto

Este anexo forma parte integrante de esta Recomendación.

Este anexo, que es un suplemento a los § 12 y 13, define con fines de referencia el servicio abstracto SMIP. Utiliza las macros PORT, ABSTRACT-OPERATION y ABSTRACT-ERROR de la Recomendación X.407.

```
IPMSAbstractService { joint-iso-ccitt
        mhs-motis(6) ipms(1) modules(0) abstract-service(3) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


--Prólogo
--Exporta todo

IMPORTS
        -- Objetos de información SMTP
                AutoForwardComment, Heading, IPM, NRN, RN
                ----
                FROM IPMSInformationObjects { joint-iso-ccitt
                    mhs-motis(6) ipms(1) modules(0) information-objects(2) }

        -- Identificadores de objeto SMIP
                id-pt-management, id-pt-origination, id-pt-reception
                ----
                FROM IPMSObjectIdentifiers { joint-iso-ccitt
                    mhs-motis(6) ipms(1) modules(0) object-identifiers(0) }

        -- Servicio abstracto STRM
                MessageDeliveryEnvelope, MessageSubmissionEnvelope,
                MessageSubmissionIdentifier, MessageSubmissionTime,
                ProbeSubmissionEnvelope, ProbeSubmissionIdentifier,
                ProbeSubmissionTime, RecipientImproperlySpecified,
                ReportDeliveryEnvelope,
                ----
                FROM MTSAbstractService { joint-iso-ccitt
                    mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }

        -- Convenios de definición del servicio abstracto
                ABSTRACT-ERROR, ABSTRACT-OPERATION, PORT
                ----
                FROM AbstractServiceNotation { joint-iso-ccitt
                    mhs-motis(6) asdc(2) modules(0) notation(1) };

Time ::= UTCTime
```

```
-- Puertos

origination PORT
        CONSUMER INVOKES {
                OriginateProbe,
                OriginateIPM,
                OriginateRN }
        ::= id-pt-origination

reception PORT
        SUPPLIER INVOKES {
                ReceiveReport,
                ReceiveIPM,
                ReceiveRN,
                ReceiveNRN }
        ::= id-pt-reception

management PORT
        CONSUMER INVOKES {
                ChangeAutoDiscard,
                ChangeAutoAcknowledgment,
                ChangeAutoForwarding }
        ::= id-pt-management


-- Operaciones abstractas de generación

OriginateProbe ::= ABSTRACT-OPERATION
        ARGUMENT SET {
                envelope   [0] ProbeSubmissionEnvelope,
                content    [0] IPM }
        RESULT SET {
                submission-identifier [0] ProbeSubmissionIdentifier,
                submission-time       [1] ProbeSubmissionTime }
        ERRORS {
                SubscriptionError,
                RecipientImproperlySpecified }

OriginateIPM ::= ABSTRACT-OPERATION
        ARGUMENT SET {
                envelope   [0] MessageSubmissionEnvelope,
                content    [0] IPM }
        RESULT SET {
                submission-identifier [0] MessageSubmissionIdentifier,
                submission-time       [1] MessageSubmissionTime }
        ERRORS {
                SubscriptionError,
                RecipientImproperlySpecified }

OriginateRN ::= ABSTRACT-OPERATION
        ARGUMENT SET {
                envelope   [0] MessageSubmissionEnvelope,
                content    [0] RN }
        RESULT SET {
                submission-identifier [0] MessageSubmissionIdentifier,
                submission-time       [1] MessageSubmissionTime }
        ERRORS {
                SubscriptionError,
                RecipientImproperlySpecified }


-- Operaciones abstractas de recepción

ReceiveReport ::= ABSTRACT-OPERATION
        ARGUMENT SET {
                envelope           [0] ReportDeliveryEnvelope,
                undelivered-object [1] InformationObject OPTIONAL }
        RESULT
        ERRORS { }
```

```
ReceiveIPM ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                envelope   [0] MessageDeliveryEnvelope,
                content    [1] IPM }
        RESULT
        ERRORS {}

ReceiveRN ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                envelope   [0] MessageDeliveryEnvelope,
                content    [1] RN }
        RESULT
        ERRORS {}

ReceiveNRN ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                envelope   [0] MessageDeliveryEnvelope,
                content    [1] NRN }
        RESULT
        ERRORS {}


-- Operaciones abstractas de gestión

ChangeAutoDiscard ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                auto-discard-expired-IPMs          [0] BOOLEAN,
                auto-discard-obsolete-IPMs         [1] BOOLEAN}
        RESULT
        ERRORS {}

ChangeAutoAcknowledgment ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                auto-acknowledge-IPMs [0] BOOLEAN
                auto-acknowledge-suppl-receipt-info [1]
                    SupplementaryInformation }
        RESULT
        ERRORS{
                SubcriptionError }

ChangeAutoForwarding ::= ABSTRACT-OPERATION
        ARGUMENT SET{
                auto-forward-IPMs          [0] BOOLEAN,
                auto-forward-recipients    [1] SEQUENCE OF ORName OPTIONAL,
                auto-forward-heading       [2] Heading OPTIONAL,
                auto-forward-comment       [3] AutoForwardComment OPTIONAL }
        RESULT
        ERRORS{
                SubcriptionError,
                RecipientImproperlySpecified }


-- Errores abstractos

SubscriptionError ::= ABSTRACT-ERROR
        PARAMETER SET{
                problem    [0] SubscriptionProblem }

SubscriptionProblem ::= ENUMERATED{
        ipms-eos-not-subscribed          (0),
        mts-eos-not-subscribed           (1) }

END  -- de ServicioAbstractoSMIP
```

