



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

X.402

(09/92)

REDES DE COMUNICACIÓN DE DATOS

**SISTEMA DE TRATAMIENTO DE MENSAJES:
ARQUITECTURAL GLOBAL**



Recomendación X.402

PREFACIO

El CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) es un órgano permanente de la Unión Internacional de Telecomunicaciones (UIT). Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Plenaria del CCITT, que se celebra cada cuatro años, establece los temas que han de estudiarse y aprueba las Recomendaciones preparadas por sus Comisiones de Estudio. La aprobación de Recomendaciones por los miembros del CCITT entre las Asambleas Plenarias de éste es el objeto del procedimiento establecido en la Resolución N.º 2 del CCITT (Melbourne, 1988).

La Recomendación X.402 ha sido revisada por la Comisión de Estudio VII y fue aprobada por el procedimiento de la Resolución N.º 2 el 10 de septiembre de 1992.

NOTAS DEL CCITT

- 1) En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una Administración de telecomunicaciones como una empresa privada de explotación reconocida de telecomunicaciones.
- 2) En el anexo J, figura la lista de abreviaturas utilizadas en la presente Recomendación.

© UIT 1993

Es propiedad. Ninguna parte de esta publicación puede reproducirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

Recomendación X.402

SISTEMAS DE TRATAMIENTO DE MENSAJES: ARQUITECTURA GLOBAL

(revisada en 1992)

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 (MHS) constituidos por cualquier número de sistemas abiertos cooperantes.

Un MHS 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 (MTS) y entregado a continuación a los agentes de uno o más usuarios adicionales, los destinatarios. Las unidades de acceso (AU) enlazan el MTS con sistemas de comunicación de otro tipo (por ejemplo, sistemas postales). El usuario recibe la ayuda de un agente de usuario (UA) para la preparación, el almacenamiento y la visualización de los mensajes. Facultativamente, puede recibir la ayuda de un dispositivo de almacenamiento de mensajes (MS) para almacenarlos. El MTS consta de cierto número de agentes de transferencia de mensajes (MTA) que, de manera colectiva, realizan la función de transferencia de almacenamiento y retransmisión de mensajes.

Esta Recomendación especifica la arquitectura global del MHS, 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/CEI 10021-2: 1990, modificada por los corrigenda 1, 2, 3 y 4, y el proyecto de enmienda 1.

1 Objeto

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

En otras Recomendaciones del CCITT | ISO/CEI 10021 se especifican otros aspectos del tratamiento de mensajes. La Rec. X.400 del CCITT | ISO/CEI 10021-1 da una visión general, no técnica, del tratamiento de mensajes. La prueba de conformidad de los componentes del MHS se describe en la Recomendación X.403. Los convenios establecidos al definir los servicios abstractos proporcionados por los componentes del MHS se definen en la Rec. X.407 del CCITT | ISO/CEI 10021-3. Las reglas detalladas según las cuales el MTS convierte los contenidos de los mensajes de un EIT a otro se definen en la Recomendación X.408. El servicio abstracto que proporciona el MTS y el procedimiento que gobierna su operación distribuida se definen en la Rec. X.411 del CCITT | ISO/CEI 10021-4. El servicio abstracto proporcionado por el MS se define en la Rec. X.413 del CCITT | ISO/CEI 10021-5. Los protocolos de aplicación que gobiernan las interacciones de los componentes del MHS se especifican en la Rec. X.419 del CCITT | ISO/CEI 10021-6. El sistema de mensajería interpersonal, que es una aplicación del tratamiento de mensajes, se define en la Rec. X.420 del CCITT | ISO/CEI 10021-7. El acceso telemático al sistema de mensajería interpersonal se especifica en la Recomendación T.330.

En el cuadro 1/X402 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

Rec. del CCITT	ISO/CEI	Tema tratado
Introducción		
X.400	10021-1	Visión de conjunto de sistemas y servicios
X.402	10021-2	Arquitectura global
Aspectos diversos		
X.403	–	Pruebas de conformidad
X.407	10021-3	Convenios para la definición del servicio abstracto
X.408	–	Reglas de conversión de tipo de información codificada
Servicios abstractos		
X.411	10021-4	Definición del servicio abstracto del MTS y procedimientos de operación distribuida
X.413	10021-5	Definición del servicio abstracto de almacenamiento de mensajes
Protocolos		
X.419	10021-6	Especificaciones de protocolo
Sistema de mensajería interpersonal		
X.420	10021-7	Sistema de mensajería interpersonal
T.330	–	Acceso telemático al IPMS

La guía, que es el instrumento principal para la difusión de la información relacionada con las comunicaciones entre los componentes del MHS, se define en las Recomendaciones de la serie X.500 del CCITT | ISO/CEI 9594. Véase el cuadro 2/X.402.

CUADRO 2/X.402

Especificaciones para las guías

Rec. del CCITT	ISO/CEI	Tema tratado
X.500	9594-1	La guía – Visión de conjunto de conceptos, modelos y servicios
X.501	9594-2	La guía – Modelos
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
X.509	9594-8	La guía – Marco de autenticación

El fundamento arquitectural del tratamiento de mensajes figura en otras Recomendaciones | Normas Internacionales. El modelo de referencia de OSI se define en la Rec. X.200 del CCITT | ISO 7498. En las Recs. X.208 y X.209 del CCITT | ISO/CEI 8824 y 8825 se definen la notación ASN.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 Recs. X.217 y X.227 del CCITT | ISO 8649 y 8650. En las Recs. X.218 y X.228 del CCITT | ISO/CEI 9066 se define el método RTSE de transporte fiable de las APDU por las asociaciones. La manera de efectuar peticiones a otros sistemas abiertos, el ROSE, se especifica en las Recs. X.219 y X.229 del CCITT | ISO/CEI 9072.

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 3/X.402

Especificaciones para los fundamentos del MHS

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

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 MHS 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 MHS puede hacer de la guía. En la sección 6 se describe cómo se realiza el MHS utilizando la OSI. Los anexos contienen importante información suplementaria.

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

2 Referencias normativas

Las Recomendaciones y las Normas Internacionales siguientes contienen disposiciones, que mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y las Normas Internacionales son objeto de revisiones, con lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y Normas Internacionales citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Secretaría del CCITT mantiene una lista de las Recomendaciones del CCITT actualmente vigentes.

2.1 *Interconexión de sistemas abiertos*

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

- Recomendación X.200 del CCITT (1988), *Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT*.
ISO 7498:1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model*.
ISO 7498:1984/Cor. 1:1988, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Technical Corrigendum 1*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.
ISO 8822:1988, *Information processing systems – Open Systems Interconnection – Connection oriented presentation service definition*.
- Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno (ASN.1)*.
ISO/CEI 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.
- Recomendación X.209 del CCITT (1988), *Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (ASN.1)*.
ISO/CEI 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
- Recomendación X.217 del CCITT (1988), *Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT*.
ISO 8649:1988, *Information processing systems – Open Systems Interconnection – Service definition for the Association Control Service Element*.
- Recomendación X.218 del CCITT (1988), *Transferencia fiable: modelo y definición del servicio*.
ISO/CEI 9066-1:1989, *Information processing systems – Text communication – Reliable Transfer – Part 1: Model and service definition*.
- Recomendación X.219 del CCITT (1988), *Operaciones a distancia: modelo, notación y definición del servicio*.
ISO/CEI 9072-1:1989, *Information processing systems – Text communication – Remote operations – Part 1: Model, notation and service definition*.
- Recomendación X.227 del CCITT (1988), *Especificación del control de protocolo de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT*.
ISO 8650:1988, *Information processing systems – Open Systems Interconnection – Protocol specification for the Association Control Service Element*.
- Recomendación X.228 del CCITT (1988), *Transferencia fiable: Especificación del protocolo*.
ISO/CEI 9066-2:1989, *Information processing systems – Text communication – Reliable Transfer – Part 2: Protocol specification*.
- Recomendación X.229 del CCITT (1988), *Operaciones a distancia: Especificación del protocolo*.
ISO/CEI 9072-2:1989, *Information processing systems – Text communication – Remote Operations – Part 2: Protocol specification*.

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:

- Recomendación X.500 del CCITT (1988), *Visión de conjunto de conceptos, modelos y servicios*.
ISO/CEI 9594-1:1990, *Information technology – Open Systems Interconnection – The Directory – Part 1: Overview of concepts, models, and services*.
- Recomendación X.501 del CCITT (1988), *La guía – Modelos*.
ISO/CEI 9594-2:1990, *Information technology – Open Systems Interconnection – The Directory – Part 2: Models*.
- Recomendación X.509 del CCITT (1988), *La guía – Marco de autenticación*.
ISO/CEI 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework*.
- Recomendación X.511 del CCITT (1988), *La guía – Definición del servicio abstracto*.
ISO/CEI 9594-3:1990, *Information technology – Open Systems Interconnection – The Directory – Part 3: Abstract service definition*.
- Recomendación X.518 del CCITT (1988), *La guía – Procedimientos para operación distribuida*.
ISO/CEI 9594-4:1990, *Information technology – Open Systems Interconnection – The Directory – Part 4: Procedures for distributed operation*.
- Recomendación X.519 del CCITT (1988), *La guía – Especificaciones de protocolos*.
ISO/CEI 9594-5:1990, *Information technology – Open Systems Interconnection – The Directory – Part 5: Protocol specifications*.
- Recomendación X.520 del CCITT (1988), *La guía – Tipos de atributo seleccionados*.
ISO/CEI 9594-6:1990, *Information technology – Open Systems Interconnection – The Directory – Part 6: Selected attribute types*.
- Recomendación X.521 del CCITT (1988), *La guía – Clases de objeto seleccionadas*.
ISO/CEI 9594-7:1990, *Information technology – Open Systems Interconnection – The Directory – Part 7: Selected object classes*.

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:

- Recomendación T.330 del CCITT (1988), *Acceso telemático al sistema de mensajería interpersonal*.
- Recomendación X.400 del CCITT (1992), *Tratamiento de mensajes – Visión de conjunto del sistema y del servicio*.
ISO/CEI 10021-1:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and service overview*.
ISO/CEI 10021-1:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and service overview – Technical Corrigendum 1*.
ISO/CEI 10021-1:1990/Cor. 2:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and service overview – Technical Corrigendum 2*.
ISO/CEI 10021-1:1990/Cor. 3:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and service overview – Technical Corrigendum 3*.
ISO/CEI 10021-1:1990/Cor. 4:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 1: System and service overview – Technical Corrigendum 4*.

- Recomendación X.403 del CCITT (1988), *Sistemas de tratamiento de mensajes – Pruebas de conformidad.*
- Recomendación X.407 del CCITT (1988), *Sistemas de tratamiento de mensajes – Convenios para la definición del servicio abstracto.*
 ISO/CEI 10021-3:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 3: Abstract service definition conventions.*
 ISO/CEI 10021-3:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 3: Abstract service definition conventions – Technical Corrigendum 1.*
 ISO/CEI 10021-3:1990/Cor. 1:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 3: Abstract service definition conventions – Technical Corrigendum 1.*
- Recomendación X.408 del CCITT (1988), *Sistemas de tratamiento de mensajes: Reglas de conversión de tipos de información codificada.*
- Recomendación X.411 del CCITT (1992), *Sistemas de tratamiento de mensajes: Sistema de transferencia de mensajes: definición del servicio abstracto y procedimientos.*
 ISO/CEI 10021-4:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures.*
 ISO/CEI 10021-4:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures – Technical Corrigendum 1.*
 ISO/CEI 10021-4:1990/Cor. 2:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures – Technical Corrigendum 2.*
 ISO/CEI 10021-4:1990/Cor. 3:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures – Technical Corrigendum 3.*
 ISO/CEI 10021-4:1990/Cor. 4:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures – Technical Corrigendum 4.*
 ISO/CEI 10021-4:1990/Amd. 1:1993, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 4: Message transfer system: Abstract service definition and procedures – Amendment 1: Minor Enhancements.*
- Recomendación X.413 del CCITT (1992), *Sistemas de tratamiento de mensajes: Definición del servicio abstracto de memoria de mensajes.*
 ISO/CEI 10021-5:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 5: Message store: Abstract service definition.*
 ISO/CEI 10021-5:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 5: Message store: Abstract service definition – Technical Corrigendum 1.*
 ISO/CEI 10021-5:1990/Cor. 2:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 5: Message store: Abstract service definition – Technical Corrigendum 2.*
 ISO/CEI 10021-5:1990/Cor. 3:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 5: Message store: Abstract service definition – Technical Corrigendum 3.*
 ISO/CEI 10021-5:1990/Cor. 4:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 5: Message store: Abstract service definition – Technical Corrigendum 4.*
- Recomendación X.419 del CCITT (1992), *Sistemas de tratamiento de mensajes: Especificaciones de protocolo.*

ISO/CEI 10021-6:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 6: Protocol specifications.*

ISO/CEI 10021-6:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 6: Protocol specifications – Technical Corrigendum 1.*

ISO/CEI 10021-6:1990/Cor. 2:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 6: Protocol specifications – Technical Corrigendum 2.*

ISO/CEI 10021-6:1990/Cor. 3:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 6: Protocol specifications – Technical Corrigendum 3.*

ISO/CEI 10021-6:1990/Cor. 4:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 6: Protocol specifications – Technical Corrigendum 4.*

- Recomendación X.420 del CCITT (1992), *Sistemas de tratamiento de mensajes – Sistema de mensajería interpersonal.*

ISO/CEI 10021-7:1990, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system.*

ISO/CEI 10021-7:1990/Cor. 1:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system – Technical Corrigendum 1.*

ISO/CEI 10021-7:1990/Cor. 2:1991, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system – Technical Corrigendum 2.*

ISO/CEI 10021-7:1990/Cor. 3:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system – Technical Corrigendum 3.*

ISO/CEI 10021-7:1990/Cor. 4:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system – Technical Corrigendum 4.*

ISO/CEI 10021-7:1990/Amd.1:1992, *Information technology – Text communication – Message-Oriented Text Interchange Systems (MOTIS) – Part 7: Interpersonal messaging system – Amendment 1: Minor Enhancements.*

2.4 Indicativos de país y planes de numeración

En esta Recomendación se indica lo siguiente:

- Recomendación X.121 del CCITT (1988), *Plan de numeración internacional para redes públicas de datos.*
- Recomendación E.163 del CCITT (1988), *Plan de numeración para el servicio telefónico internacional.*
- Recomendación E.164 del CCITT (1988), *Plan de numeración para esa RDSI.*

ISO 3166: 1988, *Codes for the representation of names of countries.*

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

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 Rec. X.200 del CCITT | ISO 7498:

- a) sintaxis abstracta;

- b) entidad de aplicación (AE, *application entity*);
- c) proceso de aplicación;
- d) unidad de datos de protocolo de aplicación (APDU, *application protocol data unit*);
- e) elemento de servicio de aplicación (ASE, *application service element*);
- f) tarea de tratamiento de la información distribuida;
- g) capa;
- h) sistema abierto;
- i) interconexión de sistemas abiertos (OSI, *open systems interconnection*);
- j) par;
- k) contexto de presentación;
- l) protocolo;
- m) modelo de referencia;
- n) sintaxis de transferencia;
- o) elemento de usuario (UE, *user element*).

En esta Recomendación y en otras de la misma serie se emplean los nombres de los tipos y valores de datos ASN.1 así como los siguientes términos definidos en las Recs. X.208 y X.209 del CCITT | ISO/CEI 8824 y 8825:

- a) notación de sintaxis abstracta uno (ASN.1, *abstract syntax notation one*);
- b) reglas básicas de codificación;
- c) explícito;
- d) exportación;
- e) implícito;
- f) importación;
- g) macro;
- h) módulo;
- i) rótulo;
- j) tipo;
- k) valor.

En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. X.217 del CCITT | ISO 8649:

- a) asociación de aplicación; asociación;
- b) contexto de aplicación (AC, *application context*);
- c) elemento de servicio de control de asociación (ACSE, *association control service element*);
- d) iniciador;
- e) respondedor.

En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. X.218 del CCITT | ISO/CEI 9066-1:

- a) transferencia fiable (RT, *reliable transfer*);
- b) elemento de servicio de transferencia fiable (RTSE, *reliable transfer service element*).

En esta Recomendación y en otras de la misma serie se emplean los siguientes términos definidos en la Rec. X.219 del CCITT | ISO/CEI 9072-1:

- a) argumento;
- b) asíncrono;
- c) vinculado;
- d) parámetro;

- e) error distante;
- f) operación distante;
- g) operaciones a distancia (RO, *remote operations*);
- h) elemento de servicio de operaciones a distancia (ROSE, *remote operations service element*);
- 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 del CCITT | ISO/CEI 9594:

- a) atributo;
- b) certificado;
- c) autoridad certificadora;
- d) trayecto de la certificación;
- e) inscripción en la guía;
- f) agente de sistema de directorio (DSA, *directory system agent*);
- 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 I.

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 I.

5 **Convenios**

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

5.1 *ASN.1*

Esta Recomendación emplea, en sus anexos A y C, diversos convenios de descripción basados en la ASN.1, para definir información propia del tratamiento de mensajes, que pueda contener la guía. Utiliza, en particular, los macros OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE-SYNTAX de la Rec. X.501 del CCITT | ISO/CEI 9594-2, para definir las clases de objetos, los atributos y las sintaxis de atributo propias del tratamiento de mensajes.

La ASN.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 ASN.1 están implícitos en todo el módulo ASN.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 (M, mandatory)**: un componente obligatorio estará presente en cada caso de la clase;
- b) **optativo (O)**: un componente optativo 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 por defecto (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 ISO/CEI 10021;
- 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 ISO/CEI 10021.

El **tratamiento de mensajes** es una tarea distribuida del tratamiento de la información, que comprende las siguientes subtarefas 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 Rec. X.420 del CCITT | ISO/CEI 10021-7.

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 del CCITT ISO/CEI 10021.

El **entorno de tratamiento de mensajes (MHE, Message Handling Environment)** comprende objetos funcionales «primarios» de varios tipos: el *sistema de tratamiento de mensajes (MHS)*, los *usuarios* y las *listas de distribución*. A su vez, el *MHS*, puede descomponerse en objetos funcionales «secundarios», de menor nivel y de varios tipos: el *sistema de transferencia de mensajes*, los *agentes de usuario*, las *memorias de mensajes* y las *unidades de acceso*. El *MTS*, 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 Recomendaciones del CCITT | ISO/CEI 10021. 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 MHE 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.

