



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

X.402

(11/1988)

SERIE X: REDES DE COMUNICACIÓN DE DATOS:
SISTEMAS DE TRATAMIENTO DE MENSAJES

**SISTEMAS DE TRATAMIENTO DE MENSAJES:
ARQUITECTURA GLOBAL**

Reedición de la Recomendación X.402 del CCITT
publicada en el Libro Azul, Fascículo VIII.7 (1988)

NOTAS

1 La Recomendación X.402 del CCITT se publicó en el fascículo VIII.7 del Libro Azul. Este fichero es un extracto del Libro Azul. Aunque la presentación y disposición del texto son ligeramente diferentes de la versión del Libro Azul, el contenido del fichero es idéntico a la citada versión y los derechos de autor siguen siendo los mismos (véase a continuación).

2 Por razones de concisión, el término «Administración» se utiliza en la presente Recomendación para designar a una administración de telecomunicaciones y a una empresa de explotación reconocida.

Recomendación X.402

SISTEMAS DE TRATAMIENTO DE MENSAJES: ARQUITECTURA GLOBAL¹⁾

(Melbourne, 1988)

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

El CCITT,

considerando

- (a) la necesidad de los sistemas de tratamiento de mensajes;
- (b) la necesidad de almacenar y transferir mensajes de diferentes tipos;
- (c) que la Recomendación X.200 define el modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT;
- (d) que las Recomendaciones X.208, X.217, X.218 y X.219 sirven de base para las aplicaciones del CCITT;
- (e) que las Recomendaciones de la serie X.500 definen los sistemas de guía;
- (f) que los sistemas de tratamiento de mensajes se definen en la serie de Recomendaciones: X.400, X.402, X.403, X.407, X.408, X.411, X.413 y X.419;
- (g) que la mensajería interpersonal se define en las Recomendaciones X.420 y T.330,

recomienda por unanimidad

- (1) que los modelos abstractos de un sistema de tratamiento de mensajes se definen en la sección 2;
- (2) que las configuraciones de un sistema de tratamiento de mensajes se definen en la sección 3;
- (3) que la denominación, el direccionamiento y el encaminamiento en los sistemas de tratamiento de mensajes se definen en la sección 4;
- (4) que el uso de la guía por los sistemas de tratamiento de mensajes se define en la sección 5;
- (5) que la realización ISA de un sistema de tratamiento de mensajes se especifica en la sección 6.

ÍNDICE

SECCIÓN 1 – Introducción

0	<i>Introducción</i>
1	<i>Objeto</i>
2	<i>Referencias</i>
2.1	Interconexión de sistemas abiertos
2.2	Sistemas de guía
2.3	Sistemas de tratamiento de mensajes

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

- 3 *Definiciones*
 - 3.1 Interconexión de sistemas abiertos
 - 3.2 Sistemas de guía
 - 3.3 Sistemas de tratamiento de mensajes
- 4 *Abreviaturas*
- 5 *Convenios*
 - 5.1 NSA.1
 - 5.2 Grado
 - 5.3 Términos

SECCIÓN 2 – *Modelos abstractos*

- 6 *Visión de conjunto*
- 7 *Modelo funcional*
 - 7.1 Objetos funcionales primarios
 - 7.2 Objetos funcionales secundarios
 - 7.3 Objetos funcionales terciarios
 - 7.4 Tipos de UA seleccionados
- 8 *Modelo de información*
 - 8.1 Mensajes
 - 8.2 Sondas
 - 8.3 Informes
- 9 *Modelo operacional*
 - 9.1 Transmisión
 - 9.2 Funciones de la transmisión
 - 9.3 Pasos de la transmisión
 - 9.4 Eventos de la transmisión
- 10 *Modelos de seguridad*
 - 10.1 Políticas de seguridad
 - 10.2 Servicios de seguridad
 - 10.3 Elementos de seguridad

SECCIÓN 3 – *Configuraciones*

- 11 *Visión de conjunto*
- 12 *Configuraciones funcionales*
 - 12.1 Respecto a la guía
 - 12.2 Respecto a la memoria de mensajes
- 13 *Configuraciones físicas*
 - 13.1 Sistemas de mensajería
 - 13.2 Configuraciones representativas
- 14 *Configuraciones organizativas*
 - 14.1 Dominios de gestión
 - 14.2 Configuraciones representativas
- 15 *El STM global*

SECCIÓN 4 – *Denominación, direccionamiento y encaminamiento*

- 16 *Visión de conjunto*
- 17 *Denominación*
 - 17.1 Nombres de guía
 - 17.2 Nombres de O/D
- 18 *Direccionamiento*
 - 18.1 Listas de atributos
 - 18.2 Juegos de caracteres
 - 18.3 Atributos normalizados
 - 18.4 Equivalencia de listas de atributos
 - 18.5 Formas de direcciones O/D
 - 18.6 Atributos condicionales
- 19 *Encaminamiento*

SECCIÓN 5 – *Uso de la guía*

- 20 *Visión de conjunto*
- 21 *Autenticación*
- 22 *Resolución de nombre*
- 23 *Ampliación de LD*
- 24 *Evaluación de capacidades*

SECCIÓN 6 – *Realización por ISA*

- 25 *Visión de conjunto*
- 26 *Elementos de servicio de aplicación*
 - 26.1 El concepto de ESA
 - 26.2 ESA simétricos y asimétricos
 - 26.3 ESA de tratamiento de mensajes
 - 26.4 ESA de apoyo
- 27 *Contextos de aplicación*

Anexo A – Clases de objetos de guía y atributos

Anexo B – Definición de referencia de identificadores de objetos

Anexo C – Definición de referencia de clases de objetos de guía y atributos

Anexo D – Amenazas contra la seguridad

Anexo E – Provisión de servicios de seguridad en la Recomendación X.411

Anexo F – Diferencias entre la Recomendación del CCITT y la Norma ISO

Anexo G – Índice

0 Introducción

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

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

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

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

1 Objeto

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

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

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

CUADRO 1/X.402

Especificaciones para sistemas de tratamiento de mensajes

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

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

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

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

CUADRO 2/X.402

Especificaciones para las guías

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

CUADRO 3/X.402

Especificaciones para los fundamentos del STM

CCITT	ISO	Tema tratado
Modelo		
X.200	7498	Modelo de referencia de ISA
NSA.1		
X.208	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 STM para satisfacer una diversidad de exigencias de tipo funcional, físico u organizativo. En la sección 4 se describe la denominación y el direccionamiento de usuarios y listas de distribución y el encaminamiento hacia ellos de los objetos de información. En la sección 5 se indican los usos que el STM puede hacer de la guía. En la sección 6 se describe cómo se realiza el STM utilizando la ISA. Los anexos contienen importante información suplementaria.