ANEXO H

(a la Recomendación X.420)

Definición de referencia de ampliaciones de encabezamiento

Este anexo forma parte integrante de esta Recomendación.

Este anexo, que constituye un suplemento al anexo A, define con fines de referencia las ampliaciones de encabezamiento definidas para mensajería interpersonal. Utiliza la macro HEADING-EXTENSION del § 12.2.17.

```
IPMSHeadingExtensions { joint-iso-ccitt
    mhs-motis(6) ipms(1) modules(0) heading-extensions(6) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo

IMPORTS
    -- Objetos de información SMIP
        HEADING-EXTENSION
        ----
        FROM IPMSInformationObjects { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) information-objects(2) };

    -- Identificadores de objeto SMIP
        id-hex-incomplete-copy, id-hex-languages
        ----
        FROM IPMSObjectIdentifiers { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) object-identifiers(0) };


-- Copia incompleta

incomplete-copy HEADING-EXTENSION
    ::= id-hex-incomplete-copy

IncompleteCopy ::= NULL


-- Idiomas

languages HEADING-EXTENSION
    VALUE SET OF Language
    ::= id-hex-languages

Language ::= PrintableString (SIZE (2..2))

END  -- de AmpliacionesdeEncabezamientoSMIP
```

ANEXO I

(a la Recomendación X.420)

Definición de referencia de tipos de parte de cuerpo ampliado

Este anexo forma parte integrante de esta Recomendación.