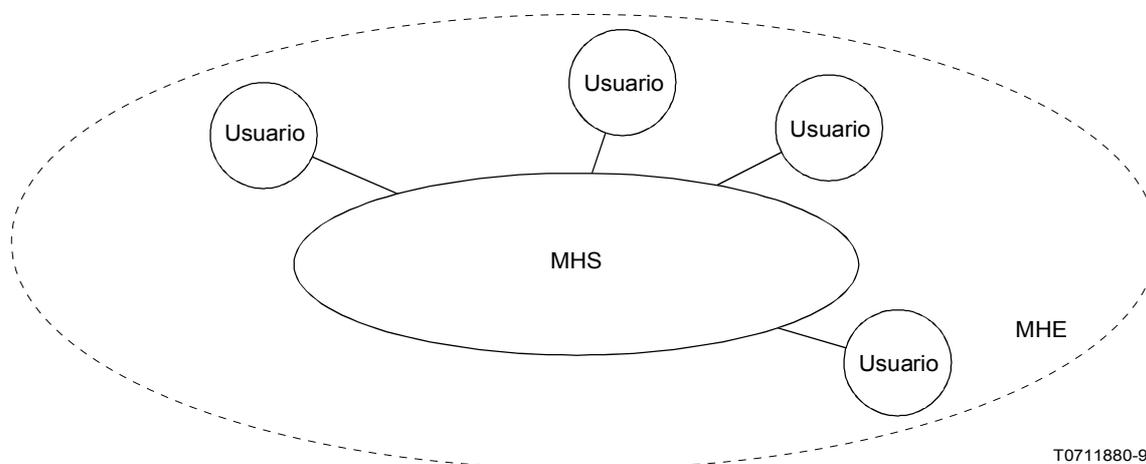


FIGURA 1/X.402

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 (MHS, message handling system)**.

El MHE consta de un solo MHS.

7.1.2 Usuarios

La finalidad principal del MHS 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 MHS.
- b) **usuario indirecto**: Usuario que participa en el tratamiento de mensajes utilizando indirectamente el MHS, es decir, a través de otro sistema de comunicaciones (por ejemplo, un sistema postal o una red télex) al que está enlazado el MHS.

El MHE consta de un número cualquiera de usuarios.

7.1.3 Lista de distribución

Mediante el MHS, un usuario puede hacer llegar objetos de información a grupos de usuarios previamente especificados, así como a usuarios individuales. Se llama **lista de distribución (DL, distribution list)** al objeto funcional que representa a un grupo de usuarios previamente especificado y a otras DL.

Una DL representa cero o más usuarios y DL, a los que se les denomina sus **miembros**. De las DL (si es que hay alguna) se dice que están **jerarquizadas**. Pedir al MHS que transporte un objeto de información (por ejemplo, un *mensaje*) a una DL 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 DL 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 DL.

El MHE consta de un número cualquiera de DL.

Nota – Una DL podría estar más restringida, limitándola por ejemplo al transporte de *mensajes* con un determinado *tipo de contenido*.

7.2 Objetos funcionales secundarios

El MHS 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.

7.2.1 Sistema de transferencia de mensajes

En el MHS se produce un transporte de objetos de información a usuarios individuales y a los miembros de las DL. El objeto funcional que realmente los transporta se llama **sistema de transferencia de mensajes (MTS, message transfer system)**. El MTS es un sistema de comunicación de almacenamiento y retransmisión, del que se puede decir que es la columna vertebral del MHS.

El MTS es de uso general y facilita toda clase de aplicaciones del tratamiento de mensajes. Además, el MTS puede adaptarse a una o más aplicaciones particulares, es decir, puede efectuar una *conversión*.

El MHS consta de un solo MTS.

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 (UA, user agent)**.

Un UA típico está adaptado a una o más aplicaciones particulares del tratamiento de mensajes.

El MHS consta de un número cualquiera de UA.

Nota – En el caso de un UA 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).

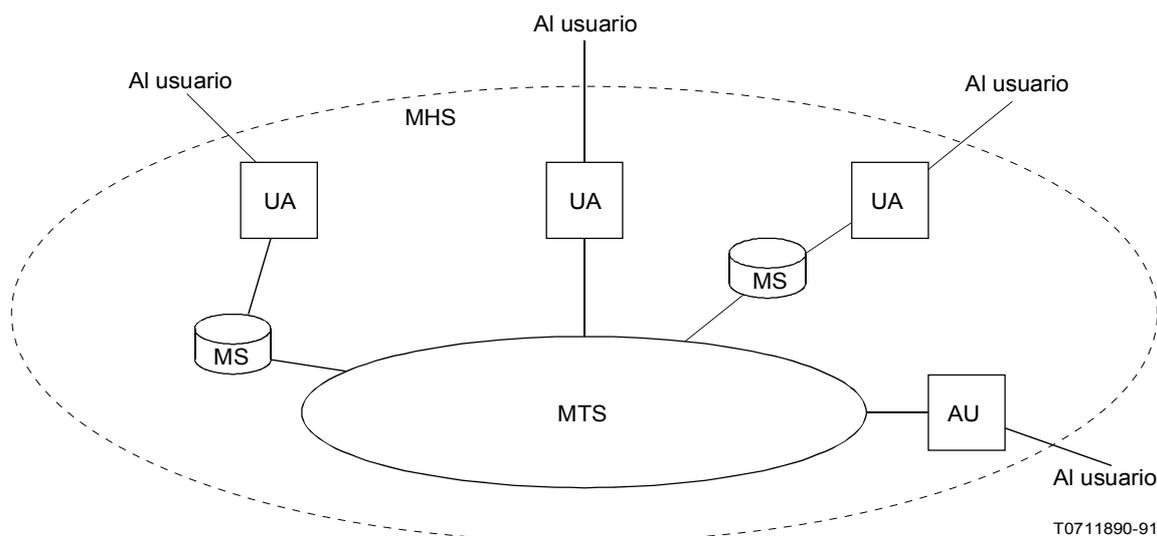


FIGURA 2/X.402
Sistema de tratamiento de mensajes

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 (MS, message store)**. Cada MS está asociada a un UA, pero no todos los UA tienen MS asociada.

Las MS son de uso general y facilitan todas las aplicaciones de tratamiento de mensajes. Además, una MS 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 MHS consta de un número cualquiera de MS.

Nota – Como asunto local, un UA puede proporcionar capacidad de almacenamiento de objetos de información que complementa o sustituye la de una MS.

7.2.4 Unidades de acceso

El objeto funcional que enlaza al MTS 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 (AU, access unit)**.

Una AU típica está adaptada a un sistema de comunicaciones particular y a una o más aplicaciones particulares del tratamiento de mensajes.

El MHS consta de un número cualquiera de AU.

7.3 Objetos funcionales terciarios

El MTS 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.

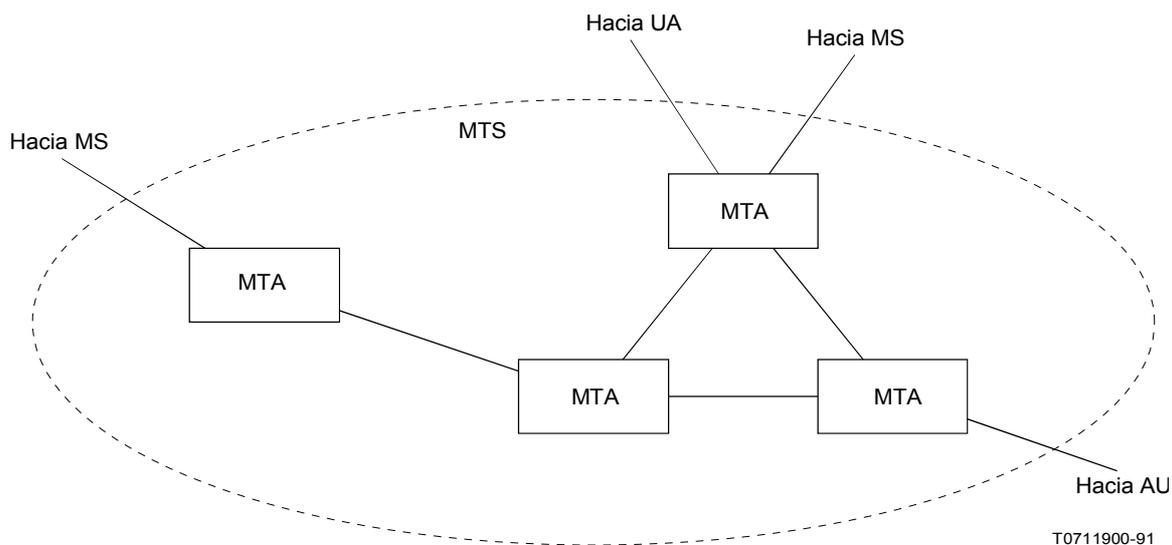


FIGURA 3/X.402
Sistema de transferencia de mensajes

7.3.1 Agentes de transferencia de mensajes

El MTS transporta objetos de información a usuarios y DL según el modo de almacenamiento y retransmisión. Al objeto funcional que proporciona el eslabón de la cadena de almacenamiento y retransmisión del MTS se le denomina **agente de transferencia de mensajes (MTA, message transfer agent)**.

Los MTA son de uso general y facilitan las aplicaciones del tratamiento de mensajes. Además, un MTA se puede adaptar a una o más aplicaciones particulares, es decir, puede efectuar una *conversión*.

El MTS consta de un número cualquiera de MTA.

7.4 Tipos de AU seleccionados

Como se ha descrito anteriormente, entre el MHS y otros tipos de sistemas de comunicaciones se produce un interfuncionamiento a través de las AU. En los párrafos que siguen se presentan varios tipos de AU seleccionados: de entrega física, de acceso telemático y por télex.

7.4.1 Entrega física

Una **unidad de acceso de entrega física (PDAU, physical delivery access unit)** es una AU 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 (PDS, physical delivery system)** es un sistema que efectúa la *entrega física*. El sistema postal es un tipo importante de PDS. Se llama **entrega física** a la transferencia de un mensaje físico a un patrón de un PDS, uno de los usuarios indirectos a los que la PDAU proporciona capacidades de tratamiento de mensajes.

La mensajería interpersonal es una de las aplicaciones del tratamiento de mensajes proporcionadas por todas las PDAU (véase la Rec. X.420 del CCITT | ISO/CEI 10021-7).

7.4.2 Telemática

En la Rec. X.420 del CCITT | ISO/CEI 10021-7 se presentan las unidades de acceso telemático, que proporcionan, en exclusiva, la mensajería interpersonal.

7.4.3 Télex

En la Rec. X.420 del CCITT | ISO/CEI 10021-7 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 del CCITT | ISO/CEI 10021.

El MHS y el MTS 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, UA, MS, MTA y AU – que son origen y destino final de tales objetos.

En los puntos que siguen se definen y describen los objetos de información cuyo resumen figura en el cuadro 4/X.402.

CUADRO 4/X.402

Objetos de información transportables

Objeto de información	Objeto funcional				
	Usuario	UA	MS	MTA	AU
Mensaje	SD	–	–	–	–
Sonda	S	–	–	D	–
Informe	D	–	–	S	–

S Último origen (*ultimate source*)

D Último destino (*ultimate destination*)

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:

- 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 MTS, y caracteriza el *contenido* del mensaje.
- contenido:** Objeto de información que el MTS ni examina ni modifica, si no es a efectos de *conversión*, mientras transporta el 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 ASN.1) que indica la sintaxis y la semántica del contenido en su conjunto. Ese identificador permite al MTS determinar si el mensaje ha de *entregarse* o no a usuarios particulares, y permite a los UA y MS interpretar y tratar el contenido.

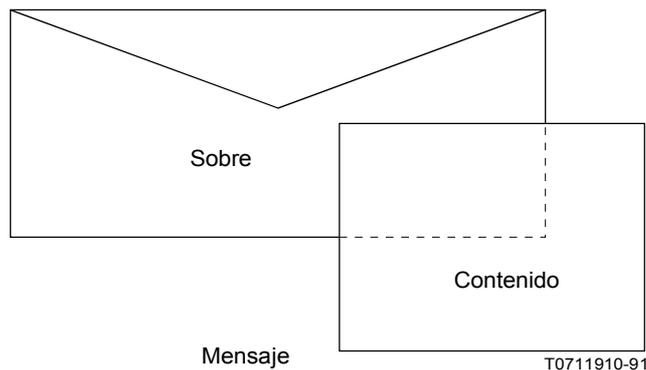


FIGURA 4/X.402
Sobre y contenido de un mensaje

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 (EIT, *encoded information type*)** es un identificador (un identificador de objeto o entero ASN.1) que indica el soporte y el formato (por ejemplo, texto IA5 o facsimil del grupo 3) de partes individuales del contenido. Permite además al MTS 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 EIT 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 MTA 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 MTS 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 DL*. En concreto, y aparte de las consecuencias de la supresión de la *ampliación de la DL*, 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 MTS, 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 DL a la que pertenezca el *destinatario miembro*. Como asunto local, (es decir, cuando exista una

política establecida para esa DL particular), el transporte del informe puede proseguir hasta el propietario de la DL, a otro que contenga DL (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 DL*.
- 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 del CCITT ISO/CEI 10021.

El MHS puede transportar un objeto de información a usuarios individuales, DL 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 DL desempeñan en éste.

9.1 Transmisión

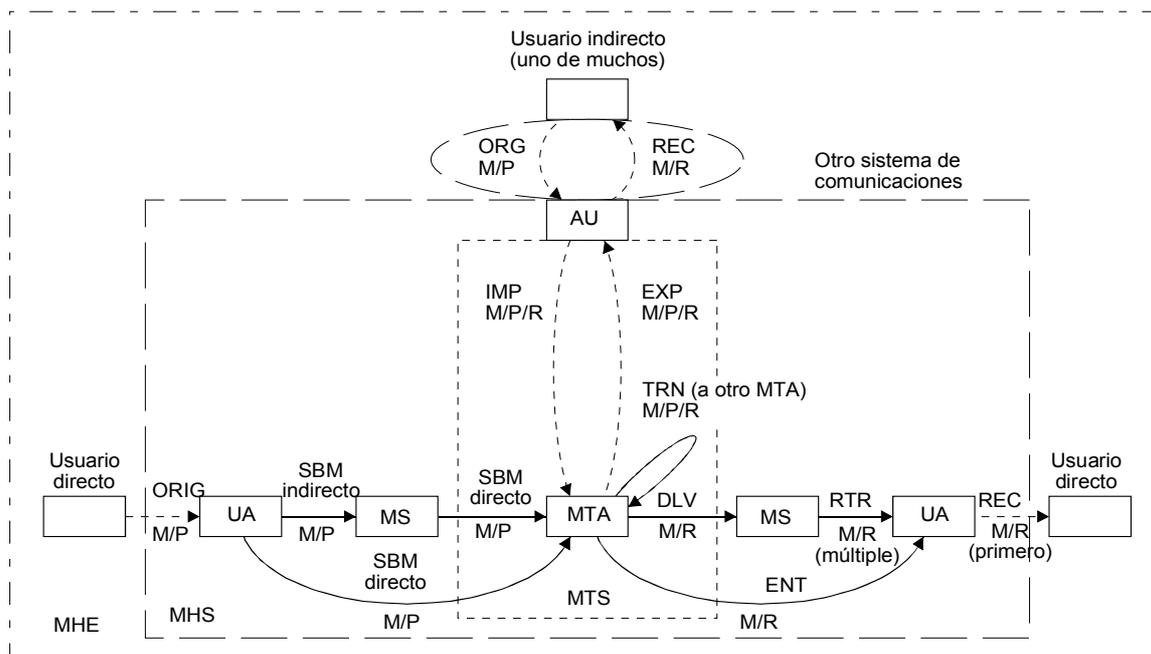
Se llama **transmisión** al transporte o tentativa de transporte de un mensaje o de una sonda. La transmisión abarca el transporte del mensaje desde su *originador* a sus *destinatarios potenciales* y el transporte de la sonda desde su *originador* hasta los MTA, facultados para *afirmar* la *entregabilidad* 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, UA, MS, MTA y AU – 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.

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 UA 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 MTA 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.



T0711920-91

— Normalizado

- - - - - No normalizado

M Mensaje (*message*)
P Sonda (*probe*)
R Informe (*report*)

ORG Origen (*origination*)
SBM Depósito (*submission*)
IMP Importación (*import*)
TRN Transferencia (*transfer*)

EXP Exportación (*export*)
DLV Entrega (*delivery*)
RTR Extracción (*retrieval*)
REC Recepción (*receipt*)

FIGURA 5/X.402

Flujo de información de la transmisión

9.2 Funciones de la transmisión

Los usuarios y las DL 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 DL.

Un usuario puede desempeñar el siguiente papel «origen» en la transmisión de un mensaje o sonda:

- originador:** Usuario (no DL) que es origen último de un mensaje o sonda.

Un usuario o una DL pueden desempeñar alguno de los siguientes papeles «destino» en la transmisión de un mensaje o sonda:

- destinatario deseado:** Uno de los usuarios o de las DL que el originador especifica como destinos de un mensaje o una sonda.
- destinatario alternativo especificado por el originador:** Usuario (o DL 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:** DL o usuario al cual se transporta un mensaje (pero no una sonda), como resultado de una *ampliación de DL*
- d) **destinatario alternativo designado por el destinatario:** Usuario (o DL si hay alguna) elegido por un destinatario miembro, o receptor deseado o alternativo al especificado por el originador, para que *redireccione* mensajes.

Un usuario o una DL pueden adquirir alguna de las siguientes categorías durante la transmisión de un mensaje o una sonda:

- a) **destinatario potencial:** Cualquier DL 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 Recomendaciones del CCITT | ISO/CEI 10021; 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, UA, MS, MTA y AU – 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	P	R	Usuario	UA	MS	MTA	AU
Origen Depósito	No	X	X	–	S	D	–	–	–
	Sí	X	X	–	–	S	SD	D	–
Importación Transferencia Exportación	No	X	X	X	–	–	–	D	S
	Sí	X	X	X	–	–	–	SD	–
	No	X	X	X	–	–	–	S	D
Entrega Recuperación Recepción	Sí	X	–	X	–	D	D	S	–
	Sí	X	–	X	–	D	S	–	–
	No	X	–	X	D	S	–	–	–

- M Mensaje
- P Sonda (*probe*)
- R Informe (*report*)
- S Origen (*source*)
- D Destino
- X Permitido

9.3.1 *Origen*

En un paso de **origen**, un usuario directo transporta un mensaje o una sonda a su UA, 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 MTA, un mensaje o sonda que quedan a cargo del MTS. Cabe distinguir los dos tipos siguientes de depósito:

- a) **depósito indirecto**: Paso de transmisión en el que el UA del originador transporta un mensaje o sonda a su MS y en el que la MS efectúa un *depósito directo*. Este paso sigue al de origen.