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

2 Referencias

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

2.1 *Interconexión de sistemas abiertos*

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

- X.200 Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 7498)
- X.208 Especificación de la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8824)
- X.209 Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (NSA.1) (véase también la Norma ISO 8825)
- X.217 Definición del servicio de control de asociación para la interconexión de sistemas abiertos para aplicaciones del CCITT (véase también la Norma ISO 8649)
- X.218 Transferencia fiable: modelo y definición de servicios (véase también la Norma ISO 9066-1)
- X.219 Operaciones a distancia: modelo, notación y definición del servicio (véase también la Norma ISO 9072-1)
- X.227 Especificación del protocolo de control de asociación para la interconexión de sistemas abiertos para aplicación del CCITT (véase también la Norma ISO 8650)
- X.228 Transferencia fiable: especificación del protocolo (véase también la Norma ISO 9066-2)
- X.229 Operaciones a distancia: especificación del protocolo (véase también la Norma ISO 9072-2)

2.2 *Sistemas de guía*

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

- X.500 La guía – Visión de conjunto de conceptos, modelos y servicios (véase también la Norma ISO 9594-1)
- X.501 La guía – Modelos (véase también la Norma ISO 9594-2)
- X.509 La guía – Marco de autenticación (véase también la Norma ISO 9594-8)
- X.511 La guía – Definición del servicio abstracto (véase también la Norma ISO 9594-3)
- X.518 La guía – Procedimientos para operación distribuida (véase también la Norma ISO 9594-4)
- X.519 La guía – Especificaciones de protocolos (véase la Norma ISO 9594-5)
- X.520 La guía – Tipos de atributos seleccionados (véase también la Norma ISO 9594-6)
- X.521 La guía – Clases de objetos seleccionadas (véase también la Norma ISO 9594-7)

2.3 *Sistemas de tratamiento de mensajes*

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

- T.330 Acceso telemático al servicio de mensajería interpersonal
- X.400 Sistema de tratamiento de mensajes: Visión de conjunto del sistema y del servicio (véase también la Norma ISO 10021-1)
- X.403 Sistemas de tratamiento de mensajes: Pruebas de conformidad
- X.407 Sistemas de tratamiento de mensajes: Convenios para la definición del servicio abstracto (véase también la Norma ISO 10021-3)
- X.408 Sistemas de tratamiento de mensajes: Reglas de conversión de tipos de información codificada
- X.411 Sistemas de tratamiento de mensajes: Definición del servicio abstracto y procedimientos (véase también la Norma ISO 10021-4)
- X.413 Sistemas de tratamiento de mensajes: Definición del servicio abstracto de almacenamiento de mensajes (véase también la Norma ISO 10021-5)
- X.419 Sistemas de tratamiento de mensajes: Especificaciones de protocolo (véase también la Norma ISO 10021-6)

3 **Definiciones**

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

3.1 *Interconexión de sistemas abiertos*

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

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

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

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

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

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

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

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

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

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

3.2 *Sistemas de guía*

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

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

3.3 *Sistemas de tratamiento de mensajes*

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

4 **Abreviaturas**

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

5 **Convenios**

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

5.1 NSA.1

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

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

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

5.2 Grado

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

- a) **obligatorio (O)**: un componente obligatorio estará presente en cada caso de la clase;
- b) **facultativo (F)**: un componente facultativo estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que suministra ese caso. No hay valor por defecto;
- c) **defectible (D)**: un componente defectible estará presente en un caso de la clase, a discreción del objeto (por ejemplo, usuario) que ofrece ese caso. En su ausencia se aplica un valor por defecto especificado por esta Recomendación;
- d) **condicional (C)**: un componente condicional estará presente en un caso de la clase, tal como exige esta Recomendación.

5.3 Términos

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

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

SECCIÓN 2 – MODELOS ABSTRACTOS

6 Visión de conjunto

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

El **tratamiento de mensajes** es una tarea distribuida del tratamiento de la información, que comprende las siguientes 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 Recomendación X.420.

7 Modelo funcional

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

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

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

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

Como asunto local, los objetos funcionales pueden tener capacidades superiores a las especificadas en esta Recomendación o en otras de la misma serie. En concreto, un *agente de usuario* típico tiene capacidades de preparación, reproducción y almacenamiento de mensajes que no están normalizadas.

7.1 Objetos funcionales primarios

El ETM comprende el *sistema de tratamiento de mensajes*, los *usuarios* y las *listas de distribución*. Entre estos objetos funcionales primarios se produce una interacción. A continuación se definen y describen los tipos de objetos.

En la figura 1/X.402 se representa de manera esquemática esa interacción.

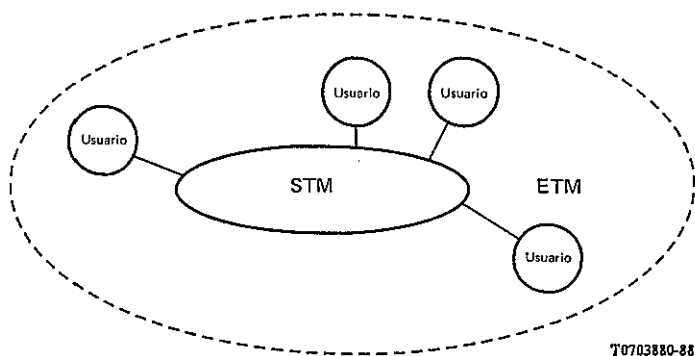


FIGURA 1/X.402
Entorno del tratamiento de mensajes

7.1.1 Sistema de tratamiento de mensajes

La finalidad principal del tratamiento de mensajes es transportar objetos de información de un usuario a otro. Al objeto funcional que lleva a cabo esta tarea se le denomina **sistema de tratamiento de mensajes (STM)**.

El ETM consta de un solo STM.

7.1.2 Usuarios

La finalidad principal del STM es transportar objetos de información entre *usuarios*. Al objeto funcional (por ejemplo, una persona) que más que proporcionar tratamiento de mensajes, participa en ese tratamiento, se le denomina **usuario**.

Cabe distinguir las siguientes clases de usuarios:

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

El ETM consta de un número cualquiera de usuarios.

7.1.3 Lista de distribución

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

Una LD representa cero o más usuarios y LD, a los que se les denomina sus **miembros**. De las LD (si es que hay alguna) se dice que están jerarquizadas. Pedir al STM que transporte un objeto de información (por ejemplo, un *mensaje*) a una LD equivale a pedirle que lo transporte a sus miembros. Téngase en cuenta que se trata de un proceso recurrente.

El derecho a transportar *mensajes* a una LD determinada, o el permiso para hacerlo, puede estar bajo control. A ese derecho, se le denomina **permiso de depósito**. Como asunto local, es posible restringir más aún el uso de una LD.

El ETM consta de un número cualquiera de LD.

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

7.2 Objetos funcionales secundarios

El STM comprende el *sistema de transferencia de mensajes*, los *agentes de usuarios*, las *memorias de mensajes* y las *unidades de acceso*. Entre estos objetos funcionales secundarios se produce una interacción. Más adelante se definen y describen los tipos de objetos.

En la figura 2/X.402 se representa de forma esquemática esa interacción.