Este anexo, que es un suplemento al anexo B, define con fines de referencia ciertos tipos de parte de cuerpo ampliado.

```
IPMSExtendedBodyPartTypes { joint-iso-ccitt
    mhs-motis(6) ipms(1) modules(0) extended-body-part-types(7) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo

IMPORTS
    -- Objetos de información SMIP
        BilaterallyDefinedBodyPart, EncryptedData,
        EncryptedParameters, EXTENDED-BODY-PART-TYPE, G3FacsimileData,
        G3FacsimileParameters, G4Class1BodyPart, IA5TextData,
        IA5TextParameters, MessageData, MessageParameters,
        MixedModeBodyPart, NationallyDefinedBodyPart, TeletexData,
        TeletexParameters, VideotexData, VideotexParameters,
        VoiceData, VoiceParameters
        ----
        FROM IPMSInformationObjects { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) information-objects(2) }

    -- Identificadores de objeto SMIP
        id-ep-encrypted,
        id-ep-g3-facsimile,
        id-ep-ia5-text,
        id-ep-message,
        id-ep-teletex,
        id-ep-videotex,
        id-ep-voice,
        id-et-bilaterally-defined, id-et-encrypted id-et-g3-facsimile,
        id-et-g4-class1, id-et-ia5-text, id-et-message,
        id-et-mixed-mode, id-et-nationally-defined, id-et-teletex,
        id-et-videotex, id-et-voice
        ----
        FROM IPMSObjectIdentifiers { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) object-identifiers(0) };


-- Parte de cuerpo ampliado texto AI5

ia5-text-body-part EXTENDED-BODY-PART-TYPE
    PARAMETERS  IA5TextParameters IDENTIFIED BY id-ep-ia5-text
    DATA        IA5TextData
    ::= id-et-ia5-text


-- Parte de cuerpo ampliado voz

voice-body-part EXTENDED-BODY-PART-TYPE
    PARAMETERS  VoiceParameters IDENTIFIED BY id-ep-voice
    DATA        VoiceData
    ::= id-et-voice
```

```
-- Parte de cuerpo ampliado facsímil G3

g3-facsimile-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  G3FacsimileParameters IDENTIFIED BY id-ep-g3-facsimile
        DATA        G3FacsimileData
        ::= id-et-g3-facsimile


-- Parte de cuerpo ampliado G4 clase 1

g4-class1-body-part EXTENDED-BODY-PART-TYPE
        DATA        G4Class1BodyPart
        ::= id-et-g4-class1


-- Parte de cuerpo ampliado teletex

teletex-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  TeletexParameters IDENTIFIED BY id-ep-teletex
        DATA        TeletexData
        ::= id-et-teletex


-- Parte de cuerpo ampliado videotex

videotex-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  VideotexParameters IDENTIFIED BY id-ep-videotex
        DATA        VideotexData
        ::= id-et-videotex


-- Parte de cuerpo ampliado cifrado

encrypted-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  EncryptedParameters IDENTIFIED BY id-ep-encrypted
        DATA        EncryptedData
        ::= id-et-encrypted


-- Parte de cuerpo ampliado mensaje

message-body-part EXTENDED-BODY-PART-TYPE
        PARAMETERS  MessageParameters IDENTIFIED BY id-ep-message
        DATA        MessageData
        ::= id-et-message


-- Parte de cuerpo ampliado modo mixto

mixed-mode-body-part EXTENDED-BODY-PART-TYPE
        DATA MixedModeBodyPart
        ::= id-et-mixed-mode


-- Parte de cuerpo ampliado definido bilateralmente

bilaterally-defined-body-part EXTENDED-BODY-PART-TYPE
        DATA BilaterallyDefinedBodyPart
        ::= id-et-bilaterally-defined


-- Parte de cuerpo ampliado definido nacionalmente

nationally-defined-body-part EXTENDED-BODY-PART-TYPE
        DATA NationallyDefinedBodyPart
        ::= id-et-nationally-defined

END  -- de TiposDeParteDeCuerpoAmpliadoSMIP
```

ANEXO J

(a la Recomendación X.420)

Definición de referencia de atributos de almacenamiento de mensajes

Este anexo forma parte integrante de esta Recomendación.