Es un paso que sólo puede darse si el usuario dispone de una MS.

- b) **depósito directo**: Paso de transmisión en el que el UA o la MS originador transportan un mensaje o sonda a un MTA. 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 MS 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 UA) y ser por ello preferible al depósito directo.

Al UA o a la MS que participa en el depósito directo se le llama **agente de depósito**. Un agente de depósito se da a conocer al MTS mediante un proceso de registro, como resultado del cual el agente de depósito y el MTS 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**, un AU transporta un mensaje, una sonda o un informe a un MTA. Este paso introduce en el MTS 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 un AU a otra.

9.3.4 *Transferencia*

En un paso de **transferencia**, un MTA transporta un mensaje, una sonda o un informe a otro MTA. 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 MTS consta de varios MTA.

Cabe distinguir, según sea el número de *MD* afectados, los siguientes tipos de transferencia:

- a) **transferencia interna**: Transferencia que implica a varios MTA en un solo *MD*.
- b) **transferencia externa**: Transferencia que implica a varios MTA en diferentes *MD*.

9.3.5 *Exportación*

En un paso de **exportación**, un MTA transporta un mensaje, una sonda o un informe a un AU. En este paso, se lanza un objeto de información desde el MTS hacia otro sistema de comunicaciones. El paso se produce a continuación del depósito directo, de la importación o de la transferencia.

El MTA puede generar, como parte de este paso, un informe de entrega. En el caso de unidades de acceso un informe de entrega positivo indica la buena aceptación de un mensaje (o una sonda) por parte de la unidad de acceso. Según las condiciones definidas en las especificaciones pertinentes de la transmisión de mensaje, el informe de entrega puede, si no, indicar que el mensaje ha sido aceptado debidamente por el usuario indirecto que utiliza la unidad de acceso. (Por ejemplo, véanse las Recomendaciones F.421, F.422, F.423, F.435, F.440, T.300, T.330 y U.204.)

Nota – El concepto de exportación es un concepto genérico. La manera cómo se efectúe este paso varía, naturalmente, de una AU a otra.

9.3.6 *Entrega*

En un paso de **entrega**, un MTA transporta un mensaje o un informe a una MS o a un UA. La MS y el UA 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 MTA puede generar, como parte de este paso, un informe de entrega.

Se llama **agente de entrega** a la MS o al UA que participan en la misma. Un agente de entrega se da a conocer al MTS mediante un proceso de registro, como resultado del cual el agente de entrega y el MTS 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 MS de un usuario transporta un mensaje o un informe a su UA. 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 MS.

9.3.8 *Recepción*

En un paso de **recepción**, un UA 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, UA, MS, MTA y AU – a los que les está permitido desarrollarlos.

Todos los eventos se producen dentro del MTS.

Los tipos de eventos de transmisión, resumidos en el cuadro 6/X.402 son definidos y descritos separadamente en los puntos que siguen.

Eventos de transmisión

Evento de transmisión	Objetos de información			Objetos funcionales				
	M	P	R	Usuario	UA	MS	MTA	AU
división	X	X	–	–	–	–	X	–
combinación	X	X	X	–	–	–	X	–
resolución de nombre	X	X	–	–	–	–	X	–
ampliación de DL	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
- P Sonda (*probe*)
- R Informe (*report*)
- X Permitido

9.4.1 *División*

En un evento de **división**, un MTA 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 MTA transportar independientemente un objeto a varios destinatarios potenciales.

Un MTA 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 MTA combina 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 MTA 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 MTA agrega la *dirección O/R* correspondiente al *nombre O/R* que identifica a uno de los destinatarios inmediatos de un mensaje o una sonda.

9.4.4 *Ampliación de DL*

En un evento de **ampliación de DL**, un MTA reemplaza a un destinatario inmediato que denota a una DL por los miembros de dicha DL, que de este modo se convierten en destinatarios miembros. El evento de ampliación de DL sólo se produce para los mensajes, no para las sondas.

A una DL determinada se le somete a ampliación siempre en una localización preestablecida, dentro del MTS. Esta localización se llama **punto de ampliación** de la DL, y viene identificada por una *dirección O/R*.

El MTA puede generar, como parte de este evento, un informe de entrega.

La ampliación de la DL está sujeta al permiso de presentación. En el caso de una DL jerarquizada, ese permiso debe haber sido concedido a la DL 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 MTA sustituye a un usuario o a una DL 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 MTA transforma partes del contenido de un mensaje de un EIT 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 EIT de la información a convertir y el EIT resultante de la conversión:

- a) **conversión explícita**: Conversión en la que el originador elige tanto el EIT inicial como el final.
- b) **conversión implícita**: Conversión en la que el MTA elige los EIT finales, en función de los EIT iniciales y de las capacidades del UA.

9.4.7 *No entrega*

En un evento de **no entrega**, un MTA establece que el MTS 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 MTS considere intransportable.

En el caso de mensaje, el MTA genera, como parte de este evento, un informe de no entrega.

Un MTA 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 MTA establece que el MTS 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 MTA genera, como parte de ese evento, un informe de no entrega.

Un MTA 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 MTA establece que el MTS 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 MTA puede generar, como parte de este evento, un informe de entrega.

Un MTA produce una afirmación una vez que ha constatado que los destinatarios inmediatos están especificados adecuadamente y, si esos destinatarios son usuarios (pero no DL), que aceptarían la entrega de cualquier mensaje descrito. Si los destinatarios inmediatos son DL, el MTA producirá una afirmación si existe la DL y si el originador tiene el permiso de presentación pertinente.

9.4.10 *Encaminamiento*

En un evento de **encaminamiento**, un MTA selecciona el MTA «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 MTS y, obviamente, sólo puede producir si el MTS consta de varios MTA.

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 *MD*).
- b) **encaminamiento externo:** Encaminamiento que prepara para una transferencia externa (es decir, una transferencia entre distintos *MD*).

Un MTA 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 del CCITT ISO/CEI 10021. 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 MTS, y de los elementos de seguridad que facilitan estos servicios.

Las características de seguridad constituyen una ampliación facultativa del MHS, 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*, *computer security*) o los servicios de seguridad proporcionados por el MHS. Según cuales sean los riesgos que se contemplen, se seleccionarán unos u otros servicios de seguridad de MHS en combinación con adecuadas medidas de seguridad física y de *COMPUSEC*. Los servicios de seguridad facilitados por el MHS se describen más adelante. La denominación y la estructuración de los servicios se basan en la norma ISO 7498-2.

Nota – pesar de estas características de seguridad, pueden producirse ciertas agresiones contra las comunicaciones entre un usuario y el MHS o contra las comunicaciones de usuario a usuario (por ejemplo, en el caso de usuarios que acceden al MHS a través de una unidad de acceso, o de usuarios con acceso a distancia a sus UA). 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 MTS. El sobre contiene argumentos propios de la seguridad, tal como se describe en la Rec. X.411 del CCITT | ISO/CEI 10021-4. 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 Rec. X.411 del CCITT | ISO/CEI 10021-4 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 Rec. X.411 del CCITT | ISO/CEI 10021-4.

Muchas de las técnicas empleadas se basan en mecanismos de cifrado. Los servicios de seguridad del MHS 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 Rec. X.400 del CCITT | ISO/CEI 10021-1. 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 MHS deben poder facilitar una amplia gama de políticas de seguridad, que va más allá de los límites del propio MHS. 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 MHS, 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 esta subcláusula 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. Un asterisco (*) debajo del 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 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 MHS 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.

10.2.1.1 *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 MTA o los usuarios del MTS 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 MTS (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 MTA 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 MTA a través de los cuales se transfiere el informe (1 a 5 inclusive, en la figura 6/X.402).

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 MTS para su entrega al destinatario o destinatarios especificados originalmente.

El servicio puede proporcionarse utilizando el elemento de seguridad de prueba de depósito.

Servicios de seguridad de la transferencia de mensajes

Servicio	UA/ UA	MS/ MTA	MTA/ MS	MTA/ UA	UA/ MS	UA/ MTA	MTA/ MTA	MS/ UA
<i>Autenticación de origen</i>								
Autenticación de origen de mensajes	*	*	—	*	—	—	—	—
Autenticación de origen de sondas	—	—	*	*	—	—	—	—
Autenticación de origen de informes	—	—	—	—	*	*	*	—
Prueba de depósito	—	—	—	—	—	—	*	—
Prueba de entrega	*	—	—	—	—	—	—	a)
<i>Gestión de acceso seguro</i>								
Autenticación de entidades pares	—	*	*	*	*	*	*	*
Contexto de seguridad	—	*	*	*	*	*	*	*
<i>Confidencialidad de datos</i>								
Confidencialidad de conexiones	—	*	*	*	*	*	*	*
Confidencialidad de contenidos	*	—	—	—	—	—	—	—
Confidencialidad de flujo de mensajes	*	—	—	—	—	—	—	—
<i>Servicios de integridad de datos</i>								
Integridad de conexiones	—	*	*	*	*	*	*	*
Integridad de contenidos	*	—	—	—	—	—	—	—
Integridad de secuencia de mensajes	*	—	—	—	—	—	—	—
<i>No rechazo</i>								
No rechazo de origen	*	—	—	*	—	—	—	—
No rechazo de depósito	—	—	—	—	—	—	*	—
No rechazo de entrega	*	—	—	—	—	—	—	a)
<i>Etiquetado de mensajes de seguridad</i>								
Etiquetado de mensajes de seguridad	*	*	*	*	*	*	*	*
<i>Servicios de gestión de la seguridad</i>								
Cambio de credenciales	—	*	—	*	*	*	*	—
Registros	—	*	—	*	—	—	—	—
Registros de la MS	—	*	—	—	—	—	—	—

a) Este servicio lo proporciona la MS del destinatario al UA del originador.

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 MTS 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.

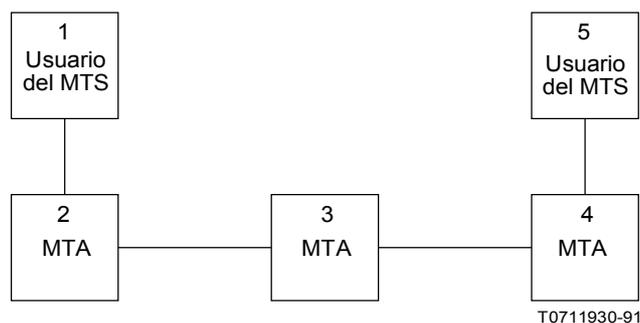


FIGURA 6/X.402
Modelo funcional de MHS simplificado

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 reactivación 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 MHS 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 MTS, de la figura 6/X.402, siendo el mensaje ininteligible para los MTA.

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 MHS 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 MTS. 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 MHS.

10.2.4.1 *Servicio de seguridad de integridad de conexión*

El MHS 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 sí 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 MTS, 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 MTS, de la figura 6/X.402, y no a los MTA 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 rechazo 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 MTS, 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 MHS, es decir, a todos los usuarios del MTS y MTA 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 MTS 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 MHS, es decir, los MTA y los usuarios del MTS. Conjuntamente con el servicio de seguridad de contexto de seguridad, facilita la ejecución de políticas de seguridad que precisen qué partes del MHS pueden tratar mensajes, mediante las etiquetas de seguridad asociadas especificadas.

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 MHS necesita cierto número de servicios de gestión de seguridad. Los únicos servicios de gestión previstos en la Rec. X.411 del CCITT | ISO/CEI 10021-4 tratan del cambio de credenciales y del registro de etiquetas de seguridad de usuario del MTS.

10.2.7.1 *Servicio de seguridad de cambio de credenciales*

Este servicio de seguridad permite a una entidad del MHS cambiar las credenciales que le afectan, contenidas en otra entidad del MHS. 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 MTA, de las etiquetas de seguridad autorizadas para un determinado usuario del MTS. Puede proporcionarse utilizando el elemento de seguridad de registros.

10.2.7.3 *Servicio de seguridad de registro de la MS*

Este servicio de seguridad permite el establecimiento de las etiquetas de seguridad que son admisibles para el usuario de la MS.

10.3 *Elementos de seguridad*

En las subcláusulas que siguen se describen los elementos de seguridad, disponibles en los protocolos de la Rec. X.411 del CCITT | ISO/CEI 10021-4, para facilitar los servicios de seguridad en el MHS. Esos elementos están relacionados directamente con los argumentos de varios servicios descritos en la Recomendación X.411 | ISO/CEI 10021-4. Este punto tiene por objeto extraer los elementos de las definiciones de servicios de la Rec. X.411 del CCITT | ISO/CEI 10021-4 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 MTS a un MTA, de un MTA a un MTA, de un MTA a un usuario del MTS de una MS a un UA o de un UA a una MS. 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 MTS, a la MS y a un MTA. 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 MTS 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 MHS 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 MTA autenticar la identidad del usuario del MTS que originó una determinada sonda.

Este elemento de seguridad utiliza la verificación de autenticación de origen de sondas, que es uno de los cinco 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 MTA o usuario del MTS que recibe un informe, autenticar la identidad del MTA 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 MHS 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 depósito, y la prueba de depósito devuelta al usuario del MTS como parte de los resultados del depósito de mensajes. El MTS 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 MHS.

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 MTS 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 MTS o un MTA se vincula a un MTA o a un usuario del MTS, 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 MTS y a un MTA.

10.3.2.2 *Elemento de seguridad de registros*

El elemento de seguridad de registros permite el establecimiento en un MTA de etiquetas de seguridad autorizadas de un usuario del MTS.

El servicio de registros proporciona este elemento. Dicho servicio permite a un usuario del MTS cambiar los argumentos, contenidos en el MTS, relativos a la entrega de mensajes a ese usuario del MTS.

10.3.2.3 *Elemento de seguridad de registro de la MS*

El elemento de seguridad de registro de la MS permite el establecimiento de las etiquetas de seguridad admisibles del usuario de la MS.

El servicio de registro de la MS proporciona este elemento. Dicho servicio permite a un usuario de la MS cambiar los argumentos, contenidos en la MS, relativos a la recuperación de mensajes dirigidos a ese usuario de la MS.

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 MHS 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 sólo 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 MTA.

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 Rec. X.411 del CCITT | ISO/CEI 10021-4 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 MHS.

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 MTA 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 envoltura 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 MTS o de un MTA.

El elemento de seguridad lo proporciona el servicio de cambio de credenciales del MTS.

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). Una vez entregado al destinatario indicado en el sobre externo, el sobre externo se suprime y se descifra el contenido si es necesario, lo que da lugar a un sobre interno y a su contenido. La información contenida en el sobre interno se utiliza para transferir el contenido del sobre interno a los recibientes indicados en el sobre interno.

El tipo de contenido es un argumento de los servicios de depósito, transferencia y entrega de mensajes.

10.3.9 *Codificación para encriptación y troceado (hashing)*

Cada parámetro MTS que se convierta en algoritmos de encriptación o troceado se codificará utilizando las reglas de codificación especificadas a los fines de esa encriptación o troceado.

Nota 1 – No puede suponerse que la codificación del sobre de entrega o del contenido entregado utilizará las reglas de codificación especificadas en el identificador de algoritmo.

Nota 2 – En el caso del contenido deben aplicarse las reglas de codificación especificadas en el identificador de algoritmo sólo a la codificación de los octetos del contenido dentro de cadena de octetos, y no a la codificación del protocolo de contenido (que permanece invariable).

SECCIÓN 3 – CONFIGURACIONES

11 **Visión de conjunto**

En esta sección se especifica cómo configurar el MHS 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 *MHS global*.

12 **Configuraciones funcionales**

Se especifican en este punto las posibles configuraciones funcionales del MHS. 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 MS.

12.1 *Respecto a la guía*

Con respecto a la guía, el MHS puede configurarse para un usuario, o colectivo de usuarios (véase por ejemplo, la cláusula 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.

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.

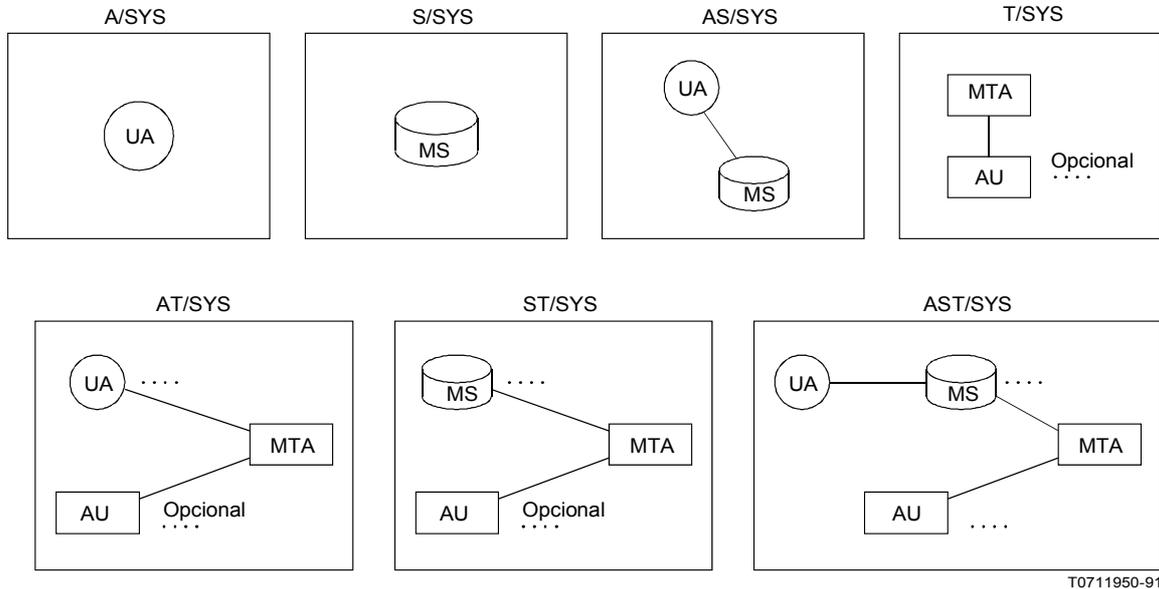


FIGURA 8/X.402
Tipos de sistemas de mensajería

Los tipos de sistemas de mensajería expuestos de manera resumida en el cuadro 8/X.402 se definen y describen en las subcláusulas siguientes.