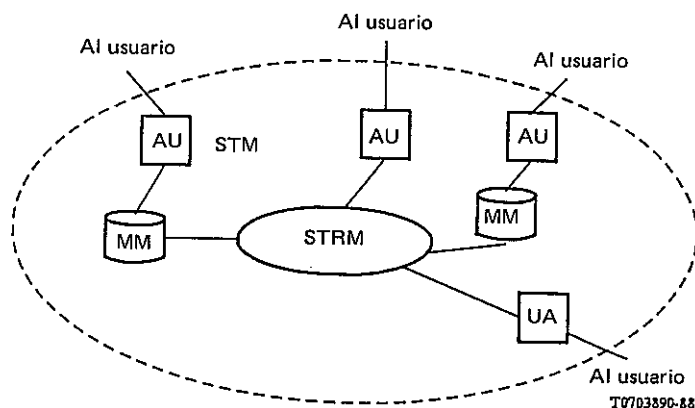


FIGURA 2/X.402

Sistema de tratamiento de mensajes

7.2.1 Sistema de transferencia de mensajes

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

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

El STM consta de un solo STRM.

7.2.2 Agentes de usuario

El objeto funcional por medio del cual un usuario directo aislado participa en el tratamiento de mensajes se denomina **agente de usuario (AU)**.

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

El STM consta de un número cualquiera de AU.

Nota – En el caso de un AU que preste servicio a un usuario humano, lo típico es que la interacción entre agente y usuario se establezca a través de un dispositivo de entrada/salida (por ejemplo, un teclado, una pantalla, un dispositivo de barrido, una impresora o una combinación de algunos de estos dispositivos).

7.2.3 Memorias de mensajes

El usuario típico debe almacenar la información que recibe. El objeto funcional que proporciona a un usuario directo (aislado) la capacidad de almacenar mensajes se llama **memoria de mensajes (MM)**. Cada MM está asociada a un AU, pero no todos los AU tienen MM asociada.

Las MM son de uso general y facilitan todas las aplicaciones de tratamiento de mensajes. Además, una MM puede adaptarse a una o más aplicaciones particulares, de tal modo que pueda, con mayor facilidad, *presentar* mensajes y permitir la *recuperación de mensajes* asociados a esa aplicación.

El STM consta de un número cualquiera de MM.

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

7.2.4 Unidades de acceso

El objeto funcional que enlaza al STRM con otro sistema de comunicaciones (por ejemplo, un sistema postal o la red télex) y, a través del cual, sus patronos participan en el tratamiento de mensajes como usuarios indirectos, se denomina **unidad de acceso (UA)**.

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

El STM consta de un número cualquiera de UA.

7.3 Objetos funcionales terciarios

El STRM está formado por *agentes de transferencia de mensajes*. Entre estos objetos funcionales terciarios se produce una interacción. Más adelante se definen y describen los tipos de objetos terciarios.

En la figura 3/X.402 se representa de manera esquemática esa interacción.

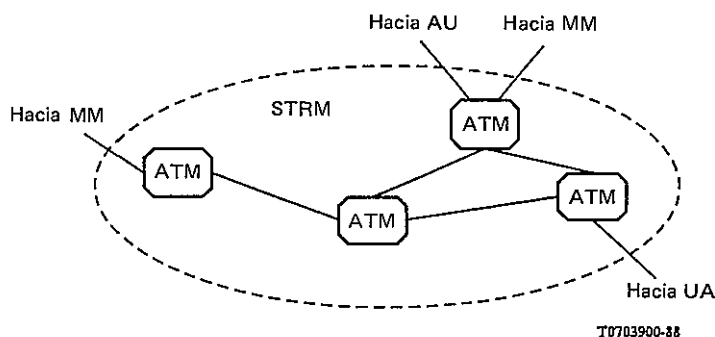


FIGURA 3/X.402

Sistema de transferencia de mensajes

7.3.1 Agentes de transferencia de mensajes

El STRM transporta objetos de información a usuarios y LD según el modo de almacenamiento y retransmisión. Al objeto funcional que proporciona el eslabón de la cadena de almacenamiento y retransmisión del STRM se le denomina **agente de transferencia de mensajes (ATM)**.

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

El STR consta de un número cualquiera de ATM.

7.4 Tipos de UA seleccionados

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

7.4.1 Entrega física

Una **unidad de acceso de entrega física (UAEF)** es una UA que somete los *mensajes* (pero no las *sondas* ni los *informes*) a *reproducción física*, y transporta los *mensajes físicos* resultantes a un *sistema de entrega física*.

A la transformación de un *mensaje* en un *mensaje físico* se le denomina **reproducción física**. Un **mensaje físico** es un objeto físico (por ejemplo, una carta y su sobre de papel) que contiene un *mensaje*.

Un **sistema de entrega física (SEF)** es un sistema que efectúa la *entrega física*. El sistema postal es un tipo importante de SEF. Se llama **entrega física** a la transferencia de un mensaje físico a un patrón de un SEF, uno de los usuarios indirectos a los que la UAEF proporciona capacidades de tratamiento de mensajes.

La mensajería interpersonal es una de las aplicaciones del tratamiento de mensajes proporcionadas por todas las UAEF (véase la Recomendación X.420).

7.4.2 Telemática

En la Recomendación X.420 se presentan las unidades de acceso telemático, que proporcionan, en exclusiva, la mensajería interpersonal.

7.4.3 Télex

En la Recomendación X.420 se presentan las unidades de acceso télex, que proporcionan, en exclusiva, la mensajería interpersonal.

8 Modelo de información

En este punto se presenta un modelo de información del tratamiento de mensajes. La realización concreta del modelo es objeto de otras Recomendaciones de la serie.

El STM y el STRM pueden transportar objetos de información de tres clases: *mensajes*, *sondas* e *informes*. En la primera columna del cuadro 4/X.402 figuran esas tres clases. Para cada una de ellas se indican, en la segunda columna, los tipos de objetos funcionales - usuario, AU, MM, ATM y UA - que son origen y destino final de tales objetos.

CUADRO 4/X.402

Objetos de información transportables

Objeto de información	Objeto funcional				
	Usuario	AU	MM	ATM	UA
Mensaje	OD	—	—	—	—
Sonda	O	—	—	D	—
Informe	D	—	—	O	—

O Último origen

D Último destino

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

8.1 *Mensajes*

La finalidad principal de la transferencia de mensajes es el transporte de objetos de información llamados **mensajes** de un usuario a otros. Un mensaje, como se muestra en la figura 4/X.402, consta de las siguientes partes:

- sobre:** Objeto de información cuya composición varía de un *paso de transmisión* a otro, y que identifica de manera diversa al *originador* del mensaje y a los *destinatarios potenciales*, informa sobre el transporte previo y dirige el siguiente por el STRM, y caracteriza el *contenido* del mensaje.
- contenido:** Objeto de información que el STRM ni examina ni modifica, si no es a efectos de *conversión*, mientras transporta el mensaje.

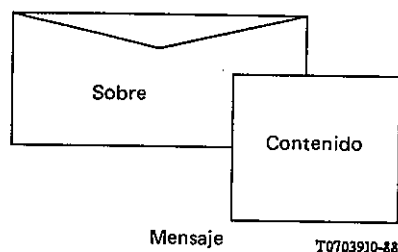


FIGURA 4/X.402

Sobre y contenido de un mensaje

Una parte de información, que figura en el sobre, identifica el tipo de contenido. El **tipo de contenido** es un identificador (un identificador de objeto o entero NSA.1) que indica la sintaxis y la semántica del contenido en su conjunto. Ese identificador permite al STRM determinar si el mensaje ha de *entregarse* o no a usuarios particulares, y permite a los AU y MM interpretar y tratar el contenido.