Este anexo, que es un suplemento al anexo C, define con fines de referencia los atributos de AM específicos a mensajería interpersonal. Utiliza la macro ATRIBUTE de la Recomendación X.500.

```
IPMSMessageStoreAttributes { joint-iso-ccitt
    mhs-motis(6) ipms(1) modules(0) message-store-attributes(8) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo.

IMPORTS
    -- Ampliaciones de encabezamiento SMIP
        IncompleteCopy, Language
        ----
        FROM IPMSHeadingExtensions { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) heading-extensions(6) }

    -- Objetos de información SMIP
        AcknowledgmentModeField, AuthorizingUsersSubfield,
        AutoForwardCommentField, AutoForwardedField,
        BilaterallyDefinedBodyPart, BlindCopyRecipientsSubfield, Body,
        ConversionEITsField, CopyRecipientsSubfield,
        DiscardReasonField, EncryptedBodyPart, EncryptedData,
        EncryptedParameters, ExpiryTimeField,
        ExternallyDefinedParameters, G3FacsimileBodyPart,
        G3FacsimileData, G3FacsimileParameters, G4Class1BodyPart,
        Heading, IA5TextBodyPart, IA5TextData, IA5TextParameters,
        ImportanceField, IPMPreferredRecipientField,
        IPNOriginatorField, MessageBodyPart, MessageData,
        MessageParameters, MixedModeBodyPart,
        NationallyDefinedBodyPart, NonReceiptReasonField,
        ObsoletedIPMsSubfield, ORDescriptor, OriginatorField,
        PrimaryRecipientsSubfield, ReceiptTimeField,
        RelatedIPMsSubfield, RepliedToIPMField,
        ReplyRecipientsSubfield, ReplyTimeField, ReturnedIPMField,
        SensitivityField, SubjectField, SubjectIPMField,
        SupplReceiptInfoField, TeletexBodyPart, TeletexData,
        TeletexParameters, ThisIPMField, VideotexBodyPart,
        VideotexData, VideotexParameters, VoiceBodyPart, VoiceData,
        VoiceParameters
        ----
        FROM IPMSInformationObjects { joint-iso-ccitt
            mhs-motis(6) ipms(1) modules(0) information-objects(2) }

    -- Identificadores de objeto SMIP
        id-bat-bilaterally-defined-body-parts, id-bat-body,
        id-bat-encrypted-body-parts, id-bat-encrypted-data,
        id-bat-encrypted-parameters, id-bat-extended-body-part-types
        id-bat-g3-facsimile-body-parts, id-bat-g3-facsimile-data,
        id-bat-g3-facsimile-parameters, id-bat-g4-class1-body-parts
        id-bat-ia5-text-body-parts, id-bat-ia5-text-data,
        id-bat-ia5-text-parameters, id-bat-message-body-parts,
        id-bat-message-data, id-bat-message-parameters,
        id-bat-mixed-mode-body-parts,
        id-bat-nationally-defined-body-parts,
```

```
                id-bat-teletex-body-parts, id-bat-teletex-data,
                id-bat-teletex-parameters, id-bat-videotex-body-parts,
                id-bat-videotex-data, id-bat-videotex-parameters,
                id-bat-voice-body-parts, id-bat-voice-data,
                id-bat-voice-parameters, id-hat-authorizing-users,
                id-hat-auto-forwarded, id-hat-blind-copy-recipients,
                id-hat-copy-recipients, id-hat-expiry-time, id-hat-heading,
                id-hat-importance, id-hat-incomplete-copy, id-hat-languages,
                id-hat-nrn-requestors, id-hat-obsoleted-IPMs,
                id-hat-originator, id-hat-primary-recipients
                id-hat-related-IPMs, id-hat-replied-to-IPM,
                id-hat-reply-recipients, id-hat-reply-requestors,
                id-hat-reply-time, id-hat-rn-requestors, id-hat-sensitivity,
                id-hat-subject, id-hat-this-ipm, id-nat-acknowledgment-mode,
                id-nat-auto-forward-comment, id-nat-conversion-eits,
                id-nat-discard-reason, id-nat-ipm-preferred-recipient,
                id-nat-ipn-originator, id-nat-non-receipt-reason,
                id-nat-receipt-time, id-nat-returned-ipm, id-nat-subject-ipm,
                id-nat-suppl-receipt-info, id-sat-ipm-entry-type,
                id-sat-ipm-synopsis
                ----
                FROM IPMSObjectIdentifiers { joint-iso-ccitt
                    mhs-motis(6) ipms(1) modules(0) object-identifiers(0) }

        -- Servicio abstracto AM
                MS-EITs, SequenceNumber
                ----
                FROM MSAbstractService { joint-iso-ccitt
                    mhs-motis(6) ms(4) modules(0) abstract-service(1) }

        -- Servicio abstracto STRM
                EncodedInformationTypes
                ----
                FROM MTSAbstractService { joint-iso-ccitt
                    mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) };

        -- Marco de información de guía
                ATTRIBUTE
                ----
                FROM InformationFramework { joint-iso-ccitt
                    ds(5) modules(1) informationFramework(1) };

Time ::= UTCTime


-- ATRIBUTOS RESUMEN

-- Tipo de inscripción MIP

ipm-entry-type ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMEntryType
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-sat-ipm-entry-type

IPMEntryType ::= ENUMERATED {
        ipm     (0),
        rn      (1),
        nrn     (2) }


-- Sinopsis MIP

ipm-synopsis ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMSynopsis
        SINGLE VALUE
        ::= id-sat-ipm-synopsis
```

```
IPMSynopsis ::= SEQUENCE OF BodyPartSynopsis

BodyPartSynopsis ::= CHOICE {
        messsage        [0] MessageBodyPartSynopsis,
        non-messsage    [1] NonMessageBodyPartSynopsis }

MessageBodyPartSynopsis ::= SEQUENCE {
        number          [0] SequenceNumber,
        synopsis        [1] IPMSynopsis }

NonMessageBodyPartSynopsis ::= SEQUENCE {
        type            [0] OBJECT IDENTIFIER,
        parameters      [1] ExternallyDefinedParameters,
        size            [2] INTEGER,
        processed       [3] BOOLEAN DEFAULT FALSE }


-- ATRIBUTOS DE ENCABEZAMIENTO

-- Encabezamiento

heading ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Heading
        SINGLE VALUE
        ::= id-hat-heading


-- Análisis de encabezamiento

rn-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-rn-requestors

nrn-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-nrn-requestors

reply-requestors ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ORDescriptor
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-reply-requestors


-- Campos de encabezamiento

this-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ThisIPMField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-this-ipm

originator ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OriginatorField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-originator

replied-to-IPM ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RepliedToIPMField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-replied-to-IPM
```

```
subject ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-hat-subject

expiry-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ExpiryTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-hat-expiry-time

reply-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReplyTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-hat-reply-time

importance ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ImportanceField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-importance

sensitivity ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SensitivityField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-sensitivity

auto-forwarded ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AutoForwardedField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-auto-forward