Nota – Para la admisión de tipos de sistemas de mensajería se han tenido en cuenta los siguientes principios fundamentales:

- Una AU y el MTA con el que interactúa se hallan típicamente ubicados en la misma posición, puesto que no se ha normalizado ningún protocolo que gobierne su interacción.
- Un MTA se halla típicamente ubicado con múltiples UA o MS, 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.
- Nada se consigue ubicando varios MTA en el mismo emplazamiento, en un sistema de mensajería, puesto que un solo MTA presta servicio a múltiples usuarios, y la finalidad de un MTA 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 MTA coexistan en un único sistema por computador).
- La ubicación de una AU con un MTA no afecta al comportamiento del sistema con respecto al resto del MHS. Un solo tipo de sistema de mensajería abarca, por tanto, la presencia y la ausencia de la AU.

13.1.1 Sistemas de acceso

Un **sistema de acceso (A/SYS, acces system)** contiene un UA, pero no una MS ni un MTA ni una AU.

Un A/SYS se dedica a un único usuario.

Sistemas de mensajería

Sistema de mensajería	Objetos funcionales			
	AU	MS	MTA	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 Múltiple

[. . .] Opcional

13.1.2 *Sistemas de almacenamiento*

Un **sistema de almacenamiento (S/SYS, storage system)** contiene una MS, pero no un UA ni un MTA ni una AU.

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, access and storage system)** contiene un UA, y una MS, pero no un MTA ni una AU.

Un AS/SYS se dedica a un único usuario.

13.1.4 *Sistemas de transferencia*

Un **sistema de transferencia (T/SYS, transfer system)** contiene un MTA, facultativamente, una o más AU, pero no un UA ni una MS.

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, access and transfer system)** contiene uno o más UA, un MTA y, facultativamente, una o más AU, pero no una MS.

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, storage and transfer system)** contiene una o más MS, un MTA y facultativamente, una o más AU, pero no UA.

Un ST/SYS puede prestar servicio a múltiples usuarios.

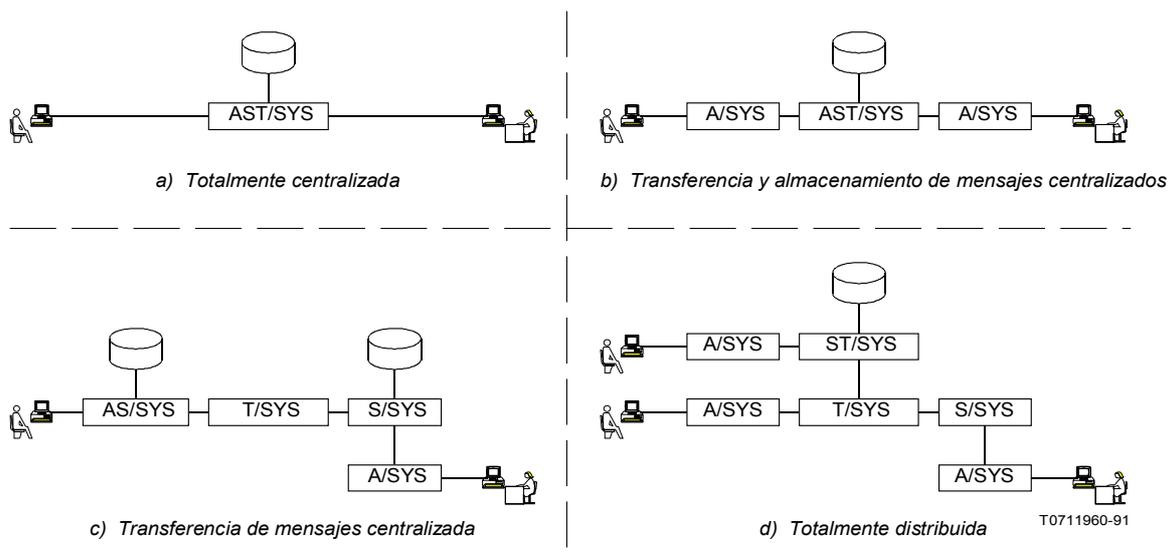
13.1.7 *Sistema de acceso, almacenamiento y transferencia*

Un **sistema de acceso, almacenamiento y transferencia (AST/SYS, acces, storage and transfer system)** contiene uno o más UA, una o más MS, un MTA y facultativamente, una o más AU.

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 MHS. 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.



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

13.2.1 Totalmente centralizada

El MHS 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 MHS puede proporcionar transferencia y almacenamiento de mensajes centralmente, pero distribuye el acceso 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 MHS puede proporcionar transferencia de mensajes centralmente, pero distribuye el almacenamiento de mensajes y acceso de usuarios [caso c) de la figura 9/X.402]. Este diseño se realiza mediante un único T/SYS y, por cada usuario, un AS/SYS sólo o un S/SYS con un A/SYS asociado.

13.2.4 *Totalmente distribuida*

El MHS puede distribuir la transferencia de mensajes [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 MHS, es decir, cómo puede realizarse el MHS 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 MHS, y se identifican unas cuantas configuraciones representativas importantes.

14.1 *Dominios de gestión*

A los bloques primarios, utilizados en la construcción de MHS, se les denomina *dominios de gestión*. Un **dominio de gestión (MD, management domain)** (o **dominio**) es un conjunto de sistemas de mensajería – por lo menos uno, que contenga o realice un MTA – 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 MD por falta de un MTA. Ese grupo de sistemas de mensajería, bloque secundario utilizado en la construcción del MHS, son de la «incumbencia» de un MD.

Los MD son de varios tipos, cada uno de los cuales se define y describe en las cláusulas que siguen.

14.1.1 *Dominio de gestión de administración*

Un **dominio de gestión de Administración (ADMD, administration management domain)** comprende varios sistemas de mensajería gestionados por una Administración. La distinción técnica principal entre un ADMD y un *PRMD* es que el primero se halla por encima del segundo en los regímenes jerárquicos de direccionamiento (véase la cláusula 18) y encaminamiento (véase la cláusula 19) del MHS.

Nota – Un ADMD proporciona tratamiento de mensajes al público.

14.1.2 *Dominio de gestión privado*

Un **dominio de gestión privado (PRMD, private management domain)** comprende sistemas de mensajería gestionados por una organización distinta de una Administración. La distinción técnica principal entre un PRMD y un ADMD es que el primero se halla por debajo del segundo en los regímenes jerárquicos de direccionamiento (véase la cláusula 18) y encaminamiento (véase la cláusula 19) del MHS.

Nota – Un PRMD 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 MD pueden combinarse de diversas maneras para constituir el MHS. 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.

14.2.1 *Totalmente centralizada*

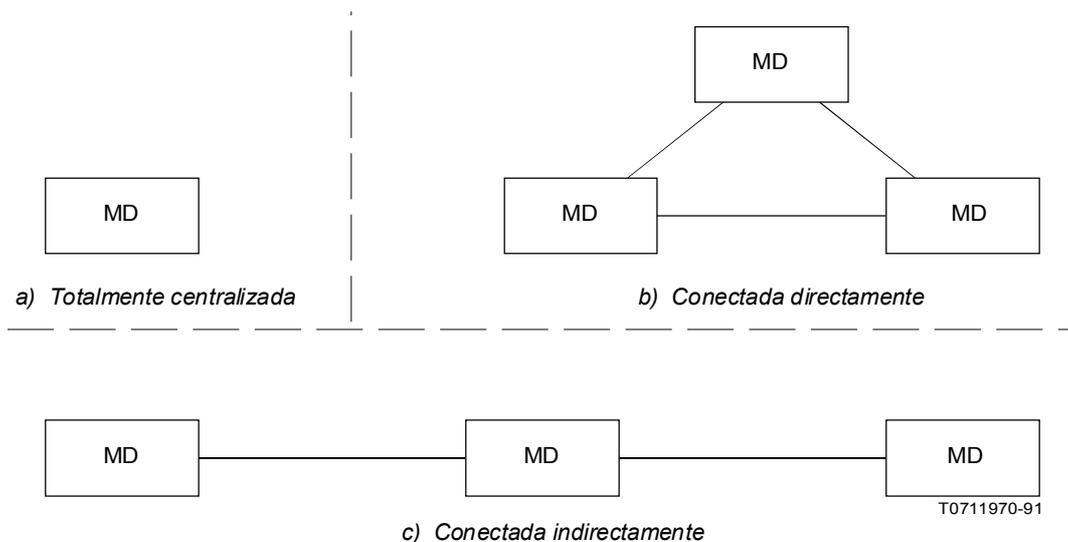
Todo el MHS puede ser gestionado por una organización [caso *a*) de la figura 10/X.402]. Este diseño se realiza mediante un único MD.

14.2.2 Conectada directamente

El MHS 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 MD interconectados por pares.

14.2.3 Conectada indirectamente

El MHS 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 MD uno de los cuales está interconectado con todos los demás.



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

15 El MHS global

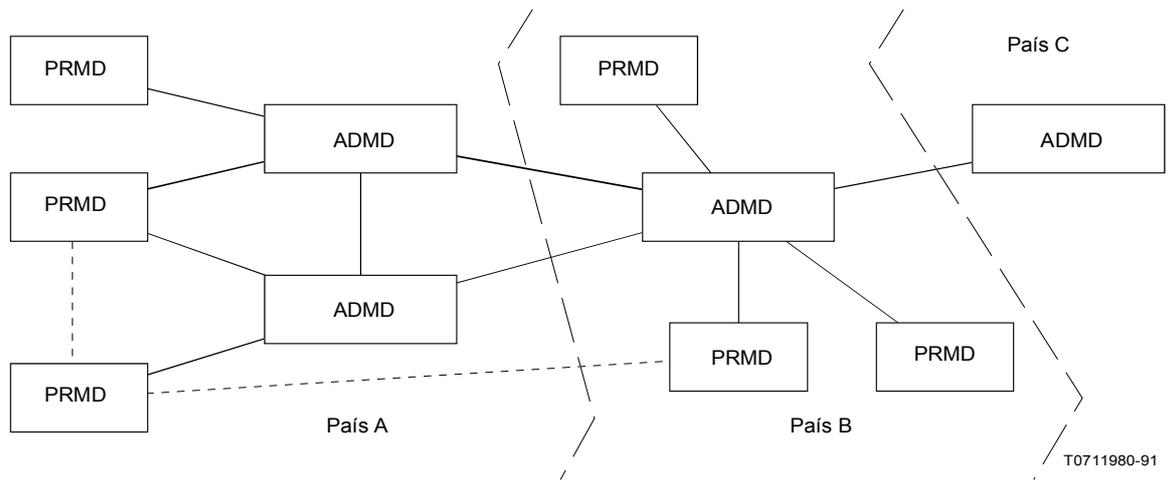
Uno de los principales objetivos de esta Recomendación y de otras Recomendaciones del CCITT es facilitar la construcción del **MHS global**, un MHS que permita el tratamiento de mensajes intra e interorganizativo, y también intra e internacional, a escala mundial.

El MHS global abarca, casi con toda seguridad, la gama completa de configuraciones funcionales especificadas en la cláusula 12.

La configuración física del MHS global es un híbrido de las configuraciones puras especificadas en la cláusula 13, sumamente complejo y con un alto grado de distribución física.

La configuración organizativa del MHS global es una combinación híbrida de las configuraciones puras especificadas en la cláusula 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 ADMD juegan un papel central en el MHS 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.



Nota – La existencia de las interconexiones representadas por las líneas de puntos entre los PRMD puede resultar afectada por la reglamentación.

FIGURA 11/X.402
El MHS global

16 Visión de conjunto

En esta sección se describen la denominación y el direccionamiento de usuarios y DL, 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 DL a efectos de tratamiento de mensajes en general y transferencia de mensajes en particular. Se definen los *nombres O/R* y se describe el papel que desempeñan en ellos los nombres de guía.

Cuando un UA o una MS depositan un mensaje o una sonda, identifican al MTS los destinatarios potenciales. Cuando el MTS entrega un mensaje, identifica el originador a cada UA o MS del destinatario potencial. Los *nombres O/R* 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/R*. El nombre de guía identifica un objeto a la guía. Presentando ese nombre a la guía, el MHS puede acceder la inscripción en la guía de un usuario o una DL. El MTS obtiene de esa inscripción, por ejemplo, la *dirección O/R* del usuario o de la DL.

No todos los usuarios o DL están inscritos en la guía y, por consiguiente, no todos ellos tienen un nombre de guía.

Nota 1 – Muchos usuarios y DL carecerán de nombre de guía mientras no se generalice la difusión de ésta, como elemento auxiliar del MHS. 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 DL 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/R típica* porque la segunda está expresada necesariamente desde el punto de vista de la estructura organizativa o física del MHS, 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 DL fuera del MHS (es decir, por otros usuarios), y que el empleo de las *direcciones O/R* se limite en gran medida al MTS (es decir, por los MTA).

17.2 Nombres O/R

Cada usuario o DL tiene uno o más *nombres O/R*. Un **nombre O/R** es un identificador por medio del cual puede un usuario ser designado como originador, o un usuario o una DL ser designados como destinatario potencial de un mensaje o sonda. El nombre O/R distingue a un usuario o una DL de otro, y puede identificar además su punto de acceso al MHS.

Un nombre O/R incluye un nombre de guía, una *dirección O/R* o ambas cosas. Si está presente y es válido, el nombre de guía identifica de manera inequívoca al usuario o a la DL (aunque no es necesariamente el único que podrá hacerlo). La *dirección O/R*, cuando existe, hace eso mismo y más (véase 18.5).

En depósito directo, el UA o la MS del originador de un mensaje o sonda pueden incluir cualquiera de los dos componentes, o ambos, en cada nombre O/R que suministran. Si se omite la *dirección O/R*, el MTS la obtiene a partir de la guía, utilizando el nombre de guía. Si se omite el nombre de guía, el MTS prescinde de él. Si se incluyen ambos, el MTS confía en primer lugar en la *dirección O/R*. Si constatará que la *dirección O/R* era inválida (por ejemplo, porque se hubiera quedado obsoleta), procedería como si la *dirección O/R* hubiera sido omitida, confiando en el nombre de guía.

En entrega, el MTS incluye una *dirección O/R* y posiblemente un nombre de guía en cada nombre O/R 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 DL ampliada.

Nota – La redirección o la ampliación de DL pueden dar lugar a que el MTS lleve a un UA o a una MS en entrega, nombres O/R que el UA o la MS no suministraron en depósito directo.

Para información sobre las organizaciones que funcionan en varios países, véase el anexo G. Véase asimismo 7.3.2 de la Rec. X.400 del CCITT | ISO/CEI 10021-1.

18 Direccionamiento

En este punto se especifica la manera de direccionar a usuarios y DL. Se definen las *direcciones O/R*, 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 DL especificada como destinatario potencial de un mensaje o una sonda, el MTS debe localizar el usuario o la DL relativos a sus propias estructuras física y organizativa. Las *direcciones O/R* son las estructuras de datos mediante las cuales se realizan todas estas localizaciones.

18.1 Lista de atributos

Las *direcciones O/R* de usuarios y DL 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 DL y que puede también ubicarlo en relación con la estructura física y organizativa del MHS (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 MD. Por tanto, el tipo y valor de un atributo-definido-por-el dominio son definidos por un MD: el MD es identificado por un *nombre-de-dominio-privado*, por un *nombre-de-dominio-de-administración*, o por ambos.

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/R más uniformes y por tanto más cómodas para el usuario. No obstante, es de prever que no todos los MD serán capaces de emplear tales atributos inmediatamente. La finalidad de los atributos definidos por el dominio es permitir a un MD que retenga durante cierto tiempo los convenios primitivos de direccionamiento existentes. Se pretende sin embargo, que todos los MD 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 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) En el caso del nombre de dominio de administración, nombre de dominio privado y código postal, el mismo valor numérico puede representarse como una cadena numérica o imprimible.
- b) Donde se permitan cadenas tanto imprimibles como teletex, podrán suministrarse cadenas de una u otra variedad. Si se suministran cadenas tanto imprimibles como teletex ambas deberán identificar sin ambigüedad al mismo usuario.

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, ASN.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 – Las reglas de paso a un grado inferior que figuran en el anexo B de la Rec. X.419 del CCITT | ISO/CEI 10021-6 estipulan que una dirección O/R no puede pasarse a un grado inferior si sólo se han suministrado cadenas teletex y contiene caracteres que están situados fuera del repertorio de la cadena imprimible.

18.3 *Atributos 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 PDS y los de la tercera, con el *direccionamiento dentro de* un PDS.

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 ADMD 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.

Atributos normalizados

Tipo de atributo normalizado	Juego de caracteres		
	NUM	PRT	TTX
<i>General</i>			
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	–	–	–
<i>Encaminamiento postal</i>			
Nombre-servicio-entrega-física	–	×	–
Nombre-país-entrega-física	×	×	–
Código-postal	×	×	–
<i>Direccionamiento postal</i>			
Componentes-ampliación-dirección-O/R 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

PRT Imprimible (*printable*)

TTX Teletex

× Permitido

a) En determinadas circunstancias, una secuencia de cadenas de octetos.

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 ADMD 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 ADMD de ese país. En relación con lo primero, es preciso que las direcciones O/R 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 ADMD de usuarios. En relación con lo segundo, ello permite que los PRMD de dentro y los ADMD de fuera del país encaminen mensajes, sondas e informes a cualquiera de ADMD de dentro del país, 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 DL 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 imprimible que da al par de caracteres asignados al país por la ISO 3166, o una cadena numérica que da uno de los números asignados al país por la Recomendación X.121.

18.3.4 *Componentes-ampliación-dirección-O/R-postal*

Componentes-ampliación-dirección-O/R-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 (PSAP).

Nota – Entre las cadenas admitidas por la Recomendación X.121 se encuentran un número télex y de teléfono precedidos por una cifra de escape.

18.3.8 *Identificador-usuario-numérico*

Identificador-usuario-numérico es un atributo normalizado que identifica numéricamente a un usuario relativo al MD, indicado por un nombre-dominio-privado o un nombre-dominio-administración; o ambos.

El valor de este atributo es una cadena numérica elegida entre un conjunto de tales cadenas, administrado para este fin por el MD aludido anteriormente.

18.3.9 *Nombre-organización*

Nombre-organización es un atributo normalizado que identifica una organización. El valor de un nombre-organización es una cadena imprimible, una cadena teletex o ambas.

Cuando se utiliza en una *dirección O/R nemotécnica* (véase 18.5.1), como asunto nacional, las organizaciones pueden identificarse con referencia al país indicado por un nombre-país (de tal modo que cada nombre-organización identifique una única entidad dentro del país) o al MD por un nombre-dominio-privado, por un nombre-dominio-administración, o por ambos.

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 MD 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.

Cuando se utiliza en una *dirección O/R terminal* (véase 18.5.4) el nombre-organización es un valor flexible, sin ningún requisito de registro.

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 MD indicado por un nombre-dominio-privado o un nombre-dominio-administración, o ambos.