Otra parte de información, que figura asimismo en el sobre, identifica los tipos de información codificada representada en el contenido. Un **tipo de información codificada (TIC)** es un identificador (un identificador de objeto o entero NSA.1) que indica el soporte y el formato (por ejemplo, texto AI N.º 5 o facsímil del grupo 3) de partes individuales del contenido. Permite además al STRM determinar si el mensaje se ha de entregar o no a usuarios particulares, e identificar las oportunidades de *hacer* el mensaje entregable, convirtiendo una porción del contenido de un TIC a otro.

8.2 Sondas

Un segundo objetivo de la transferencia de mensajes es transportar objetos de información llamados **sondas** desde un usuario a otros (es decir, llevarlos hasta los ATM que prestan servicio a esos usuarios). Una sonda describe una clase de mensajes y se utiliza para determinar si deben *entregarse* o no dichos mensajes.

A un mensaje descrito por una sonda se le llama **mensaje descrito**.

La sonda consta de un solo sobre. El sobre contiene, en gran parte, la misma información que para un mensaje. Además del tipo de contenido y los tipos de información codificada del mensaje descrito, en el sobre figura la longitud de su contenido.

El *depósito* de una sonda da lugar a un comportamiento del STRM que es, en buena medida, el mismo que suscitaría el *depósito* de cualquier mensaje descrito, salvo que en el caso de la sonda, se prescinde de la *ampliación y de la entrega de la LD*. En concreto, y aparte de las consecuencias de la supresión de la *ampliación de la LD*, la sonda da lugar a los mismos *informes* a que daría lugar cualquier mensaje descrito. En esto reside la utilidad de las sondas.

8.3 Informes

Un tercer objetivo de la transferencia de mensajes es transportar a los usuarios unos objetos de información, llamados **informes**. Un informe, generado por el STRM, comunica el resultado o la marcha de la *transmisión* de un mensaje o de una sonda a uno o más destinatarios potenciales.

Al mensaje o a la sonda que sean objeto de un informe se les llama **mensaje objeto** o **sonda objeto**, respectivamente.

Un informe referido a un determinado *destinatario potencial* se lleva hasta el *originador* del mensaje o de la sonda objeto, a menos que el *destinatario potencial* sea un *destinatario miembro*. En este último caso, el informe es transportado a la LD a la que pertenezca el *destinatario miembro*. Como asunto local, (es decir, cuando exista una política establecida para esa LD particular), el transporte del informe puede proseguir hasta el propietario de la LD, a otro que contenga LD (en caso de jerarquización) o al originador del mensaje objeto (en su caso), o a ambos.

Los resultados a los que puede referirse un informe único son de las siguientes clases:

- a) **informe de entrega:** *Entrega, exportación o afirmación* del mensaje objeto o de la sonda objeto, o bien *ampliación de la LD*.
- b) **informe de no entrega:** *No entrega o no afirmación* del mensaje objeto o de la sonda objeto.

Un informe puede comprender uno o más informes de entrega y/o no entrega.

Un mensaje o una sonda puede dar lugar a varios informes de entrega y/o no entrega relativos a un determinado *destinatario potencial*. Cada uno de ellos marca el tránsito de un *paso* o *evento* de transmisión diferente.

9 Modelo operacional

En este punto se presenta un modelo operacional de tratamiento de mensajes. La realización concreta del modelo es objeto de otras Recomendaciones de la serie.

El STM puede transportar un objeto de información a usuarios individuales, LD o una combinación de ambos. El transporte se lleva a cabo por un proceso llamado *transmisión*, que comprende *pasos* y *eventos*. A continuación se definen y describen el proceso y sus subdivisiones, así como el papel que los usuarios y las LD desempeñan en éste.

9.1 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 ATM, facultados para *afirmar* la *entregabilidad* o no del mensaje descrito a los *destinatarios potenciales* de aquélla. La transmisión comprende también el transporte o tentativa de transporte al *originador* de cuantos informes provoquen el mensaje o la sonda.

La transmisión se desarrolla a través de una secuencia de *pasos de transmisión* y *eventos*. Un **paso de transmisión** (o **paso**) consiste en el transporte de un mensaje, una sonda o un informe desde un objeto funcional a otro «adyacente» al primero. Un **evento de transmisión** (o **evento**) consiste en el tratamiento de un mensaje, una sonda o un informe en un objeto funcional, tratamiento que puede influir en la selección, por parte del objeto funcional, del siguiente paso o evento.

En la figura 5/X.402 se presenta de manera esquemática el flujo de información de la transmisión. Se muestran en ella los tipos de objetos funcionales - usuarios directos, usuarios indirectos, AU, MM, ATM y UA - que pueden tomar parte en una transmisión, los objetos de información - mensajes, sondas, e informes - que pueden ser transportados entre aquéllos y los nombres de los pasos de transmisión mediante los cuales se efectúan esos transportes.

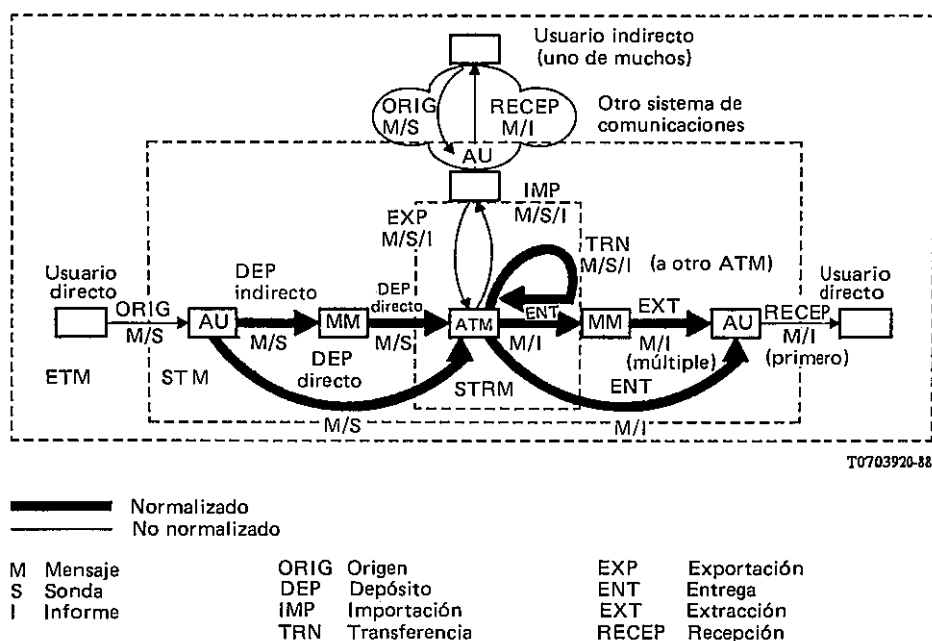


FIGURA 5/X.402

Flujo de información de la transmisión

La figura 5/X.402 destaca el hecho de que, un mensaje o informe, pueden ser extraídos repetidamente y que sólo el primer transporte de un objeto extraído desde el AU al usuario constituye *recepción*.