-- Subcampos de encabezamiento

authorizing-users ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Authorizing-UsersSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-authorizing-users

primary-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX PrimaryRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-primary-recipients

copy-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX CopyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-copy-recipients

blind-copy-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX BlindCopyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-blind-copy-recipients

obsoleted-IPMs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ObsoletedIPMsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-obsoleted-IPMs
```

```
related-IPMs ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX RelatedIPMsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-related-IPMs

reply-recipients ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReplyRecipientsSubfield
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-reply-recipients


-- Ampliaciones de encabezamiento

incomplete-copy ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IncompleteCopy
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-hat-incomplete-copy

languages ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Language
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-hat-languages


-- ATRIBUTOS DE CUERPO

-- Cuerpo

body ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Body
        SINGLE VALUE
        ::= id-bat-body


-- Partes de cuerpo básico

ia5-text-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IA5TextBodyPart
        MULTI VALUE
        ::= id-bat-ia5-text-body-parts

voice-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VoiceBodyPart
        MULTI VALUE
        ::= id-bat-voice-body-parts

g3-facsimile-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G3FacsimileBodyPart
        MULTI VALUE
        ::= id-bat-g3-facsimile-body-parts

g4-class1-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G4Class1BodyPart
        MULTI VALUE
        ::= id-bat-g4-class1-body-parts

teletex-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX TeletexBodyPart
        MULTI VALUE
        ::= id-bat-teletex-body-parts
```

```
videotex-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VideotexBodyPart
        MULTI VALUE
        ::= id-bat-videotex-body-parts

encrypted-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EncryptedBodyPart
        MULTI VALUE
        ::= id-bat-encrypted-body-parts

message-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SequenceNumber
        MULTI VALUE
        ::= id-bat-message-body-parts

mixed-mode-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MixedModeBodyPart
        MULTI VALUE
        ::= id-bat-mixed-mode-body-parts

bilaterally-defined-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX BilaterallyDefinedBodyPart
        MULTI VALUE
        ::= id-bat-bilaterally-defined-body-parts

nationally-defined-body-parts ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX NationallyDefinedBodyPart
        MULTI VALUE
        ::= id-bat-nationally-defined-body-parts


-- Componentes parámetros de parte de cuerpo básico

ia5-text-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IA5TextParameters
        MULTI VALUE
        ::= id-bat-ia5-text-parameters

voice-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VoiceParameters
        MULTI VALUE
        ::= id-bat-voice-parameters

g3-facsimile-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G3FacsimileParameters
        MULTI VALUE
        ::= id-bat-g3-facsimile-parameters

teletex-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX TeletexParameters
        MULTI VALUE
        ::= id-bat-teletex-parameters

videotex-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VideotexParameters
        MULTI VALUE
        ::= id-bat-videotex-parameters

encrypted-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EncryptedParameters
        MULTI VALUE
        ::= id-bat-encrypted-parameters

message-parameters ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageParameters
        MULTI VALUE
        ::= id-bat-message-parameters
```

```
-- Componentes datos de parte de cuerpo básico

ia5-text-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IA5TextData
        MULTI VALUE
        ::= id-bat-ia5-text-data

voice-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX Voice-Data
        MULTI VALUE
        ::= id-bat-voice-data

g3-facsimile-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX G3FacsimileData
        MULTI VALUE
        ::= id-bat-g3-facsimile-data

teletex-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX TeletexData
        MULTI VALUE
        ::= id-bat-teletex-data

videotex-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX VideotexData
        MULTI VALUE
        ::= id-bat-videotex-data

encrypted-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX EncryptedData
        MULTI VALUE
        ::= id-bat-encrypted-data

message-data ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MessageData
        MULTI VALUE
        ::= id-bat-message-data


-- Tipos de parte de cuerpo ampliado

extended-body-part-types ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX OBJECT IDENTIFIER
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-bat-extended-body-part-types


-- Partes de cuerpo ampliado

-- (Estos atributos no pueden enumerarse. Véase el § C.3.6)

-- ATRIBUTOS DE NOTIFICACIÓN

-- Campos comunes

subject-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SubjectIPMField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-subject-ipm

ipn-originator ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPNOriginatorField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-ipn-originator

ipm-preferred-recipient ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX IPMPreferredRecipientField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-ipm-preferred-recipient
```

```
conversion-eits ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX MS-EITs
        MATCHES FOR EQUALITY
        MULTI VALUE
        ::= id-nat-conversion-eits


-- Campos de no recepción

non-receipt-reason ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX NonReceiptReasonField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-non-receipt-reason

discard-reason ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX DiscardReasonField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-discard-reason

auto-forward-comment ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AutoForwardCommentField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-auto-forward-comment

returned-ipm ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReturnedIPMField
        SINGLE VALUE
        ::= id-nat-returned-IPM


-- Receipt fields

receipt-time ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX ReceiptTimeField
        MATCHES FOR EQUALITY ORDERING
        SINGLE VALUE
        ::= id-nat-receipt-time

acknowledgment-mode ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX AcknowledgmentModeField
        MATCHES FOR EQUALITY
        SINGLE VALUE
        ::= id-nat-acknowledgment-mode

suppl-receipt-info ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX SupplReceiptInfoField
        MATCHES FOR EQUALITY SUBSTRINGS
        SINGLE VALUE
        ::= id-nat-suppl-receipt-info

END -- of IPMSMessageStoreAttributes
```