El valor de este atributo es una cadena imprimible elegida de entre un conjunto de tales cadenas, administrado para este fin el MD 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 apellidos, 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 PRMD. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre de PRMD identifique una única entidad dentro del país) o referirse al ADMD 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 ADMD aludido anteriormente.

Nota – En los países en que cada nombre de PRMD 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*, *facsimil G3*, *facsimil G4*, *terminal IA5* o *videotex*.

18.3.25 *Dirección-postal-no-formatada*

Dirección-postal-no-formatada 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/R, y por tanto varias listas de atributos, pueden indicar el mismo usuario o la misma DL. Esta multiplicidad de direcciones O/R 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 tipo o valor de un atributo definido por el dominio, o el valor de un atributo normalizado conste de caracteres del repertorio de cadena imprimible, la elección que se permita entre su codificación en una cadena teletex y una cadena imprimible se considerará intrascendente.
- e) Cuando el valor de un atributo normalizado puede contener letras, los tipos de esas letras se considerarán intrascendentes.
- f) 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.
- g) En una cadena teletex el carácter gráfico de subrayado no espaciador se considerará intrascendente, así como todas las funciones de control excepto el espacio y las utilizadas para los procedimientos de ampliación de código.
- h) En una cadena teletex, la elección entre diferentes codificaciones del mismo carácter se considerará intrascendente.

Nota – Un MD puede imponer reglas de equivalencia adicionales a los atributos que asigna a sus propios usuarios y DL. 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.

18.5 *Formas de direcciones O/R*

Todo usuario o DL tiene asignadas una o más direcciones O/R. Una **dirección O/R** es una lista de atributos que distingue a un usuario de otro e identifica el punto de acceso del usuario al MHS o al punto de ampliación de la DL.

Una dirección O/R 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/R. Para cada forma de dirección O/R, la segunda columna indica los atributos que pueden aparecer en estas direcciones O/R y sus grados (véase también 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, pero una dirección postal no formatizada puede utilizarse como ampliación de la dirección terminal. La cuarta sección comprende los atributos definidos por el dominio.

Las formas de direcciones O/R, expuestas de manera resumida en el cuadro 10/X.402, se definen y describen individualmente en los puntos que siguen.

Formas de direcciones O/R

Tipos de atributos	Formas de direcciones O/R				
	MNEM	NUMR	Postal		TERM
			F	U	
<i>General</i>					
Nombre-dominio-administración	M	M	M	M	C
Nombre-común	C	-	-	-	C*
Nombre-país	M	M	M	M	C
Dirección-red	-	-	-	-	M
Identificador-usuario-numérico	-	M	-	-	-
Nombre-organización	C	-	-	-	C*
Nombre-unidades-organizativas	C	-	-	-	C*
Nombre-personal	C	-	-	-	C*
Nombre-dominio-privado	C	C	C	C	C
Identificador-terminal	-	-	-	-	C
Tipo-terminal	-	-	-	-	C
<i>Encaminamiento postal</i>					
Nombre-servicio-entrega-física	-	-	C	C	-
Nombre-país-entrega-física	-	-	M	M	-
Código-postal	-	-	M	M	-
<i>Direccionamiento postal</i>					
Componentes-ampliación-dirección-O/R 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-formatada	-	-	-	M	C*
Nombre-postal-exclusivo	-	-	C	-	-
<i>Definido por el dominio</i>					
Definido por el dominio (uno o más)	C	C	-	-	C

MNEM Nemotécnica (*mnemonic*)U No formatada (*unformatted*)NUMR Numérica (*numeric*)M Obligatoria (*mandatory*)

TERM Terminal

C Condicional

F Formatada

C* Condicional, pero concebida para utilizarse con fines de rendición y no para el direccionamiento o el encaminamiento del MHS

18.5.1 *Dirección O/R nemotécnica*

Dirección O/R nemotécnica es la que proporciona una identificación memorizable de un usuario o una DL. Identifica a un MD y a un usuario o una DL relativos a éste.

Una dirección O/R nemotécnica consta de los siguientes atributos:

- a) un nombre-país, un nombre-dominio-administración, y de manera condicional, un nombre-dominio-privado, que juntos identifican a un MD;
- b) un nombre-organización, o un nombres-unidades-organizativas, o un nombre-personal o nombre-común, uno o más atributos definidos por el dominio, o una combinación de los anteriores que, conjuntamente, identifican a un usuario o una DL relativos al MD mencionado en el apartado a). Si hay presentes nombres-unidades-organizativas, estará entonces presente el nombre-organización.

18.5.2 *Dirección O/R numérica*

Dirección O/R numérica es una dirección que identifica numéricamente a un usuario. Identifica a un MD y a un usuario relativo a él.

Una dirección O/R numérica consta de los siguientes atributos:

- a) un nombre-país, un nombre-dominio-administración y, de manera condicional, un nombre-dominio-privado, que conjuntamente identifican a un MD;
- b) un identificador-usuario-numérico, que identifica al usuario relativo al MD mencionado en el apartado 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/R postal*

Dirección O/R 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/R postales:

- a) **formatada**: Dirección O/R postal que especifica la dirección postal de un usuario mediante varios atributos. Para esta forma de dirección O/R postal, la presente Recomendación prescribe, con cierto detalle, la estructura de direcciones postales;
- b) **no formatada**: Dirección O/R postal que especifica una dirección postal de un usuario en un solo atributo. Para esta forma de dirección O/R postal, la presente Recomendación no prescribe mayormente la estructura de las direcciones postales.

Una dirección O/R postal, tanto si es formatada como si no lo es, consta de los siguientes atributos:

- a) un nombre-país, un nombre-país-administración y de manera condicional, un nombre-dominio privado, que juntos identifican a un MD;
- b) de manera condicional, un nombre-servicio-entrega-física, que identifica 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/R postal formatada comprende, además, uno de cada uno de los atributos de direccionamiento postal (véase el cuadro 9/X.402) excepto el de dirección-postal-no-formatada, que necesita el PDS para identificar el patrón postal.

Una dirección O/R postal no formatada incluye, adicionalmente, un atributo de dirección-postal-no-formatada.

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/R 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 PDAU, pero es probable que incluya delimitadores de inserción (por ejemplo, espacios) entre algunos de los valores de atributos.

18.5.4 Dirección O/R terminal

Dirección O/R 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 MD 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/R 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 MD;
- e) de manera condicional, uno o más atributos elegidos del nombre-organización, nombres-unidad-organizativa, nombre-personal, dirección postal no formatada y nombre-común y, condicionalmente asimismo, uno o más atributos definidos por el dominio, todos los cuales proporcionan información adicional para identificar 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/R particular, de los atributos señalados como condicionales en el cuadro 10/X.402, se determina según los criterios que a continuación se exponen.

Todos los atributos condicionales, excepto los específicos de las direcciones O/R postales, figuran en una dirección O/R a discreción del MD indicado por los atributos nombre-país, nombre-dominio-administración y, si estuviera presente, nombre-dominio-privado, y de acuerdo con las reglas establecidas por él.

Todos los atributos condicionales específicos de las direcciones O/R postales están presentes o ausentes en tales direcciones O/R, 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 DL, un MTA debe, no sólo localizar el usuario o la DL (es decir obtener su dirección O/R), 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 MHS que conste de un único MD, la cuestión del encaminamiento, naturalmente, no se plantea;
- b) un PRMD puede estar conectado a un único ADMD. Cuando esto ocurre, el encaminamiento implica necesariamente al ADMD;
- c) un ADMD puede estar conectado a múltiples PRMD. Si este es el caso, el encaminamiento puede basarse en atributos de dirección O/R condicionales, incluyendo el de nombre-dominio-privado, pero sin limitarse a él;
- d) un MD puede estar conectado directamente a algunos otros MD, pero no a todos. Cuando la dirección O/R identifica a un MD con el que no existe conexión directa, el encaminamiento se puede basar en *acuerdos bilaterales* con los MD con los que sí existen conexiones directas, y en otras reglas locales;
- e) cuando el MD está conectado directamente al MD identificado por la dirección O/R, el objeto es encaminado, por sistema, directamente a ese MD;

- f) por *acuerdo bilateral*, un MD podría encaminar un objeto a otro MD a efectos de, por ejemplo, conversión;
- g) un MD puede encaminar a una dirección O/R 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 MHS puede hacer de la guía, cuando se dispone de ella. Si el MHS 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 DL;
- 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 DL y cuya dirección o direcciones O/R desea obtener, presenta ese nombre a la guía y pide los siguientes atributos de la inscripción en la guía del objeto:

- a) *direcciones O/R del MHS*;
- b) *métodos de entrega preferidos del MHS*.

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 DL**

Un objeto funcional puede llevar a cabo la ampliación de una DL utilizando la guía, previa verificación de que existen los permisos de depósitos necesarios.

Para obtener los miembros de una DL 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 DL del MHS*;
- b) *permisos de depósito de DL del MHS*;
- c) *métodos de entrega preferidos del MHS*.

Para hacerlo de manera satisfactoria, el MTA 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 MS 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 MHS;*
- b) *tipos de contenido entregables del MHS;*
- c) *EIT entregables del MHS;*
- d) *métodos de entrega preferidos del MHS.*

Los atributos de guía siguientes representan capacidades de MS de posible importancia en el tratamiento de mensajes:

- a) *acciones automáticas facilitadas por el MHS;*
- b) *tipos de contenido facilitados por el MHS;*
- c) *atributos facultativos facilitados por el MHS.*

Para evaluar determinada capacidad de un usuario o MS 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 MTA debe primero autenticarse él mismo a la guía y tener derechos de acceso a la información solicitada.

SECCIÓN 6 – REALIZACIÓN POR OSI

25 Visión de conjunto

En esta sección se describe cómo se realiza el MHS por medio de la OSI.

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 (ASE) que figuran en la realización mediante OSI del tratamiento de mensajes.

En la OSI, las capacidades de comunicación de sistemas abiertos se organizan en grupos de capacidades relacionadas, llamados ASE. En la presente sección, se examina este concepto, a partir del modelo de referencia OSI, se establece una distinción entre ASE *simétricos* y *asimétricos* y se presentan los ASE definidos para el tratamiento de mensajes o que le sirven de apoyo.

Nota – El MHS depende no sólo de los ASE examinados, sino también del elemento de servicio de acceso a la guía, definido en la Rec. X.519 del CCITT | ISO/CEI 9594-6. Sin embargo, como este ASE no figura en los AC para tratamiento de mensajes (véase la Rec. X.419 del CCITT | ISO/CEI 10021-6), no se analiza aquí.

La figura 12/X.402 ilustra el concepto de ASE. En ella se representan de manera esquemática dos sistemas abiertos en comunicación. Sólo se muestran las partes de los sistemas abiertos relacionados con la OSI, a las que se llama entidades de aplicación (AE). Cada AE consta de un UE y de uno o más ASE. El UE representa la parte organizativa o de control de una AE, que define el cometido del sistema abierto (por ejemplo, el de un MTA). Por su parte, un ASE representa uno de los conjuntos de capacidad de comunicaciones, o servicios (por ejemplo, depósito o transferencia de mensajes), que el UE necesita para desempeñar su cometido.

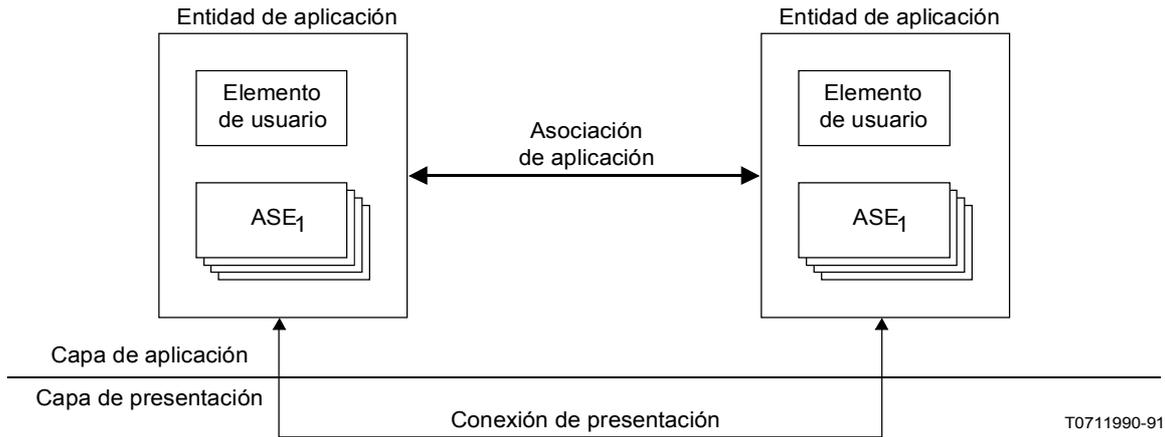


FIGURA 12/X.402
El concepto de ASE

A la relación entre dos AE en sistemas abiertos diferentes se le llama asociación de aplicación. Los ASE de un sistema abierto se comunican con sus ASE 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 ASE se combinen de manera satisfactoria en una única AE, deben estar diseñados de manera que coordinen su utilización de la asociación de aplicación.

Un ASE desempeña el papel, en gran medida mecánico, de trasladar las peticiones formuladas por su UE, y las respuestas, a y desde la forma dictada por el protocolo de aplicación que gobierna la interacción del ASE con su ASE par del sistema abierto al que la asociación le conecta. El ASE efectúa un servicio, o una parte del mismo, abstracto, a efectos de comunicación de la OSI (véase la Rec. X.407 del CCITT | ISO/CEI 10021-3).

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 la cláusula 7. A su vez, un UE es una parte de un proceso de aplicación.

26.2 ASE simétricos y asimétricos

Cabe distinguir los siguientes dos tipos de ASE, ilustrados en la figura 13/X.402:

- a) **simétrico**: ASE por medio del cual un UE suministra y consume un servicio. El ASE para transferencia de mensajes, por ejemplo, es simétrico, porque ambos sistemas abiertos, cada uno de los cuales incorpora un MTA, ofrece y puede consumir por medio de él el servicio de transferencia de mensajes;

- b) **asimétrico**: ASE por medio del cual un UE suministra y consume un servicio, pero no ambas cosas; dependiendo de cómo esté configurado el ASE. El ASE para entrega de mensajes, por ejemplo, es asimétrico, porque sólo el sistema abierto que incorpora un MTA ofrece el servicio asociado, y sólo el otro sistema abierto, que incorpora un AU o una MS, lo consume.

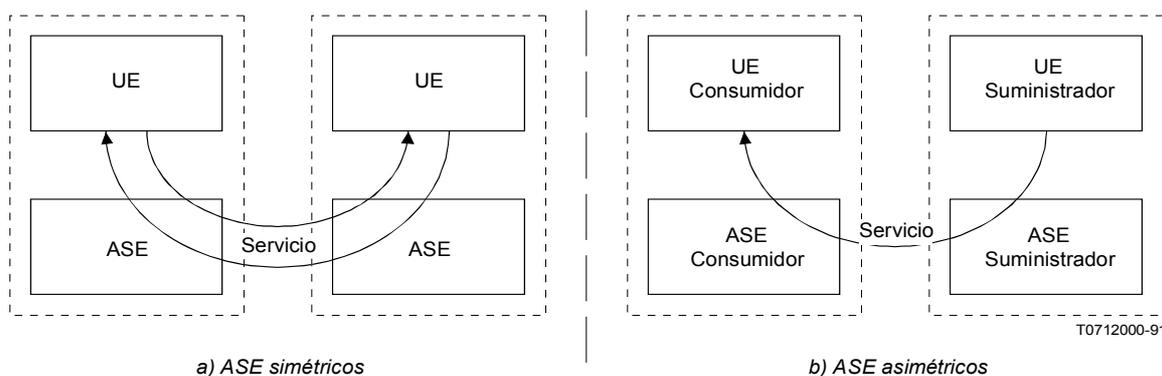


FIGURA 13/X.402
ASE simétricos y asimétricos

Con respecto a un determinado ASE asimétrico, un UE suministra un servicio que el otro consume. Los ASE, coubicados con los UE, ayudan en el suministro y consumo del servicio. Los cuatro papeles resultantes se muestran en la figura 14/X.402, con la siguiente terminología:

- UE suministrador de x**: Proceso de aplicación que suministra el servicio representado por el ASE asimétrico x .
- ASE suministrador de x**: ASE asimétrico x configurado para coubicación con un UE suministrador de x .
- UE consumidor de x**: Proceso de aplicación que consume el servicio representado por el ASE asimétrico x .
- ASE consumidor de x**: ASE asimétrico x configurado para coubicación con un UE consumidor de x .

Como se ha indicado, los cuatro papeles descritos anteriormente están definidos en relación con un determinado ASE. Cuando una AE consta de varios ASE asimétricos, estos papeles se asignan independientemente a cada ASE. Así, tal como se muestra en la figura 15/X.402, un único UE podría servir como consumidor con respecto a un ASE y como suministrador con respecto a otro.

26.3 ASE de tratamiento de mensajes

En la primera columna del cuadro 11/X.402 figura la lista de los ASE que proporcionan los diversos servicios del tratamiento de mensajes. Para cada ASE de la primera columna, se indica en la segunda si es simétrico o asimétrico. La tercera columna identifica los objetos funcionales –UA, MS, MTA y AU– que están asociados al ASE, como consumidores o como suministradores.

Los ASE de tratamiento de mensajes, resumidos en el cuadro 11/X.402, se presentan por separado en las subcláusulas que siguen. En la Rec. X.419 del CCITT | ISO/CEI 10021-6 figuran sus definiciones.