El evento tiene un papel destacado en la transmisión. La *división* duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus *destinatarios inmediatos*. Se llaman **destinatarios inmediatos** a los destinatarios potenciales asociados a un caso particular de un mensaje o sonda. Un ATM efectúa una división si el siguiente paso o evento, necesario para transportar un mensaje o sonda a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros. En cada una de las descripciones de pasos y eventos que a continuación se hacen, se supone que el paso o evento es adecuado para todos los destinatarios inmediatos, situación que puede crearse, si es preciso, por división.

9.2 Funciones de la transmisión

Los usuarios y las LD desempeñan una diversidad de papeles en la transmisión de un mensaje o una sonda. A esos papeles se les clasifica, de manera informal, en paquetes «origen», papeles «destino» y categorías a las que se pueden elevar los usuarios o las LD.

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

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

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

- destinatario deseado:** Uno de los usuarios o de las LD que el originador especifica como destinos de un mensaje o una sonda.
- destinatario alternativo especificado por el originador:** Usuario (o LD si hay alguna) al que el originador pide que sea transportado un mensaje o sonda, si no puede transportarse a un determinado destinatario deseado.
- destinatario miembro:** LD o usuario al cual se transporta un mensaje (pero no una sonda), como resultado de una *ampliación de LD*.

- d) **destinatario alternativo designado por el destinatario:** Usuario (o LD si hay alguna) elegido por un destinatario miembro, o receptor deseado o alternativo al especificado por el originador, para que *redireccione* mensajes.

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

- a) **destinatario potencial:** Cualquier LD o usuario hacia el cual se transporta un mensaje en cualquier momento durante la transmisión. Ha de tratarse necesariamente de un destinatario deseado o alternativo al especificado por el originador o al asignado.
- b) **destinatario efectivo (o receptor):** Un destinatario potencial para el cual tiene lugar la *entrega* o la *afirmación*.

9.3 Pasos de la transmisión

En la primera columna del cuadro 5/X.402 figura una lista de los tipos de pasos que pueden producirse en una transmisión. Para cada tipo de la lista se indica, en la segunda columna, si ese paso está normalizado o no en la presente Recomendación o en otras de la misma serie; en la tercera columna, las clases de objetos de información - mensajes, sondas e informes - cuyo transporte está permitido en ese paso y en la cuarta columna, las clases de objetos funcionales - usuarios, AU, MM, ATM y UA - que pueden participar en ese paso como origen o destino del objeto.

El cuadro 5/X.402 está dividido en tres secciones. Los pasos de la primera sección corresponden a la «creación» de mensajes y sondas, los de la última a la «distribución» de mensajes e informes y los de la de en medio a la «remisión» de mensajes, sondas e informes.

En los puntos que siguen se definen y describen cada uno de los tipos de pasos de transmisión cuya relación figura en el cuadro 5/X.402.

CUADRO 5/X.402

Pasos de transmisión

Paso de transmisión	¿Normalizado?	Objetos de información			Objetos funcionales				
		M	S	I	Usuario	AU	MM	ATM	UA
Origen	No	X	X	–	O	D	–	–	–
Depósito	Sí	X	X	–	–	O	OD	D	–
Importación	No	X	X	X	–	–	–	D	O
Transferencia	Sí	X	X	X	–	–	–	OD	–
Exportación	No	X	X	X	–	–	–	O	D
Entrega	Sí	X	–	X	–	D	D	O	–
Recuperación	Sí	X	–	X	–	D	O	–	–
Recepción	No	X	–	X	D	O	–	–	–

M Mensaje O Origen
S Sonda D Destino
I Informe X Permitido

9.3.1 Origen

En un paso de **origen**, un usuario directo transporta un mensaje o una sonda a su AU, o bien un usuario indirecto hace otro tanto al sistema de comunicaciones que le presta servicio. Este paso genera el mensaje o la sonda y constituye el primero de su transmisión.

El referido usuario es el originador del mensaje o de la sonda. Como tal originador identifica los destinatarios deseados de uno u otro objetos funcionales. Además, para cada destinatario deseado, puede identificar un destinatario alternativo, aunque no es preciso que lo haga.

9.3.2 Depósito

En un paso de **depósito** se transporta a un ATM, un mensaje o sonda que quedan a cargo del STRM. Cabe distinguir los dos tipos siguientes de depósito:

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

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

- b) **depósito directo:** Paso de transmisión en el que el AU o la MM originador transportan un mensaje o sonda a un ATM. Este paso sigue al de origen o se produce como parte de un depósito indirecto.

Es posible dar este paso tanto si el usuario está equipado con una MM como si no lo está.

El depósito indirecto y el directo son funcionalmente equivalentes, salvo en lo que se refiere a las capacidades adicionales de las que es posible disponer con el primero. El depósito indirecto puede diferir del directo en otros aspectos (por ejemplo, en el número de sistemas abiertos con los que debe establecer una interacción aquel que incorpore un AU) y ser por ello preferible al depósito directo.

Al AU o a la MM que participa en el depósito directo se le llama **agente de depósito**. Un agente de depósito se da a conocer al STRM mediante un proceso de registro, como resultado del cual el agente de depósito y el STRM quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.3 Importación

En un paso de **importación**, una UA transporta un mensaje, una sonda o un informe a un ATM. Este paso introduce en el STRM un objeto de información llevado en otro sistema de comunicaciones, y se produce a continuación de su transporte por dicho sistema.

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

9.3.4 Transferencia

En un paso de **transferencia**, un ATM transporta un mensaje, una sonda o un informe a otro ATM. En este paso, el transporte del objeto de información tiene lugar a lo largo de distancias físicas y, a veces, organizativas. Se produce a continuación del depósito directo o de la importación o de una transferencia previa.

Por supuesto, este paso sólo puede darse si el STRM consta de varios ATM.

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

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

9.3.5 Exportación

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

El ATM puede generar, como parte de este paso, un informe de entrega.

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

9.3.6 Entrega

En un paso de **entrega**, un ATM transporta un mensaje o un informe a una MM o a un AU. La MM y el AU corresponden a un destinatario potencial del mensaje o al originador del mensaje o sonda objeto del informe. En este paso se confía el objeto de información a un representante del usuario y se produce tras el depósito directo, la importación o la transferencia. Además, se eleva al usuario en cuestión a la categoría de destinatario efectivo.

En el caso de un mensaje el ATM puede generar, como parte de este paso, un informe de entrega.

Se llama **agente de entrega** a la MM o al AU que participan en la misma. Un agente de entrega se da a conocer al STRM mediante un proceso de registro, como resultado del cual el agente de entrega y el STRM quedan mutuamente informados de sus respectivos nombres, de sus localizaciones y de cualesquiera otras características necesarias para su interacción.