ANEXO K

(a la Recomendación X.420)

Definición de referencia de límites superiores

Este anexo forma parte integrante de esta Recomendación pero no forma parte integrante de la Norma Internacional ISO correspondiente.

Este anexo define, con fines de referencia, los límites superiores de diversos ítems de información de longitud variable cuyas sintaxis están definidas en los módulos NSA.1 de anexos anteriores.

```
IPMSUpperBounds { joint-iso-ccitt
    mhs-motis(6) ipms(1) modules(0) upper-bounds(10) }
DEFINITIONS IMPLICIT TAGS ::=
BEGIN


-- Prólogo
-- Exporta todo.

IMPORTS -- nada --;


-- Límites superiores.

ub-auto-forward-comment   INTEGER ::= 256

ub-free-form-name         INTEGER ::= 64

ub-ipm-identifier-suffix  INTEGER ::= 2

ub-local-ipm-identifier   INTEGER ::= 64

ub-subject-field          INTEGER ::= 128

ub-telephone-number       INTEGER ::= 32


END -- of IPMSUpperBounds
```

ANEXO L

(a la Recomendación X.420)

Sustentación del servicio de mensajería interpersonal

Este anexo forma parte integrante de esta Recomendación.

El servicio de mensajería interpersonal proporcionado por el SMIP a los usuarios se define en términos no técnicos en la Recomendación X.400. El servicio comprende cierto número de elementos de servicio (**EDS MIP**), cada uno de los cuales representa un aspecto del servicio, y está definido en uno o dos párrafos de texto ordinario. El presente anexo indica con detalle cómo la presente especificación, más técnica, realiza cada EDS MIP. De manera equivalente, el anexo identifica los aspectos de la especificación que un AU, por ejemplo, tiene que establecer para que pueda decirse del mismo que admite un EDS MIP determinado.

Asociados con cada EDS MIP hay uno o más elementos de información que pueden aparecer como componentes de MIP. El elemento de información asociado con el EDS MIP indicación de sensibilidad, por ejemplo, es el campo de encabezamiento sensibilidad. Se dice que un AU, ATLM, o UA admite un determinado EDS MIP en la generación o recepción si y solo si admite en la generación o recepción (véase el § 22.1) los elementos de información asociados con ese EDS MIP.