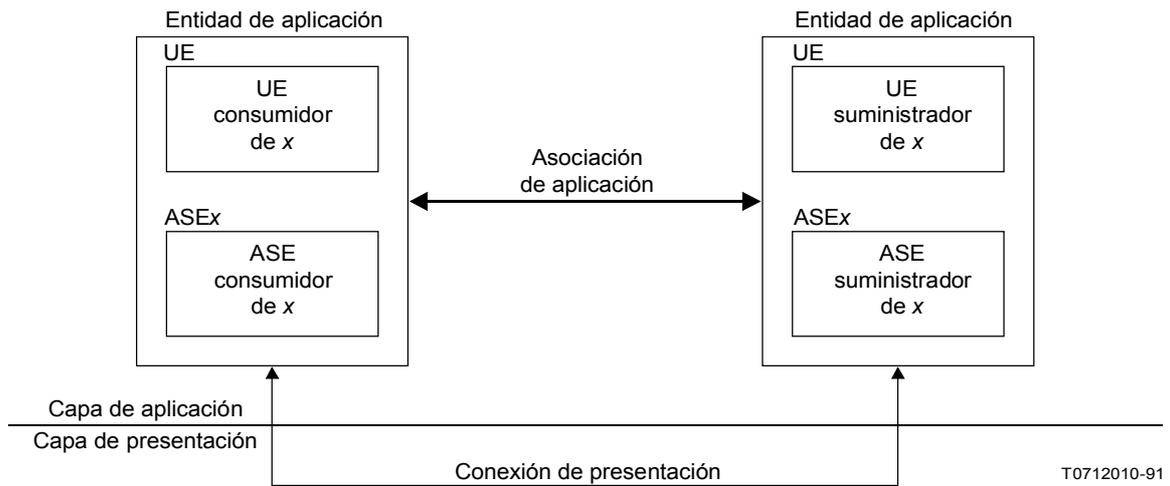


FIGURA 14/X.402
Terminología para ASE asimétricos

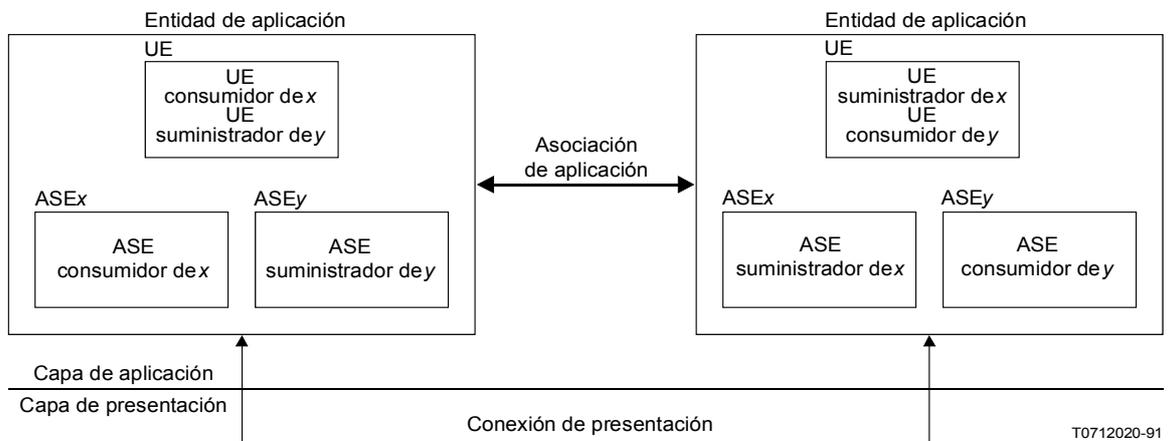


FIGURA 15/X.402
ASE asimétricos múltiples

26.3.1 Transferencia de mensajes

El elemento de servicio transferencia de mensajes (MTSE, *message transfer service element*) 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 (MSSE, *message submission service element*) es el medio por el cual se efectúa el paso de transmisión de depósito.

CUADRO 11/X.402

ASE de tratamiento de mensajes

ASE	Forma	Objetos funcionales			
		UA	MS	MTA	AU
MTSE	SY	–	–	CS	–
MSSE	ASY	C	CS	S	–
MDSE	ASY	C	C	S	–
MRSE	ASY	C	S	–	–
MASE	ASY	C	CS	S	–

SY Simétrico (*symetric*)

ASY Asimétrico (*asymetric*)

C Consumidor (*consumer*)

S Suministrador (*supplier*)

26.3.3 Entrega de mensajes

El elemento de servicio entrega de mensajes (MDSE, *message delivery service element*) 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 (MRSE, *message retrieval service element*) 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 (MASE, *message administration service element*) es el medio por el cual un UA, una MS o MTA archiva, en cada uno de los otros dos la información que facilita y controla su interacción subsiguiente, mediante el MSSE, MDSE, el MRSE y el MASE.

26.4 ASE de apoyo

En la primera columna del cuadro 12/X.402 figura la lista de los ASE de uso general, de los que dependen los ASE de tratamiento de mensajes. Para cada ASE de la primera columna, se indica en la segunda si es simétrico o asimétrico.

Los ASE de apoyo, resumidos en el cuadro 12/X.402 se presentan por separado en las subcláusulas que siguen.

CUADRO 12/X.402

ASE de apoyo

ASE	Forma
ROSE	SY
RTSE	SY
ACSE	SY

SY Simétrico (*symetric*)

26.4.1 *Operaciones distantes*

El elemento de servicio de operaciones a distancia (ROSE) es el medio por el cual, los ASE asimétricos de tratamiento de mensajes, estructuran sus interacciones de petición-respuesta, entre sistemas abiertos consumidores y suministradores.

El ROSE se define en la Rec. X.219 del CCITT | ISO/CEI 9072-1.

26.4.2 *Transferencia fiable*

El elemento de servicio transferencia fiable (RTSE) es el medio por el cual diversos ASE 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 RTSE se define en la Rec. X.218 del CCITT | ISO/CEI 9066-1.

26.4.3 *Control de asociación*

El elemento de servicio control de asociación (ACSE) 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 ACSE se define en la Rec. X.217 del CCITT | ISO 8649.

27 **Contextos de aplicación**

En la OSI, las capacidades de comunicación (es decir, los ASE) de dos sistemas abiertos son dirigidos, para un fin determinado, mediante contextos de aplicación (AC). Un AC es una especificación detallada del empleo de una asociación entre dos sistemas abiertos, es decir, un protocolo.

Un AC especifica cómo debe establecerse la asociación (por ejemplo, qué parámetros de inicialización se deben intercambiar), qué ASE 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 ASE asimétrico es el iniciador o el contestador y cómo puede liberarse la asociación (por ejemplo, qué parámetros de finalización se deben intercambiar).

Todo AC tiene asignado un nombre (un identificador de objeto ASN.1). El iniciador de una asociación indica al contestador cuál es el AC que dirigirá el uso de la asociación, haciéndole llegar el nombre del AC por medio del ACSE.

Un AC identifica también con un nombre (un identificador de objeto ASN.1) las sintaxis abstractas de las APDU que puede llevar una asociación, como resultado de su utilización por los ASE del AC. De manera convencional, se asigna un nombre bien al conjunto de las APDU asociadas a cada ASE individual o bien al AC como un todo. El iniciador de una asociación indica al contestador la o las sintaxis abstractas, enviándole sus nombres por medio del ACSE.

Las sintaxis abstractas de una APDU es su estructura como objeto de información (por ejemplo, un conjunto ASN.1 que comprenda un código de instrucción entero y un argumento de instrucción cadena IA5). Se diferencia de la sintaxis de transferencia de la APDU, que es como se representa el objeto de información para transmisión entre dos sistemas abiertos (por ejemplo, un octeto indicando un conjunto ASN.1, seguido por un octeto que dé la longitud del conjunto, etc.).

Los AC, por medio de los cuales se proporcionan los diversos servicios de tratamiento de mensajes, se especifican en la Rec. X.419 del CCITT | ISO/CEI 10021-6 A estos protocolos (P, *protocols*) se les conoce por P1, P3 y P7.

Nota – La naturaleza del contenido de un mensaje no entra en la definición del AC 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 X.402)

Clases de objetos de guía y atributos

(Este anexo es parte integrante de esta 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 Rec. X.501 del CCITT | ISO/CEI 9594-2.

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 Rec. X.521 del CCITT | ISO/CEI 9594-7. En la cláusula 9 de la Rec. X.501 del CCITT | ISO/CEI 9594-2 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 Rec. X.521 del CCITT | ISO/CEI 9594-7 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 MHS*

Un objeto **lista de distribución del MHS** es una DL. Los atributos de su inscripción identifican su nombre común, permisos de depósito y direcciones O/R y, en la medida en que estén presentes los atributos pertinentes, describen la DL, identifican su organización, sus unidades organizativas y su propietario, mencionan objetos relacionados e identifican sus tipos de contenido entregable, EIT 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,  
    organizationName,  
    organizationalUnitName,  
    owner,  
    seeAlso,  
    mhs-deliverable-content-types,  
    mhs-deliverable-eits,  
    mhs-dl-members,  
    mhs-preferred-delivery-methods }  
::= id-oc-mhs-distribution-list
```

A.1.2 *Memoria de mensajes del MHS*

Un objeto **memoria de mensajes del MHS** es una AE que realiza una MS. Los atributos de su inscripción, en la medida en que estén presentes, describen la MS, 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 applicationEntity  
MAY CONTAIN {  
    owner,  
    mhs-supported-optional-attributes,  
    mhs-supported-automatic-actions,  
    mhs-supported-content-types }  
::= id-oc-mhs-message-store
```

A.1.3 *Agente de transferencia de mensajes del MHS*

Un objeto **agente de transferencia de mensajes del MHS** es una AE que pone en ejecución un MTA. Los atributos de su inscripción, en la medida que estén presentes, describen el MTA e identifican a su propietario y la longitud de su contenido entregable.

```
mhs-message-transfer-agent OBJECT-CLASS  
SUBCLASS OF applicationEntity  
MAY CONTAIN {  
    owner,  
    mhs-deliverable-content-length }  
::= id-oc-mhs-message-transfer-agent
```

A.1.4 *Usuario del MHS*

Un objeto **usuario del MHS** es un usuario genérico del MHS (el usuario genérico del MHS puede tener, por ejemplo, una dirección comercial, o una dirección privada, o ambas). Los atributos de su inscripción identifican la dirección O/R 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 EIT, su MS y sus métodos de entrega preferidos.

```
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-dn,  
    ::= id-oc-mhs-user
```

Nota – La información método de entrega preferido es heredada en el juego de atributos de telecomunicaciones de la clase de objeto de denominación de usuario de guía.

A.1.5 *Agente de usuario del MHS*

Un objeto **agente de usuario del MHS** es una AE que realiza un UA. Los atributos de su inscripción, en la medida en que estén presentes, identifican al propietario del UA, la longitud de su contenido entregable, tipos de contenido y EIT, y su dirección O/R.

```
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 MHS*

El atributo **longitud de contenido entregable del MHS** 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 MHS*

El atributo **tipos de contenido entregable del MHS** 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 *EIT entregables del MHS*

El atributo **EIT entregables del MHS** identifica los EIT 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 objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-eits

A.2.4 *Miembros de DL del MHS*

El atributo **miembros de DL del MHS** identifica los miembros de una DL.

Un valor de este atributo es un nombre O/R.

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 DL del MHS*

El atributo **permisos de depósito de DL del MHS** identifica los usuarios y las DL que pueden depositar mensajes a una DL.

Un valor de este atributo es un permiso de depósito de DL.

mhs-dl-submit-permissions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
MULTI VALUE
::= id-at-mhs-dl-submit-permissions

A.2.6 *Nombre de guía-Memoria de mensajes del MHS*

El atributo **nombre de guía-memoria de mensajes del MHS** identifica una MS de usuario por un nombre.

El valor de este atributo es un nombre distinguido de guía.

mhs-message-store-dn ATTRIBUTE
WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
SINGLE VALUE
::= id-at-mhs-message-store-dn

A.2.7 *Direcciones O/R del MHS*

El atributo **direcciones O/R del MHS** especifica las direcciones O/R de un usuario o de una DL.

Un valor de este atributo es una dirección O/R.

mhs-or-addresses ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
MULTI VALUE
::= id-at-mhs-or-addresses

A.2.8 Acciones automáticas permitidas por el MHS

El atributo **acciones automáticas permitidas por el MHS** identifica las acciones automáticas que un MS 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.2.9 Tipos de contenido permitidos por el MHS

El atributo **tipos de contenido permitidos por el MHS** identifica los tipos de contenido de los mensajes cuya sintaxis semántica permite totalmente una MS.

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.2.10 Atributos facultativos permitidos por el MHS

El atributo **atributos facultativos permitidos por el MHS** identifica los atributos facultativos que permite totalmente una MS.

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 DL del MHS

La sintaxis de atributo **permiso de depósito de DL del MHS** 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 DL presentado será del tipo *individual*.

Un permiso de depósito de DL concede, dependiendo de su tipo, acceso de presentación a los cero o más usuarios o listas de distribución siguientes:

- Individual*: Usuario o DL (no ampliada) alguno de cuyos nombres O/R es igual al nombre O/R especificado.
- Miembro-de-dl*: Cada miembro de la DL, o de cada DL jerarquizada de manera recurrente, alguno de cuyos nombres O/R es igual al nombre O/R especificado.
- Concordancia-de-esquemas*: Cada usuario o DL (no ampliada) alguno de cuyos nombres O/R satisface el esquema de nombres O/R 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/R del MHS*

La sintaxis del atributo **dirección O/R del MHS** caracteriza a un atributo cada uno de cuyos valores es una dirección O/R.

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX  
SYNTAX ORAddress  
MATCHES FOR EQUALITY  
::= id-as-mhs-or-address
```

Un valor de dirección O/R presentado es igual a un valor de dirección O/R objetivo en las condiciones especificadas en 18.4.

A.3.3 *Nombre O/R del MHS*

La sintaxis del atributo **nombre O/R del MHS** caracteriza a un atributo cada uno de cuyos valores es un nombre O/R.

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX  
SYNTAX ORName  
MATCHES FOR EQUALITY  
::= id-as-mhs-or-name
```

Un valor de nombre O/R presentado es igual a un valor de nombre O/R 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 es parte integrante de esta Recomendación)

En él se definen, a efectos de referencia, diversos identificadores de objetos mencionados en el módulo ASN.1 de los anexos A y C. Se utiliza ASN.1.

Todos los identificadores de objetos asignados por esta Recomendación lo son en el presente anexo. Este anexo es definitivo para todos, excepto para los de los módulos del ASN.1 y del propio MHS. 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 MHS
```

```
id-mhs-protocols ID ::= { joint-iso-ccitt mhs-motis(6) protocols(0) }
```

```
-- Contextos y protocolos de aplicación del MHS  
-- Véase la Rec. X.419 del CCITT | ISO/CEI 10021-6.
```

```
id-ipms ID ::= { joint-iso-ccitt mhs-motis(6) ipms (1) }
```

-- Mensajería interpersonal
-- Véase la Rec. X.420 del CCITT | ISO/CEI 10021-7.
id-asdc ID ::= { joint-iso-ccitt mhs-motis(6) asdc (2) }

-- Convenios de definición de servicio abstracto
-- Véase la Rec. X.407 del CCITT | ISO/CEI 10021-3.
id-mts ID ::= { joint-iso-ccitt mhs-motis(6) mts (3) }

-- Sistema de transferencia de mensajes
-- Véase la Rec. X.411 del CCITT | ISO/CEI 10021-4.
id-ms ID ::= { joint-iso-ccitt mhs-motis(6) ms (4) }

-- Memoria de mensajes
-- Véase la Rec. X.413 del CCITT | ISO/CEI 10021-5.
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-dn ID ::= { id-at 5 }
id-at-mhs-or-addresses ID ::= { id-at 6 }
- El valor { id-at 7 } ya no está definido
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 MHS

ANEXO C
(a la Recomendación X.402)

Definición de referencia de clases de objetos de guía y atributos

(Este anexo es parte integrante de esta 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 Rec. X.501 del CCITT | ISO/CEI 9594-2.

**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 MHS

**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-dn, 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) }**

-- Servicio abstracto del MHS (de la Rec. X.411)

ORAddress, ORName, RequestedDeliveryMethod

**FROM MTSAbstractService { joint-iso-ccitt
mhs-motis(6) mts(3) modules(0) mts-abstract-service(1) }**

-- Marco de información (de la Rec. X.501)

ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS

**FROM InformationFramework { joint-iso-ccitt
ds(5) modules(1) informationFramework(1) }**

-- Clases de objeto seleccionadas (de la Rec. X.521)

applicationEntity, top

FROM SelectedObjectClasses { joint-iso-ccitt ds(5) modules(1) selectedObjectClasses(6) }

-- Tipos de atributo seleccionados (de la Rec. X.520)

**commonName, description, distinguishedNameSyntax, integerSyntax, objectIdentifiersSyntax,
organization, organizationalUnitName, owner, seeAlso**

FROM SelectedAttributeTypes { joint-iso-ccitt ds(5) modules(1) selectedAttributeTypes(5) };

-- CLASES DE OBJETOS

-- Lista de distribución del MHS

**mhs-distribution-list OBJECT-CLASS
SUBCLASS OF top
MUST CONTAIN {
commonName,
mhs-dl-submit-permissions,
mhs-or-addresses }**

```
MAY CONTAIN {
    description,
    organizationName,
    organizationalUnitName,
    owner,
    seeAlso,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-dl-members,
    mhs-preferred-delivery-methods }
::= id-oc-mhs-distribution-list
```

-- Memoria de mensajes del MHS

```
mhs-message-store OBJECT-CLASS
SUBCLASS OF applicationEntity
MAY CONTAIN {
    owner,
    mhs-supported-optional-attributes,
    mhs-supported-automatic-actions,
    mhs-supported-content-types }
::= id-oc-mhs-message-store
```

-- Agente de transferencia de mensajes del MHS

```
mhs-message-transfer-agent OBJECT-CLASS
SUBCLASS OF applicationEntity
MAY CONTAIN {
    owner,
    mhs-deliverable-content-length }
::= id-oc-mhs-message-transfer-agent
```

-- Usuario del MHS

```
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-dn,
::= id-oc-mhs-user
```

-- Agente de usuario del MHS

```
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 MHS

```
mhs-deliverable-content-length ATTRIBUTE
WITH ATTRIBUTE-SYNTAX integerSyntax
SINGLE VALUE
::= id-at-mhs-deliverable-content-length
```

-- Tipos de contenido entregable del MHS

mhs-deliverable-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-content-types

-- EIT entregables del MHS

mhs-deliverable-eits ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-deliverable-eits

-- Miembros de DL del MHS

mhs-dl-members ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
MULTI VALUE
::= id-at-mhs-dl-members

-- Permisos de depósito de DL del MHS

mhs-dl-submit-permissions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
MULTI VALUE
::= id-at-mhs-dl-submit-permissions

-- Direcciones O/R del MHS

mhs-or-addresses ATTRIBUTE
WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
MULTI VALUE
::= id-at-mhs-or-addresses

-- Nombre de guía de memoria de mensajes del MHS

mhs-message-store-dn ATTRIBUTE
WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
SINGLE VALUE
::= id-at-mhs-message-store-dn

-- Acciones automáticas admitidas por el MHS

mhs-supported-automatic-actions ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-automatic-actions

-- Tipos de contenido admitidos por el MHS

mhs-supported-content-types ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-content-types

-- Atributos facultativos admitidos por el MHS

mhs-supported-optional-attributes ATTRIBUTE
WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
MULTI VALUE
::= id-at-mhs-supported-optional-attributes

-- SINTAXIS DE ATRIBUTO

-- Permiso de presentación de DL de MHS

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/R del MHS