9.3.7 Recuperación

En un paso de **recuperación**, la MM de un usuario transporta un mensaje o un informe a su AU. El usuario en cuestión es un destinatario efectivo del mensaje o el originador del mensaje o de la sonda objeto. Este paso extrae del almacenamiento el objeto de información de manera no destructiva. Se produce tras el paso de entrega o de una recuperación previa.

El paso de recuperación sólo puede darse si el usuario está equipado con una MM.

9.3.8 Recepción

En un paso de **recepción**, un AU transporta un mensaje o informe a su usuario directo, o bien el sistema de comunicaciones que presta servicio a un usuario indirecto transporta ese objeto de información a dicho usuario. En cualquier caso, este paso transporta el objeto a su destino último.

Si se trata de un usuario directo, este paso sucede a la entrega del objeto o a la primera recuperación (solamente). Si se trata de un usuario indirecto, sucede al transporte de un objeto de información por el sistema de comunicaciones que sirve al usuario. En cualquiera de los dos casos, el usuario es un destinatario potencial (pero si es usuario directo, es destinatario no ya potencial sino efectivo) del mensaje objeto o la sonda objeto.

9.4 Eventos de la transmisión

En la primera columna del cuadro 6/X.402 se da una relación de los tipos de eventos que pueden producirse en una transmisión. Para cada tipo de evento se indica, en la segunda columna, los tipos de objetos de información, - mensajes, sondas e informes - para los que pueden desarrollarse tales eventos, y en la tercera columna, los tipos de objetos funcionales - usuarios, AU, MM, ATM y UA - a los que les está permitido desarrollarlos.

Todos los eventos se producen dentro del STRM.

CUADRO 6/X.402
Eventos de transmisión

Evento de transmisión	Objetos de información			Objetos funcionales				
	M	S	I	Usuario	UA	MM	ATM	AU
División	X	X	—	—	—	—	X	—
Combinación	X	X	X	—	—	—	X	—
Resolución de nombre	X	X	—	—	—	—	X	—
Ampliación de LD	X	—	—	—	—	—	X	—
Redireccionamiento	X	X	—	—	—	—	X	—
Conversión	X	X	—	—	—	—	X	—
No entrega	X	—	X	—	—	—	X	—
No afirmación	—	X	—	—	—	—	X	—
Afirmación	—	X	—	—	—	—	X	—
Encaminamiento	X	X	X	—	—	—	X	—

M Mensaje
S Sonda
I Informe
X Permitido

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

9.4.1 *División*

En un evento de **división**, un ATM duplica un mensaje o sonda y reparte, entre los objetos de información resultantes, la responsabilidad de sus destinatarios inmediatos. Este evento permite de manera efectiva a un ATM transportar independientemente un objeto a varios destinatarios potenciales.

Un ATM efectúa una división cuando el siguiente paso o evento, necesario para el transporte de una sonda o mensaje a algunos destinatarios inmediatos, difiere del necesario para transportarlo a otros.

9.4.2 *Combinación*

En un evento de **combinación**, un ATM 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 ATM puede, aunque no necesariamente, efectuar una combinación cuando determine que, para transportar a sus destinos varios objetos de información muy relacionados, hacen falta los mismos eventos y el mismo paso siguiente.

9.4.3 *Resolución de nombre*

En un evento de **resolución de nombre**, un ATM agrega la *dirección O/D* correspondiente al *nombre O/D* que identifica a uno de los destinatarios inmediatos de un mensaje o una sonda.

9.4.4 *Ampliación de LD*

En un evento de **ampliación de LD**, un ATM asigna una LD de entre los destinatarios de un mensaje (pero no de una sonda) a sus miembros, que de este modo se convierten en destinatarios miembros. Este evento elimina la falta de dirección de la especificación de los destinatarios inmediatos.

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

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

La ampliación de la LD está sujeta al permiso de presentación. En el caso de una LD jerarquizada, ese permiso debe haber sido concedido a la LD de la que aquella es miembro. De lo contrario, el permiso debe haber sido concedido al originador.

9.4.5 *Redireccionamiento*

En un evento de **redireccionamiento**, un ATM sustituye a un usuario o a una LD entre los destinatarios inmediatos de un mensaje o de una sonda, por un destinatario alternativo, especificado por el originador o asignado por el destinatario.

9.4.6 *Conversión*

En un evento de **conversión**, un ATM transforma partes del contenido de un mensaje de un TIC en otro, o altera una sonda de modo que parezca que los mensajes descritos fueron igualmente modificados. Este evento aumenta la probabilidad de que un objeto de información pueda ser entregado o afirmado, adaptándolo a sus destinatarios inmediatos.

Se distinguen los dos tipos de conversión que se indican a continuación, y que difieren en cómo se eligen el TIC de la información a convertir y el TIC resultante de la conversión:

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

9.4.7 *No entrega*

En un evento de **no entrega**, un ATM establece que el STRM no puede entregar un mensaje a sus destinatarios inmediatos, o no puede entregar un informe al originador de su mensaje o sonda objeto. Este evento detiene el transporte de un objeto al que el STRM considere intransportable.

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

Un ATM efectúa una no entrega cuando, por ejemplo, determina que los destinatarios inmediatos no están especificados adecuadamente, que no aceptan la entrega de mensajes como el mensaje de que se trate, o que no se les ha entregado dentro de los límites de tiempo preestablecidos.

9.4.8 No afirmación

En un evento de **no afirmación**, un ATM establece que el STRM no puede entregar un mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda.

El ATM genera, como parte de ese evento, un informe de no entrega.

Un ATM produce una no afirmación cuando, por ejemplo, encuentra que los destinatarios inmediatos no están especificados adecuadamente o que no aceptarían la entrega de un mensaje descrito.

9.4.9 Afirmación

En un evento de **afirmación**, un ATM establece que el STRM puede entregar cualquier mensaje descrito a los destinatarios inmediatos de una sonda. Este evento determina parcial o totalmente la respuesta a la cuestión planteada por una sonda y eleva a los destinatarios inmediatos a la categoría de destinatarios efectivos.

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

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

9.4.10 Encaminamiento

En un evento de **encaminamiento**, un ATM selecciona el ATM «adyacente» al que transferirá un mensaje, sonda o informe. Este evento determina, de manera incremental, el camino de un objeto de información a través del STRM y, obviamente, sólo puede producir si el STRM consta de varios ATM.

Hay dos tipos de encaminamiento, que difieren entre sí por la clase de transferencia para la que preparan:

- a) **encaminamiento interno:** Encaminamiento que prepara para una transferencia interna (es decir, una transferencia dentro de un DG).
- b) **encaminamiento externo:** Encaminamiento que prepara para una transferencia externa (es decir, una transferencia entre distintos DG).

Un ATM realiza un encaminamiento cuando determina que no puede efectuar ningún otro evento ni dar ningún paso con respecto a un objeto.

10 Modelo de seguridad

En este punto se presenta un modelo de seguridad abstracto para la transferencia de mensajes. La realización concreta del modelo es tema de otras Recomendaciones de la serie. El modelo de seguridad proporciona un marco para la descripción de los servicios de seguridad que contrarrestan los riesgos potenciales (véase el anexo D) del STM, y de los elementos de seguridad que facilitan estos servicios.