Nota 1 – La tarea de realizar un EDS MIP puede incumbir, en principio a cualquiera de los objetos secundarios obtenidos mediante el perfeccionamiento del SMIP. En el presente contexto, sin embargo, se supone que el STRM y cada AM, por el hecho de ser independientes de la aplicación, admiten todo EDS MIP, y que proceden de esta manera sin haber tomado disposiciones especiales acerca de los mismos.

Nota 2 – Como se describe en el § 14, un AU pone a disposición de su usuario muchas de las capacidades que ofrece su AM. Estas capacidades realizan los elementos del servicio de extracción de mensajes que se define en la Recomendación X.400. La correspondencia entre los elementos de ese servicio y las capacidades técnicas asociadas se especifica en la Recomendación X.413.

Nota 3 – Como se describe en el § 14, un AU pone a disposición de su usuario muchas de las capacidades que ofrece el STRM. Estas capacidades realizan los elementos del servicio de transferencia de mensajes que se define en la Recomendación X.400. La correspondencia entre los elementos de ese servicio y las capacidades técnicas asociadas se especifican en la Recomendación X.411.

L.1 *Sustentación de componentes de especificador de destinatario*

Algunos EDS MIP se realizan por medio de componentes especificador de destinatario. Los EDS MIP de esta categoría se indican en la primera columna del cuadro L-1/X.420. La segunda y tercera columnas identifican el componente especificador de destinatario, y el valor de ese componente, que son los elementos de información asociados con cada EDS MIP que figura en la lista.

CUADRO L-1/X.420

Sustentación de componentes especificador de destinatario

Elemento de servicio	Componente especificador de destinatario	Valor
Petición de notificación de no recepción	Peticiones de notificación	nnr
Indicación de petición de notificación de recepción	Peticiones de notificación	nr
Indicación de petición de respuesta (véase también el cuadro L-2/X.420)	Respuesta solicitada	verdadero

Nota 1 – Los especificadores de destinatario aparecen como subcampos de los campos de encabezamiento destinatarios primarios, destinatarios de copia, y destinatarios de copia ciega.

Nota 2 – Cada EDS MIP, excepto indicación de petición de respuesta, pertenece únicamente a una categoría. El EDS MIP indicación de petición de respuesta pertenece a dos categorías, como se indica en el cuadro.

L.2 *Sustentación de campos de encabezamiento*

Algunos EDS MIP se realizan por medio de campos de encabezamiento. Los EDS MIP de esta categoría se indican en la primera columna del cuadro L-2/X.420. La segunda columna indica los campos de encabezamiento que son los elementos de información asociados con cada EDS MIP que figura en la lista. En el caso del campo ampliaciones, la segunda columna indica también, entre paréntesis, la ampliación de encabezamiento correspondiente.

L.3 *Sustentación de aspectos de cuerpo*

Algunos EDS MIP se realizan por medio de aspectos del cuerpo. Los EDS MIP de esta categoría se indican en la primera columna del cuadro L-3/X.420. La segunda columna indica el aspecto del cuerpo que es el elemento de información asociado con cada EDS MIP que figura en la lista.

CUADRO L-2/X.420

Sustentación de campos de encabezamiento

Elemento de servicio	Campo de encabezamiento
Indicación de usuarios autorizantes	Usuarios autorizantes
Indicación de retransmitido automáticamente	Retransmitido automáticamente
Indicación de destinatario de copia ciega	Destinatarios de copia ciega
Indicación de referencia recíproca	MIP relacionado
Indicación de fecha de expiración	Hora de expiración
Indicación de importancia	Importancia
Identificación de mensaje IP	Este MIP
Indicación de copia incompleta	Ampliaciones (copia incompleta)
Indicación de idioma	Ampliaciones (idiomas)
Indicación de Obsoleto	MIP Obsoletos
Indicación de Originador	Originador
Indicación de destinatarios primario y de copia	Destinatarios primarios Destinatarios de Copia
Indicación de petición de respuesta (véase también el cuadro L-3/X.420)	Hora de respuesta Destinatarios de respuesta
Indicación de Mensaje IP de respuesta	MIP contestado
Indicación de sensibilidad	Sensibilidad
Indicación de asunto	Asunto

Nota – Cada uno de los EDS MIP, excepto indicación de petición de respuesta, pertenece únicamente a una categoría. El EDS MIP indicación de petición de respuesta pertenece a dos categorías, como se indica en el cuadro.