```
mhs-or-address-syntax ATTRIBUTE-SYNTAX
SYNTAX ORAddress
MATCHES FOR EQUALITY
::= id-as-mhs-or-address
```

-- Nombre O/R del MHS

```
mhs-or-name-syntax ATTRIBUTE-SYNTAX
SYNTAX ORName
MATCHES FOR EQUALITY
::= id-as-mhs-or-name
```

END -- final de la guía del MHS

ANEXO D

(a la Recomendación X.402)

Amenazas contra la seguridad

(Este anexo no es parte de esta Recomendación)

En la subcláusula 15.1 de la Rec. X.400 del CCITT | ISO/CEI 10021-1 se da una visión general de las amenazas contra la seguridad del MHS. En esta Recomendación se consideran las amenazas tal como se plantean en el MHS: 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 MHS.

Además, las amenazas pueden surgir por accidente o intento doloroso, y pueden tener un carácter activo o pasivo. Las agresiones al MHS 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 MHS. La lista de amenazas que aquí se da es indicativa, no definitiva.

Utilización de los servicios de seguridad del MHS

Amenaza	Servicios
<p><i>Suplantación</i></p> <p>Simulación y mal uso del MTS</p> <p>Falso acuse de recibo</p> <p>Falsa originación de un mensaje</p> <p>Simulación de un MTA a un usuario del MTS</p> <p>Simulación de un MTA a otro MTA</p>	<p>Autenticación de origen de mensajes</p> <p>Autenticación de origen de sondas</p> <p>Gestión de acceso seguro</p> <p>Prueba de entrega</p> <p>Autenticación de origen de mensajes</p> <p>Prueba de depósito</p> <p>Autenticación de origen de informes</p> <p>Gestión de acceso seguro</p> <p>Autenticación de origen de informes</p> <p>Gestión de acceso seguro</p>
<p><i>Secuenciación de mensajes</i></p> <p>Reactuación de mensajes</p> <p>Reordenación de mensajes</p> <p>Adelanto de mensajes</p> <p>Retraso de mensajes</p>	<p>Integridad de secuencia de mensajes</p> <p>Integridad de secuencia de mensajes</p>
<p><i>Modificación de información</i></p> <p>Modificación de mensajes</p> <p>Destrucción de mensajes</p> <p>Degradación del encaminamiento y de otra información de gestión</p>	<p>Integridad de conexión</p> <p>Integridad de contenido</p> <p>Integridad de secuencia de mensajes</p>
<p><i>Denegación de servicio</i></p> <p>Denegación de comunicaciones</p> <p>Saturación de MTA</p> <p>Saturación del MTS</p>	
<p><i>Rechazo</i></p> <p>Denegación de origen</p> <p>Denegación de depósito</p> <p>Denegación de entrega</p>	<p>No rechazo de origen</p> <p>No rechazo de depósito</p> <p>No rechazo de entrega</p>
<p><i>Fuga de información</i></p> <p>Pérdida de confidencialidad</p> <p>Pérdida de anonimato</p> <p>Apropiación indebida de mensajes</p> <p>Análisis del tráfico</p>	<p>Confidencialidad de conexión</p> <p>Confidencialidad de contenido</p> <p>Confidencialidad de flujo de mensajes</p> <p>Gestión de acceso seguro</p> <p>Confidencialidad de flujo de mensajes</p>
<p><i>Otras amenazas</i></p> <p>Originador no autorizado para etiqueta de seguridad de mensajes</p> <p>Usuario MTA/MTS no autorizado para el contexto de seguridad</p> <p>Encaminamiento erróneo</p> <p>Procedimientos de etiquetado diferentes</p>	<p>Gestión de acceso seguro</p> <p>Etiquetado de seguridad de mensajes</p> <p>Gestión de acceso seguro</p> <p>Gestión de acceso seguro</p> <p>Etiquetado de seguridad de mensajes</p>

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 MTS puede simular a otro para acceder sin permiso a las facilidades del MTS, o actuar en detrimento de un usuario válido, por ejemplo, desechando sus mensajes. Un usuario del MTS puede suplantar a otro y acusar recibo, falsamente, de un mensaje en nombre del receptor «válido». Un mensaje puede ser introducido en el MTS por un usuario que utilice falsamente la identidad de otro. Un usuario del MTS, un MS o un MTA se pueden enmascarar como si fuesen un usuario, un MS o un MTA distintos.

Entre las amenazas de tipo suplantación figuran las siguientes:

- a) simulación y mal uso del MTS;
- b) falso acuse de recibo;
- c) falsa originación de un mensaje;
- d) simulación de un MTA a un usuario del MTS;
- e) simulación de un MTA a otro MTA.

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 MHS 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 MTA o utilizada por ellos, puede dar lugar a que el MTS 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 MTS si se provoca el fallo o el funcionamiento incorrecto de un MTA. Además, un usuario del MTS puede dar lugar a que dicho servicio se deniegue a otro usuario, saturándolo con mensajes que podrían sobrecargar la capacidad de conmutación de un MTA 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 MTA;
- c) saturación del MTS.

D.5 *Rechazo*

El rechazo tiene lugar cuando un usuario del MTS o el propio MTS 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 MHS o por suplantación. En algunos casos, la presencia en el sistema de un usuario del MTS puede ser un asunto delicado y debe preservarse su anonimato. También es posible que un usuario del MTS 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 MTS, o de haber provocado el funcionamiento incorrecto de un MTA. Además, observando el tráfico se pueden obtener otros detalles sobre la información que fluye por un MTS.

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 MTS origine un mensaje y le asigne una etiqueta para la que no está autorizado. Cabe también que un usuario del MTS o un MTA 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 MTA/MTS no autorizado para el contexto;
- c) encaminamiento erróneo;
- d) procedimientos de etiquetado diferentes.

ANEXO E

(a la Recomendación X.402)

Provisión de servicios de seguridad en la Rec. X.411 del CCITT | ISO/CEI 10021-4

(Este anexo es parte integrante de esta Recomendación)

En el cuadro E-1/X.402 se indica qué elementos de servicio de la Rec. X.411 del CCITT | ISO/CEI 10021-4 pueden utilizarse para facilitar los servicios de seguridad descritos en 10.2.

CUADRO E-1/X.402

Provisión de servicios de seguridad del MHS

Servicio	Argumentos/servicios del MTS
<i>Servicios de seguridad de autenticación de origen</i> Autenticación de origen de mensajes Autenticación de origen de sondas Autenticación de origen de informes Prueba de depósito Prueba de entrega	Verificación de autorización de origen de mensajes Testigo de mensajes Verificación de autenticación de origen de sondas Verificación de autenticación de origen de informes Petición de prueba de depósito Prueba de depósito Petición de prueba de entrega Prueba de entrega
<i>Servicios de seguridad de gestión de acceso seguro</i> Autenticación de entidades pares Contexto de seguridad	Credenciales de iniciador Credenciales de respondedor Contexto de seguridad
<i>Servicios de seguridad de confidencialidad de datos</i> Confidencialidad de conexiones Confidencialidad de contenidos Confidencialidad del flujo de mensajes	No proporcionado Identificador del algoritmo de confidencialidad de contenidos Testigo de mensajes Tipo de contenido
<i>Servicios de seguridad de integridad de datos</i> Integridad de conexiones Integridad de contenidos Integridad de secuencia de mensajes	No proporcionado Verificación de integridad de contenidos Testigo de mensajes Verificación de autenticación de origen de mensajes Número de secuencia de mensajes Testigo de mensajes
<i>Servicios de seguridad de no rechazo</i> No rechazo de origen No rechazo de depósito No rechazo de entrega	Verificación de integridad de contenido Testigo de mensajes Verificación de autenticación de origen de mensajes Petición de prueba de depósito Prueba de depósito 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
<i>Servicios de seguridad de gestión de la seguridad</i> Cambio de credenciales Registros	Cambio de credenciales Registros

ANEXO F

(a la Recomendación X.402)

Representación de las direcciones O/R para su utilización por el hombre

(Este anexo no es parte integrante de esta Recomendación)

Este material figura en el anexo B a la Recomendación F. 401.

ANEXO G

(a la Recomendación X.402)

La utilización de direcciones O/R por parte de las organizaciones multinacionales

(Este anexo no es parte integrante de esta Recomendación)

Véase asimismo el anexo E de la Rec. F.400.

Está admitido que, cuando las reglamentaciones lo permiten, muchas organizaciones pueden desear explotar sistemas de transmisión de mensajes que están situados en más de un país. Estas organizaciones pueden ser organizaciones privadas y proveedores del servicio MH de carácter público. Las políticas de direccionamiento y encaminamiento de los mencionados sistemas deben ser compatibles con el modelo general MHS, para asegurar el interfuncionamiento con el resto del sistema.

La existencia de servicios de guía puede influir considerablemente en las políticas de direccionamiento que las organizaciones decidan adoptar. Si se dispone de un servicio de guía universal, es posible referirse a los originadores y destinatarios de los mensajes mediante un nombre de guía sencillo; el sistema de transmisión de mensaje permite obtener las direcciones O/R en la guía. En este caso los usuarios humanos no necesitan recurrir a los valores de dirección O/R utilizados, y la política de direccionamiento puede decidirse con arreglo a criterios puramente técnicos. Si no se dispone de un servicio de guía de este tipo, será necesario que los usuarios traten las direcciones O/R de forma manual. En este caso, las consideraciones estéticas y otros factores humanos han de influir igualmente en la selección de la política de direccionamiento.

G.1 *Principios de direccionamiento*

Es posible obtener que los nombres de MHS tengan un carácter inequívoco, a nivel mundial, mediante una estructura de registro jerárquica y la aplicación constante de convenciones sobre denominación. Ello implica que, cada vez que se use una dirección O/R, es necesario registrar los valores de atributo de dirección con arreglo a los procedimientos aplicables para el país indicado por el valor del atributo nombre-país. En el caso del nombre-dominio-privado y nombre-dominio-administración, ello exige el registro ante las autoridades de registro competentes en ese país o dominio. Estos principios sientan la base de la mensajería mundial.

La interconexión de dominios (PRMD a ADMD, ADMD a ADMD, PRMD a PRMD) está sujeta a acuerdos bilaterales. Dichos acuerdos dependen de criterios comerciales y técnicos; entre otras cuestiones, estos convenios pueden especificar la gama de valores de dirección O/R que están aceptados.

Cuando una organización exige nombres de dominios con más de un código de país, es necesario registrar los nombres de conformidad con los procedimientos en cada país. Con frecuencia será posible registrar el mismo valor de nombre-dominio-privado (o nombre-dominio-administración, según corresponda) en cada país; con todo, por factores ajenos al alcance del MHS (como la propiedad jurídica del nombre) a veces será necesario que una organización supra nacional utilice valores diferentes para su nombre-dominio, con arreglo al código de país utilizado.

Lo ideal para los usuarios de MHS sería tener una dirección que pudieran utilizar en la mensajería mundial y que estuviera consignada en los membretes y tarjetas comerciales (que indique el país en que está situado el usuario), y que sus potenciales asociados puedan utilizar en sus comunicaciones por conducto de los sistemas MHS. La posibilidad de llegar a interlocutores distantes por conducto de un proveedor de servicios depende de las posibilidades de conexión que existan.

G.2 Ejemplos de configuraciones

Las organizaciones multinacionales pueden optar por organizar sus sistemas de mensajería en cualquier forma que sea compatible con estos principios básicos. Entre los ejemplos de configuraciones posibles de un PRMD Multinacional pueden citarse:

G.2.1 PRMD independientes múltiples

Veáse la figura G-1/X.401.

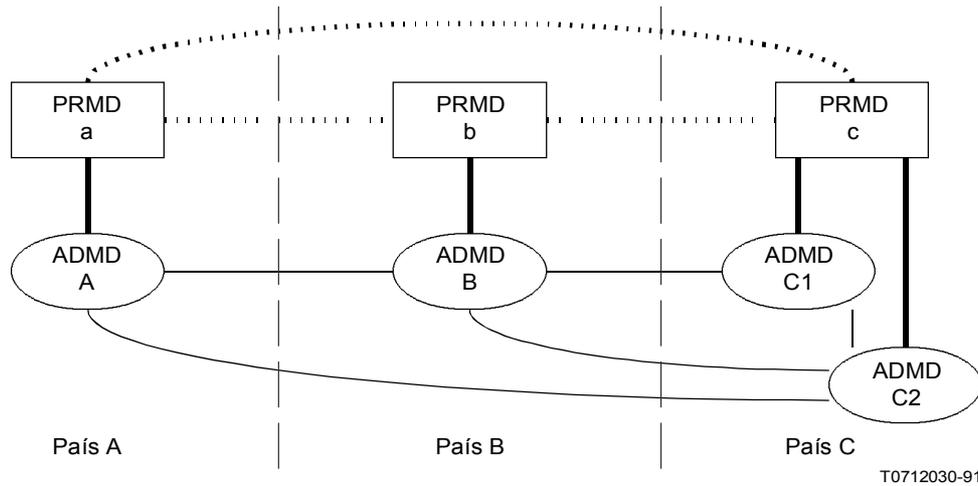


FIGURA G-1/X.402
PRMD independientes múltiples

La organización multinacional puede dividir su sistema de mensajería de forma lógica en porciones que estén contenidas íntegramente en un solo país. Cada porción funciona como un PRMD distinto y utiliza direcciones registradas en su propio país.

Cada PRMD puede conectar con uno o más ADMD de su propio país. En el caso en que el PRMD esté conectado a más de un ADMD, y que no se utilice el nombre de ADMD de espacio único, cada usuario (o DL) tendrá múltiples direcciones O/R (seudónimos) con diferentes valores para el atributo nombre-dominio-administración. Algunos de los valores de estos seudónimos pueden utilizarse como el valor de la dirección O/R del originador. Si el propio país permite la utilización del nombre ADMD de espacio único y el PRMD opta por utilizarlo, cada usuario (o DL) puede tener un valor único de dirección O/R, independientemente del número de ADMD a los que esté conectado el PRMD, suponiendo que todos los dominios de que se trata puedan aplicar esta convención.

Nota 1 – La elección de un seudónimo tiene una serie de consecuencias, que se examinan más adelante.

Nota 2 – Puede haber limitaciones en cuanto a la utilización del nombre ADMD de espacio único con carácter internacional y su aceptación por parte de ADMD de otros países.

Nota 3 – Los procedimientos MTS pueden tener que revisarse para admitir PRMD multinacionales en un entorno de mensajería global.

Este caso no es específico de las organizaciones multinacionales; no puede distinguirse de los múltiples PRMD empleados por organizaciones distintas.

Esta configuración permite reglamentaciones diferentes en diversos países y además prevé la asignación de direcciones O/R únicas. Para más información y una mayor comprensión, véase asimismo el anexo E de la Recomendación F.400 (1992) que comporta la misma semántica que el § G.2.1.

G.2.2 *Un PRMD único, nombrado a partir del país de origen*

Véase la figura G-2/X.402.

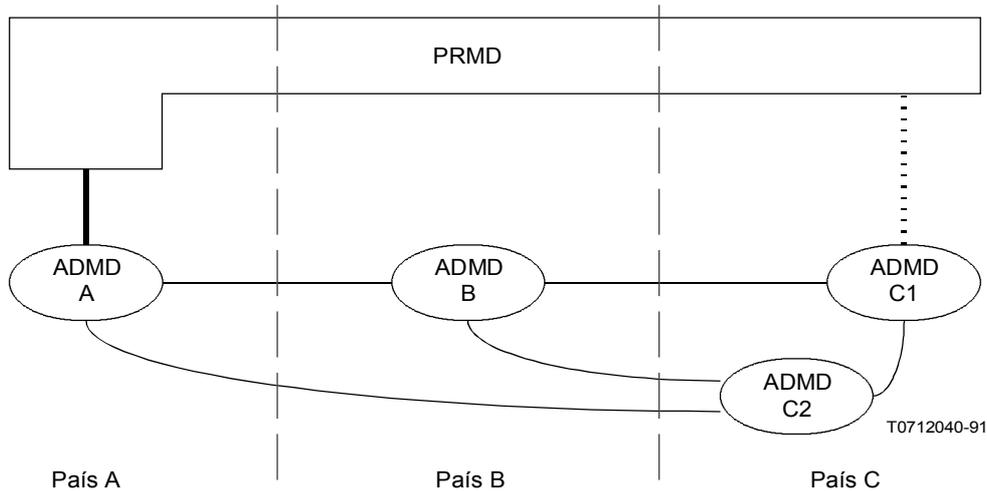


FIGURA G-2/X.402
PRMD único con nombre único

La organización multinacional puede utilizar un dominio de gestión único que esté situado físicamente en más de un país. Un solo país se selecciona como país de origen a los efectos del direccionamiento. En este caso, todos los UA dentro del MD están direccionados con los mismos valores para nombre-país, nombre-dominio-administración y nombre-dominio-privado. Esta serie de valores de atributos se registra con arreglo a las exigencias del país elegido.

El PRMD puede conectarse con uno o más ADMD del país de origen y además (con sujeción a la reglamentación nacional y los criterios comerciales) a los ADMD de otros países. La conexión a los ADMD situados fuera del país de origen exige que esos ADMD tengan la capacidad y voluntad de encaminar mensajes directamente a un PRMD cuando el nombre-país utilizado en la dirección O/R es diferente de la utilizada por el ADMD.

Esta configuración no presenta ningún problema técnico para los interlocutores fuera del PRMD ni para los proveedores del servicio que participan en la transferencia o la entrega de mensajes. Puede ser que los usuarios de este PRMD no estén satisfechos con la consiguiente utilización de un nombre-país en la dirección O/R a la que no pertenezcan.

G.2.3 *Un PRMD único con múltiples nombres de dominio y de país*

Véase la figura G-3/X.402.

La organización multinacional puede utilizar un sistema único de mensajería, pero utilizar nombres PRMD registrados en más de un país. Al formar las direcciones O/R, el nombre-dominio-administración debe corresponder a uno de los valores autorizados por el país indicado en el valor del nombre-país. El valor nombre-dominio-privado utilizado en una dirección O/R en particular debe ser uno registrado de forma compatible con el nombre de país y el nombre-dominio-administración siguiendo los procedimientos del país o el ADMD de que se trate.

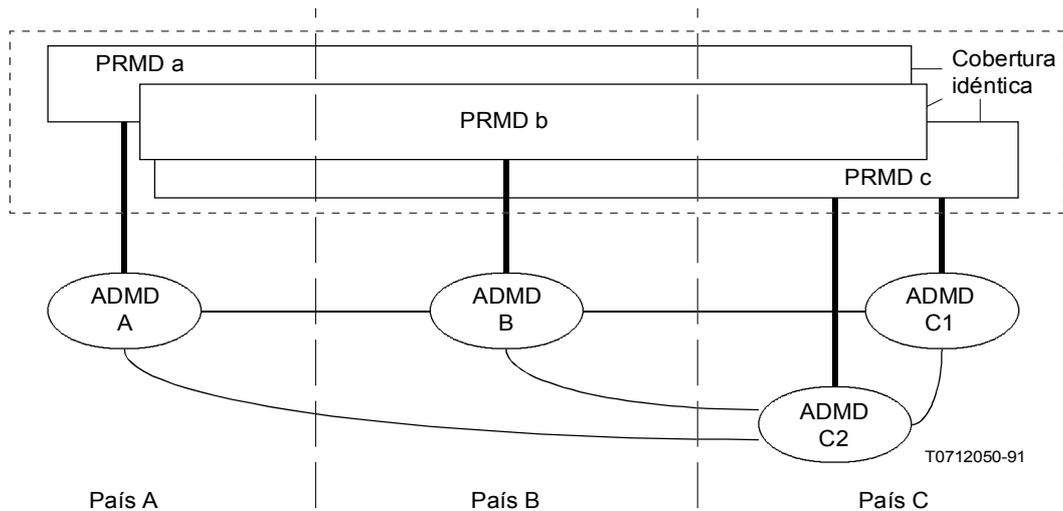


FIGURA G-3/X.402
PRMD único con múltiples nombres de dominio y de país