Las características de seguridad constituyen una ampliación facultativa del STM, que pueden emplearse para minimizar el riesgo de exposición de bienes de capital y recursos a las infracciones de una política de seguridad (riesgos). Su objetivo es proporcionar seguridad con independencia de los servicios de comunicaciones proporcionados por otras entidades, de nivel superior o inferior. Los riesgos pueden combatirse mediante el recurso a la seguridad de tipo físico, la seguridad de los computadores (COMPUSEC) o los servicios de seguridad proporcionados por el STM. Según cuales sean los riesgos que se contemplen, se seleccionarán unos u otros servicios de seguridad de STM en combinación con adecuadas medidas de seguridad física y de COMPUSEC. Los servicios de seguridad facilitados por el STM se describen más adelante. La denominación y la estructuración de los servicios se basan en la norma ISO 7498-2.

Nota – A pesar de estas características de seguridad, pueden producirse ciertas agresiones contra las comunicaciones entre un usuario y el STM o contra las comunicaciones de usuario a usuario (por ejemplo, en el caso de usuarios que acceden al STM a través de una unidad de acceso, o de usuarios con acceso a distancia a sus AU). Para contrarrestar esas agresiones es preciso ampliar los servicios y modelos actuales de seguridad, lo que requiere *ulterior estudio*.

En muchos casos, la amplitud de los tipos de riesgos queda cubierta por varios de los servicios anotados.

Los servicios de seguridad se facilitan mediante el uso de elementos de servicio del sobre de mensajes del STRM. El sobre contiene argumentos propios de la seguridad, tal como se describe en la Recomendación X.411. La descripción de los servicios de seguridad que figura más adelante, se hace de la siguiente manera: en el § 10.2 se da una relación de los servicios con su definición e indicación, en cada caso, de cómo pueden ser proporcionados empleando los elementos de seguridad de la Recomendación X.411 y en el § 10.3 se describen uno a uno los elementos de seguridad con definición, en cada caso, del elemento de servicio, y referencias a sus argumentos constituyentes, según la Recomendación X.411.

Muchas de las técnicas empleadas se basan en mecanismos de cifrado. Los servicios de seguridad del STM permiten elegir los algoritmos con flexibilidad. Sin embargo, en algunos casos, sólo se ha definido totalmente en esta Recomendación la utilización del cifrado asimétrico. En una futura versión de la Recomendación se podrán utilizar mecanismos alternativos de cifrado simétrico.

Nota – Las expresiones «servicio de seguridad» y «elemento de seguridad» que se emplean en este punto no deben confundirse con las expresiones «elemento de servicio» y «servicio» empleadas en la Recomendación X.400. Las primeras expresiones se utilizan en este punto para mantener la armonía con ISO 7498-2.

10.1 *Políticas de seguridad*

Los servicios de seguridad del STM deben poder facilitar una amplia gama de políticas de seguridad, que va más allá de los límites del propio STM. Los servicios seleccionados y los riesgos contra los que se pretende asegurarse dependerán de la aplicación concreta y de los niveles de confianza que se tenga en las distintas partes del sistema.

La política de seguridad define cómo reducir a un nivel aceptable el riesgo de exposición al peligro de los bienes de capital.

Además será preciso el funcionamiento entre dominios diferentes, cada uno de ellos con su propia política de seguridad. Se deberán establecer acuerdos bilaterales sobre ese interfuncionamiento, ya que las políticas globales de seguridad, más amplias que la del mero STM, a que esos dominios estén sujetos, diferirán de todos modos entre sí. Debe definirse esto de tal manera que no se entre en conflicto con la política de seguridad de ninguno de los dos dominios y que el acuerdo llegue efectivamente a formar parte de la política de seguridad global de ambos.

10.2 *Servicio de seguridad*

Se definen en este punto los servicios de seguridad de la transferencia de mensajes. La denominación y la estructura de los mismos se basa en la norma ISO 7498-2.

Los servicios de seguridad de la transferencia de mensajes son de amplias y variadas clases. Esas clases, y los servicios correspondientes a cada una de ellas, aparecen relacionadas en el cuadro 7/X.402.

A lo largo de la serie de definiciones de servicios que viene a continuación se hace referencia a la figura 6/X.402, que representa el modelo funcional del STM de forma simplificada. En el texto se hace referencia en varias ocasiones a las etiquetas numeradas.

10.2.1 *Servicios de seguridad de autenticación de origen*

Estos servicios de seguridad facilitan la autenticación de la identidad de entidades pares comunicantes y de fuentes de datos.

10.2.2.1 *Servicios de seguridad de autenticación de origen de datos*

Estos servicios de seguridad permiten la confirmación del origen de un mensaje, una sonda o un informe a todas las entidades afectadas (es decir, los ATM o los usuarios del STRM destinatarios). No pueden proteger contra la duplicación de mensajes, sondas e informes.

10.2.1.1.1 *Servicio de seguridad de autenticación de origen de mensajes*

Este servicio de seguridad permite la confirmación del origen de un mensaje.

El servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de mensajes o el de integridad de argumento de mensajes. El primero se puede emplear para dar servicio de seguridad a cualquiera de las partes afectadas (1 a 5 inclusive, en la figura 6/X.402), mientras que el segundo sólo puede utilizarse para proporcionar servicio de seguridad a los usuarios del STRM (1 ó 5 en la figura 6/X.402). El elemento de seguridad elegido depende de la política de seguridad vigente.

10.2.1.1.2 *Servicio de seguridad de autenticación de origen de sondas*

El servicio de seguridad de autenticación de origen de sondas permite la confirmación del origen de una sonda.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de sondas. Puede emplearse el elemento de seguridad para dar el servicio a cualquiera de los ATM a través de los cuales se transfiere la sonda (2 a 4 inclusive, en la figura 6/X.402).

10.2.1.1.3 *Servicio de seguridad de autenticación de origen de informes*

El servicio de seguridad de autenticación de origen de informes permite la confirmación del origen de un informe.

Este servicio puede proporcionarse utilizando el elemento de seguridad de autenticación de origen de informes. El elemento de seguridad se emplea para dar servicio de seguridad al originador del mensaje o de la sonda objeto, así como a cualquiera de los ATM a través de los cuales se transfiere el informe (1 a 5 inclusive, en la figura 6/X.402).

CUADRO 7/X.402

Servicios de seguridad de la transferencia de mensajes

	Servicio							
	AU/ AU	AM/ ATM	ATM/ MM	ATM/ AU	AU/ MM	AU/ ATM	ATM/ ATM	MM/ AU
<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	*	—	—	—	—	—	—	—
<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 MM	—	*	—	—	—	—	—	—

* Un asterisco debajo de un encabezamiento del tipo X/Y significa que el servicio puede ser proporcionado desde un objeto funcional de tipo X a uno de tipo Y.

a) Este servicio lo proporciona la MM del destinatario al AU del originador.