CUADRO L-3/X.420

Sustentación de aspectos de cuerpo

Elemento de servicio	Aspecto de cuerpo
Indicación de cifrado de parte de cuerpo	Parte de cuerpo cifrada
Indicación de mensaje IP retransmitido	Parte de cuerpo mensaje
Cuerpo de múltiples partes	Cuerpo con dos o más partes
Cuerpo tipificado	Cuerpo (propiamente dicho)

Nota – La sustentación del EDS MIP cuerpo tipificado es intrínseca a cualquier realización de cualquier objeto secundario.

ANEXO M

Diferencias entre la Recomendación del CCITT y Norma de la ISO

Este anexo no forma parte de esta Recomendación.

Este anexo enumera todas las diferencias que existen entre esta Recomendación y la correspondiente Norma Internacional de la ISO, salvo las que son puramente redaccionales.

Las diferencias que existen son las siguientes:

a) La Norma Internacional de la ISO correspondiente a la presente Recomendación define una parte de cuerpo texto general, definición que no figura en esta Recomendación.

b) Los límites superiores del anexo K forman parte integrante de esta Recomendación, pero no forman parte integrante de la correspondiente Norma Internacional de la ISO.

c) El texto del CCITT sobre el especificador de destinatario asunto del § 8, establece que puede contener «un nombre O/D del destinatario preferido» o «un nombre O/D que aparece en la historia de ampliación de la LD». La Norma ISO ha excluido esta segunda posibilidad.

ANEXO N

Resumen de las modificaciones de la Recomendación del CCITT de 1984

Este anexo no forma parte integrante de esta Recomendación.

Desde el punto de vista de la redacción, esta Recomendación difiere sustancialmente de la Recomendación X.420 (versión de 1984). Desde el punto de vista técnico, sin embargo, las diferencias son pequeñas. El presente anexo enumera las modificaciones técnicas. Tiene por finalidad ayudar al realizador de la Recomendación X.420 (1984), permitiéndole saber, mediante una rápida ojeada, cómo su realización podría resultar afectada por la especificación de 1988.

La presente especificación recoge únicamente las siguientes modificaciones sustanciales relativas al interfuncionamiento entre los AU, AM, ATLM y UA según las versiones de 1984 y 1988. Todas, salvo la primera, son modificaciones del formato de los objetos de información ahora definidos en el módulo NSA.1, IPMSInformationObjects:

a) El tipo de contenido asignado a P2 ha cambiado. P2, que antes se identificaba por el entero 2, se identifica ahora por el entero 2 ó 22, según la funcionabilidad empleada en un caso particular de comunicación por medio del STRM (véase el § 20.2).

b) Se desaconseja ahora la omisión del miembro usuario de IPMIdentifier.

c) Se ha añadido a encabezamiento el miembro ampliaciones. Su grado es facultativo.

d) Se han abandonado los tipos de parte de cuerpo télex y documento formatizable simple. (La primera había sido identificada pero no definida.)

e) Se ha añadido el miembro sintaxis a VideotexParameters. Su grado es facultativo.

f) Se desaconseja ahora la presencia del miembro hora de entrega de MessageParameters en ausencia de su miembro sobre de entrega, o viceversa.

g) Se han añadido a BodyPart las alternativas definido-bilateralmente y definido-externamente.

h) Han variado los siguientes elementos de protocolo, definidos en la Recomendación X.411 e incorporados en elementos de protocolo de esta Recomendación, mediante referencia:
   i) ORName
   ii) ORAddress
   iii) MessageDeliveryEnvelope
   iv) EncodedInformationTypes
   v) SupplementaryInformation

i) Actualmente se desaconseja especificar un valor de longitud cero a cualquiera de los siguientes tipos de datos:
   i) LocalIPMIdentifier
   ii) FreeFormName
   iii) TelephoneNumber
   iv) SubjectField
   v) AutoForwardComment

j) Se han impuesto límites superiores a ciertos elementos de protocolo de longitud variable.

Nota – Los límites superiores impuestos son los indicados en el § 4.3 de la versión 6 de la *Guía del realizador de las Recomendaciones de la serie X.400.*

ISBN 92-61-03723-2