El PRMD multinacional puede conectarse a uno o más ADMD. Cada usuario (o DL) tiene actualmente múltiples seudónimos de direcciones O/R, con diferentes valores para el nombre-país, el nombre-dominio-administración y el nombre-dominio-privado. Cualquiera de estos seudónimos puede ser utilizado como el valor de la dirección O/R del originador; los usuarios pueden optar por utilizar una dirección que identifica el país en el que están situados físicamente, pero no están obligados a hacerlo, siempre que el ADMD de que se trata acepte la dirección O/R elegida del originador que se propone.

Si aparecen múltiples (seudónimos de) direcciones O/R para el mismo usuario, el interlocutor de este usuario puede no saber cómo resolver la situación. El emisor y el destinatario deben entender cuál de las diversas direcciones O/R es necesario utilizar en los diferentes casos. Si no lo entienden, ello obstaculizará una buena comunicación abierta. Además, los costos de un determinado mensaje pueden variar con arreglo al punto de acceso elegido para el primer ADMD.

Nota – La elección del seudónimo presenta diversas consecuencias que se examinan a continuación.

Los acuerdos bilaterales entre el PRMD y cada ADMD a los cuales se conecta identificarán el criterio utilizado por el ADMD para encaminar mensajes dentro del PRMD. Con arreglo a estos acuerdos, se puede optar por encaminar directamente mensajes dirigidos a cualquiera de los seudónimos que identifican el PRMD o encaminar directamente sólo los mensajes direccionados utilizando el código de país local, encaminando los demás por conducto de un ADMD del país, especificado en la dirección O/R del destinatario, en la medida en que los proveedores del servicio de que se trata puedan aplicar los principios de tasación y contabilidad.

Nota – Puede ser necesario revisar los procedimientos MTS para apoyar los PRMD multinacionales en un entorno de mensajería mundial.

G.3 *Seudónimos de direcciones O/R*

Los casos mencionados a continuación muestran que pueden aparecer seudónimos de los nombres de dominio de gestión. La presencia de dichos seudónimos tiene diversas consecuencias, tanto para los usuarios como para los explotadores del sistema.

Nota – Pueden también presentarse seudónimos de direcciones para los usuarios dentro de un dominio; el tratamiento de éstos suele ser independiente de los seudónimos del dominio de gestión.

Cada usuario puede seleccionar un ADMD preferido entre los disponibles y citar el nombre-país, nombre-dominio-administración y nombre-dominio-privado correspondientes cuando comunique su dirección O/R, ya sea en una tarjeta comercial o en la dirección O/R de mensajes del originador.

Si el usuario desea asimismo utilizar los servicios de otros ADMD a los que esté conectado el PRMD, pueden plantearse algunas dificultades. En algunos pocos casos el usuario (o agente del usuario) puede seleccionar otro seudónimo del nombre del PRMD correspondiente al ADMD que ha de utilizarse, y cambiar la dirección O/R del originador en consecuencia. Sin embargo, esto es sólo posible en el caso de que llegue a todos los destinatarios del mensaje por conducto del mismo ADMD, y que se conozca el ADMD elegido en el momento del depósito. No es posible cambiar la dirección O/R después del depósito, pues está en pugna con los servicios de seguridad. Además, puede ser confuso para los usuarios recibir mensajes del mismo originador pero con direcciones O/R diferentes.

Por estos motivos sería más satisfactorio que el usuario utilizara sólo una dirección O/R, y que algunos ADMD aceptaran los mensajes en los que la dirección O/R del originador no corresponda a ese nombre-país y el nombre-dominio-administración. Puede suceder que direcciones O/R del originador no correspondan al PRMD local si se utilizan los servicios listas de distribución y redireccionamientos (por ejemplo, el servicio destinatario-alternativo-asignado-destinatario). Los acuerdos bilaterales entre operadores de ADMD deberán tener en cuenta la utilización de estas posibilidades (entre otras) en el caso de tránsito por conducto de más de un dominio. Puede suceder que su alcance no sea mundial.

La dirección O/R del originador utilizada al enviar mensajes puede afectar el encaminamiento seguido por los mensajes que se envíen como respuesta. En el caso general, los mensajes de respuesta se encaminarán por conducto del país y el ADMD especificados en la dirección O/R. Los acuerdos bilaterales entre los PRMD o entre el PRMD y los ADMD pueden permitir la utilización de otros caminos. Estos factores ejercerán influencia en el usuario al seleccionar el nombre de dominio adecuado que utilizará en la dirección O/R. Debe tenerse presente que la utilización de múltiples direcciones O/R para el mismo usuario puede también tener consecuencias sobre los potenciales destinatarios. Esta situación confusa no favorecería una buena comunicación abierta.

ANEXO H

(a la Recomendación X.402)

Diferencias entre la Recomendación del CCITT y la norma ISO

(Este anexo no es parte integrante de esta Recomendación)

En él se da una relación de todas las diferencias, excepto las puramente estilísticas, entre esta Recomendación del CCITT 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 no requiere que los ADMD y los PRMD estén relacionados jerárquicamente para direccionamiento y encaminamiento; mientras que esta Recomendación sí lo requiere (véanse las subcláusulas 14.1.1, 14.1.2 y las 15 y 19).
- b) En la subcláusula 18.3.1, el párrafo que define al nombre-dominio-administración de espacio único es una parte normativa de la Norma ISO/CEI, mientras que en la Recomendación del CCITT es una Nota. El párrafo que define al nombre-dominio-administración de caso único es una parte normativa de la Norma ISO/CEI, mientras que está omitido en la Recomendación del CCITT.
- c) La representación de direcciones O/R para utilización por personas es un anexo a la Norma ISO internacional correspondiente a la presente Recomendación, pero en ésta el material es referenciado, en el anexo F, remitiéndose al anexo B informativo de la Recomendación F.401.

ANEXO I

(a la Recomendación X.402)

(Este anexo no es parte integrante de esta Recomendación)

Índice

Este anexo constituye el índice de esta Recomendación. Proporciona los número(s) de la(s) página(s) 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 ASN.1;
- e) macros ASN.1;
- f) tipos ASN.1;
- g) valores ASN.1;
- h) acuerdos bilaterales.

I.1 *Abreviaturas*

	<i>Página</i>		<i>Página</i>
A/SYS	36	MRSE	59
AC	8	MS	13
ACSE	8,60	MSSE	58
ADMD	39	MTA	14
AE	8	MTS	12
APDU	8	MTSE	58
AS/SYS	37	O	10
ASE	8	OSI	8
ASN.1	8	P1	60
AST/SYS	37	P3	60
AT/SYS	37	P7	60
AU	13	PDAU	14
C	10	PDS	14
COMPUSEC	24	PRMD	39
D	10	RO	9
DL	12	ROSE	9
DSA	9	RT	8
EIT	16	RTSE	8
M	10	S/SYS	37
MASE	59	ST/SYS	37
MD	39	T/SYS	37
MDSE	59	UA	12
MHE	11	UE	8
MHS	11		

I.2 *Términos*

access, storage, and transfer system	37	administration-domain-name	44
access and storage system	37	administration management domain	39
access and transfer system	37	affirmation	23
access system	36	application association; association	8
access unit	13	application context (AC)	8
actual recipient	19	argument	8

	<i>Página</i>		<i>Página</i>
Association Control Service Element (ACSE)	8	local-postal-attributes	46
asymmetric	57	macro	8
asynchronous	8	management domain	39
attribute	9,43	mandatory	10
attribute type	43	member recipient	19
attribute value	43	members	12
attribute list	43	message	15
bind	8	Message Handling	10
certificate	9	Message Handling Environment	11
certification authority	9	Message Handling System	11
certification path	9	Message Storage	10
common-name	46	message store	13
conditional	10	Message Transfer	10
consuming ASE	57	message transfer agent	14
consuming UE	57	Message Transfer System	12
content	15	messaging system	35
content type	15	mnemonic O/R address	52
conversion	23	module	8
country-name	46	name	9
defaultable	10	name resolution	22
delivery	21	nested	12
delivery agent	21	network-address	46
delivery report	16	non-affirmation	23
described message	16	non-delivery	23
direct submission	20	non-delivery report	17
direct user	12	numeric-user-identifier	47
Directory	9	numeric O/R address	52
directory entry; entry	9	O/R address	50
directory system agent (DSA)	9	O/R name	42
distribution list	12	object	9
DL expansion	22	object class	9
domain	39	optional	10
domain-defined attribute	43	organization-name	47
encoded information type	16	organizational-unit-names	47
envelope	15	origination	20
event	17	originator	18
expansion point	22	originator-specified alternate recipient	18
explicit	8	parameter	8
explicit conversion	23	pds-name	47
export	8,21	personal-name	47
extension-physical-delivery-address-components	46	physical-delivery-country-name	48
extension-postal-O/R-address-components	46	physical-delivery-office-name	48
external routing	24	physical-delivery-office-number	48
external transfer	20	physical-delivery-organization-name	48
formatted	52	physical-delivery-personal-name	48
Global MHS	40	Physical delivery	14
grade	10	physical delivery access unit	14
hash function	9	physical delivery system	14
immediate recipient	17	physical message	14
implicit	8	physical rendition	14
implicit conversion	23	post-office-box-address	48
import	8,20	postal-code	48
indirect submission	20	postal O/R address	52
indirect user	12	poste-restante-address	49
initiator; and	8	potential recipient	19
intended recipient	18	private-domain-name	49
internal routing	24	private management domain	39
internal transfer	20	probe	16
joining	22	receipt	21

	<i>Página</i>		<i>Página</i>
recipient	19	submission agent	20
recipient-assigned alternate recipient	19	submit permission	12
redirection	23	supplying ASE	57
remote error	9	supplying UE	57
remote operation	9	symmetric	56
Remote Operations (RO)	9	synchronous; and	9
Remote Operations Service Element (ROSE)	9	tag	8
report	16	terminal O/R address	53
responder	8	terminal-identifier	49
result	9	terminal-type	49
retrieval	21	transfer	20
ROSE	60	transfer system	37
routing	23	transmittal	17
RTSE	60	transmittal event	17
simple authentication; and	9	transmittal step	17
splitting	22	type	43
standard attribute	43	type; and	8
step	17	unbind	9
storage and transfer system	37	unformatted	52
storage system	37	unformatted-postal-address	49
street-address	49	unique-postal-name	49
strong authentication	9	user	12
subject message	16	user agent	12
subject probe	16	value	8,43
submission	20		
I.3	<i>Elementos de información</i>		
MHS Deliverable Content Length	62	MHS O/R Address	65
MHS Deliverable Content Types	63	MHS O/R Addresses	63
MHS Deliverable EITs	63	MHS O/R Name	65
MHS DL Members	63	MHS Supported Automatic Actions	64
MHS DL Submit Permission	64	MHS Supported Content Types	64
MHS DL Submit Permissions	63	MHS Supported Optional Attributes	64
MHS Message Store	61	MHS User	62
MHS Message Store Directory Name	63	MHS Distribution List	61
MHS Message Transfer Agent	62	MHS User Agent	62
I.4	<i>Módulos ASN.1</i>		
MHSDirectoryObjectsAndAttributes	67	MHSObjectIdentifiers	65
I.5	<i>Macros ASN.1</i>		
ATTRIBUTE	67	OBJECT-CLASS	67
ATTRIBUTE-SYNTAX	67		
I.6	<i>Tipos ASN.1</i>		
DLSubmitPermission	64,70	ORName	67
ID	65	ORNamePattern	64,70
ORAddress	65,67	RequestedDeliveryMethod	67
I.7	<i>Valores ASN.1</i>		
applicationEntity	67	id-arch	66
commonName	67	id-as	66
description	67	id-as-mhs-dl-submit-permission	66
distinguishedNameSyntax	67	id-as-mhs-or-address	66

	<i>Página</i>		<i>Página</i>
id-as-mhs-or-name	66	id-oc-mhs-user-agent	66
id-asdc	66	IntegerSyntax	67
id-at	66	mhs-deliverable-content-length	62,68
id-at-mhs-deliverable-content-length	66	mhs-deliverable-content-types	63,69
id-at-mhs-deliverable-content-types	66	mhs-deliverable-eits	63,69
id-at-mhs-deliverable-eits	66	mhs-distribution-list	61,67
id-at-mhs-dl-members	66	mhs-dl-members	63,69
id-at-mhs-dl-submit-permissions	66	mhs-dl-submit-permission-syntax	64,69
id-at-mhs-message-store-dn	66	mhs-dl-submit-permissions	63,69
id-at-mhs-or-addresses	66	mhs-message-store	61,68
id-at-mhs-supported-automatic-actions	66	mhs-message-store-dn	63,69
id-at-mhs-supported-content-types	66	mhs-message-transfer-agent	62,68
id-at-mhs-supported-optional-attributes	66	mhs-or-address-syntax	65,70
id-directory-objects-and-attributes	66	mhs-or-addresses	63,69
id-group	66	mhs-or-name-syntax	65,70
id-ipms	65	mhs-supported-automatic-actions	64,69
id-mhs-protocols	65	mhs-supported-content-types	64,69
id-mod	66	mhs-supported-optional-attributes	64,69
id-ms	66	mhs-user	62,68
id-mts	66	mhs-user-agent	62,68
id-object-identifiers	66	objectIdentifiersSyntax	67
id-oc	66	organization	67
id-oc-mhs-distribution-list	66	organizationalUnitName	67
id-oc-mhs-message-store	66	owner	67
id-oc-mhs-message-transfer-agent	66	seeAlso	67
id-oc-mhs-user	66	top	67
I.8	<i>Acuerdos bilaterales</i>		
routing	54		

ANEXO J

(a la Recomendación X.402)

Lista por orden alfabético de las abreviaturas contenidas en esta Recomendación

A/SYS	Sistema de acceso (<i>access system</i>)
AC	Contexto de aplicación (<i>application context</i>)
ACSE	Elemento de servicio de control de asociación (<i>association control service element</i>)
ADMD	Dominio de gestión de Administración (<i>administration management domain</i>)
AE	Entidad de aplicación (<i>application-entity</i>)
APDU	Unidad de datos de protocolo de aplicación (<i>application protocol data unit</i>)
AS/SYS	Sistema de acceso y almacenamiento (<i>access and storage system</i>)
ASE	Elemento de servicio de aplicación (<i>application service element</i>)
ASN.1	Notación de sintaxis abstracta uno (<i>abstract syntax notation one</i>)
AST/SYS	Sistema de acceso, almacenamiento y transferencia (<i>access, storage and transfer system</i>)
AT/SYS	Sistema de acceso y transferencia (<i>access and transfer system</i>)
AU	Unidad de acceso (<i>access unit</i>)

C	Condicional (<i>conditional</i>)
COMPUSEC	Seguridad de los computadores (<i>computer security</i>)
D	Defectible (<i>defaultable</i>)
DL	Lista de distribución (<i>distribution list</i>)
DSA	Agente de sistema de directorio (<i>directory system agent</i>)
EIT	Tipo de información codificada (<i>encoded information type</i>)
IA5	Alfabeto internacional n° 5 (<i>international alphabet No. 5</i>)
M	Obligatorio (<i>mandatory</i>)
MASE	Elemento de servicio de administración de mensajes (<i>message administration service element</i>)
MD	Dominio de gestión (<i>management domain</i>)
MDSE	Elemento de servicio entrega de mensajes (<i>message delivery service element</i>)
MHE	Entorno de tratamiento de mensajes (<i>message handling environment</i>)
MHS	Sistema de tratamiento de mensajes (<i>message handling system</i>)
MRSE	Elemento de servicio recuperación de mensajes (<i>message retrieval service element</i>)
MS	Memoria de mensajes (<i>message store</i>)
MSSE	Elemento de servicio depósito de mensajes (<i>message submission service element</i>)
MTA	Agente de transferencia de mensajes (<i>message transfer agent</i>)
MTS	Sistema de transferencia de mensajes (<i>message transfer system</i>)
MTSE	Elemento de servicio de transferencia de mensajes (<i>message transfer service element</i>)
O	Optativo (<i>optional</i>)
O/R	Originador/recibiente (<i>originator/recipient</i>)
OSI	Interconexión de sistemas abiertos (<i>open systems interconnection</i>)
P1	Protocolo 1 (<i>protocol 1</i>)
P3	Protocolo 3 (<i>protocol 3</i>)
P7	Protocolo 7 (<i>protocol 7</i>)
PDAU	Unidad de acceso de entrega física (<i>physical delivery access unit</i>)
PDS	Sistema de entrega física (<i>physical delivery system</i>)
PRMD	Dominio de gestión privado (<i>private management domain</i>)
RO	Operaciones a distancia (<i>remote operation</i>)
ROSE	Elemento de servicio de operaciones a distancia (<i>remote operation service element</i>)
RT	Transferencia fiable (<i>reliable transfer</i>)
RTSE	Elemento de servicio de transferencia fiable (<i>reliable transfer service element</i>)
S/SYS	Sistema de almacenamiento (<i>storage system</i>)
ST/SYS	Sistema de almacenamiento y transferencia (<i>storage and transfer system</i>)
T/SYS	Sistema de transferencia (<i>transfer system</i>)
UA	Agente de usuario (<i>user agent</i>)
UE	Elemento de usuario (<i>user element</i>)