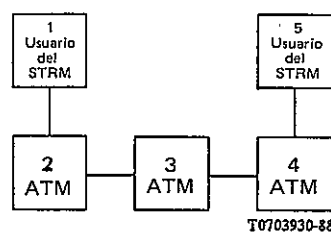


FIGURA 6/X.402
Modelo funcional de STM simplificado

10.2.1.2 Servicio de seguridad de prueba de depósito

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido recibido por el STRM para su entrega al destinatario o destinatarios especificados originalmente.

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

10.2.1.3 Servicio de seguridad de prueba de entrega

Este servicio de seguridad permite al originador de un mensaje obtener la confirmación de que ha sido entregado por el STRM al destinatario o destinatarios deseados.

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

10.2.2 Servicio de seguridad de gestión de acceso seguro

El servicio de seguridad de gestión de acceso seguro se ocupa de la protección de los recursos contra su utilización no autorizada. Puede dividirse en dos componentes: servicio de autenticación de entidades pares y servicio de contexto de seguridad.

10.2.2.1 Servicio de seguridad de autenticación de entidades pares

Este servicio de seguridad se proporciona al establecer una conexión, para confirmar la identidad de la entidad que se conecta. Puede utilizarse en los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402 y asegura, al utilizarlo únicamente, contra los intentos de suplantación o de 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 STM no presta un servicio de seguridad de confidencialidad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, como resultado del empleo del elemento de seguridad de intercambio de autenticación, para proporcionar el servicio de seguridad de autenticación de entidades pares. Este servicio de seguridad puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402.

10.2.3.2 Servicio de seguridad de confidencialidad de contenido

El servicio de seguridad de confidencialidad de contenido garantiza que el contenido de un mensaje sólo sea conocido por su emisor y su destinatario.

Es posible proporcionar este servicio mediante una combinación de los elementos de seguridad de confidencialidad de contenido y de confidencialidad de argumento de mensajes. Este último se puede emplear para transferir una clave secreta, utilizada con el primero en el cifrado del contenido del mensaje. Con estos elementos de seguridad, se proporciona el servicio desde el usuario 1 al usuario 5 del STRM, de la figura 6/X.402, siendo el mensaje ininteligible para los ATM.

10.2.3.3 *Servicio de seguridad de confidencialidad de flujo de mensajes*

Este servicio de seguridad protege contra la extracción de información que podría lograrse mediante la observación del flujo de mensajes. El STM proporciona este servicio sólo de forma limitada.

La técnica del sobre doble permite que un mensaje completo se convierta en contenido de otro mensaje. Esta técnica puede emplearse para ocultar la información de direccionamiento en determinados tramos del STRM. Junto con el rellano de tráfico (que queda fuera del objeto actual de esta Recomendación) podría utilizarse para lograr la confidencialidad del flujo de mensajes. Otros elementos de este servicio, tales como el control del encaminamiento o los pseudónimos, quedan también fuera del objeto de esta Recomendación.

10.2.4 *Servicios de seguridad de integridad de datos*

Estos servicios de seguridad se proporcionan para contrarrestar riesgos activos contra el STM.

10.2.4.1 *Servicio de seguridad de integridad de conexión*

El STM no presta un servicio de seguridad de integridad de conexión. No obstante, pueden proporcionarse datos en capas subyacentes para la invocación de tal servicio, utilizando el elemento de seguridad de intercambio de autenticación en la prestación del servicio de seguridad de autenticación de entidades pares. El servicio puede ser necesario en alguno de los enlaces 1-2, 2-3, 3-4 ó 4-5 de la figura 6/X.402.

10.2.4.2 *Servicio de seguridad de integridad de contenido*

Este servicio de seguridad garantiza la integridad del contenido de un mensaje. Para ello, se habilita la determinación de si el contenido del mensaje ha sido o no modificado. El servicio no permite detectar reactuaciones de mensajes, lo que si es facilitado, en cambio, por el servicio de seguridad de integridad de secuencia de mensajes.

El servicio puede proporcionarse de dos modos diferentes, utilizando dos diferentes combinaciones de elementos de seguridad.

El elemento de seguridad de integridad de contenido junto con el de integridad de argumento de mensajes y, en algunos casos, el de confidencialidad de argumento de mensajes, pueden utilizarse para prestar servicio de seguridad a un destinatario de mensajes, es decir, para la comunicación del usuario 1 al usuario 5 del STRM, de la figura 6/X.402. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cual sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de argumento de mensajes se protege la verificación de integridad del contenido contra posibles cambios. La integridad de cualquier argumento de mensaje confidencial se garantiza utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

También puede emplearse el elemento de seguridad de autenticación de origen de mensajes para prestar este servicio de seguridad.

10.2.4.3 *Servicio de seguridad de integridad de secuencia de mensajes*

Este servicio de seguridad protege al originador y al destinatario de una secuencia de mensajes, contra el reordenamiento de la secuencia. Al mismo tiempo, protege contra la reactuación de mensajes.

Puede proporcionarse el servicio haciendo uso de una combinación de los elementos de seguridad de integridad de secuencia de mensajes y de integridad de argumento de mensajes. El primero da a cada mensaje un número de secuencia que puede protegerse contra posibles cambios mediante el segundo elemento. Es posible proporcionar simultáneamente confidencialidad e integridad del número de secuencia de mensajes, empleando el elemento de seguridad de confidencialidad de argumento de mensajes.

Estos elementos de seguridad facilitan el servicio para la comunicación del usuario 1 al usuario 5 del STRM, de la figura 6/X.402, y no a los ATM intermedios.

10.2.5 *Servicio de seguridad de no rechazo*

Estos servicios de seguridad dan garantía absoluta a un tercero, después de que el mensaje ha sido depositado, enviado o entregado, de que el depósito, el envío o la recepción se han producido tal como se dice. Téngase en cuenta

que, para que esto funcione correctamente, la política de seguridad debe abarcar de manera explícita la gestión de claves asimétricas, a efectos de servicios de no rechazo, si se utilizan algoritmos asimétricos.

10.2.5.1 *Servicio de seguridad de no 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 STRM, de la figura 6/X.402. El elemento de seguridad de integridad de contenido se emplea para computar una verificación de integridad de contenido, como una función del contenido total del mensaje. Dependiendo de cuál sea el método de cómputo de la verificación, puede ser necesaria una clave secreta que se envía, de manera confidencial, al destinatario del mensaje utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. Mediante el elemento de seguridad de integridad de mensajes se protege la verificación y, si hace falta, a la etiqueta de seguridad de mensajes, contra un posible cambio y/o rechazo. Cualquier argumento de mensaje confidencial queda protegido contra cambio y/o rechazo utilizando el elemento de seguridad de confidencialidad de argumento de mensajes.

Si no se requiere el servicio de seguridad de confidencialidad de contenido, también es posible emplear, como base de este servicio de seguridad, el elemento de seguridad de autenticación de origen de mensajes. En este caso puede proporcionarse el servicio de seguridad a todos los elementos del STM, es decir, a todos los usuarios del STRM y ATM de la figura 6/X.402.

10.2.5.2 *Servicio de seguridad de no rechazo de depósito*

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido depositado en el STRM para su entrega al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de depósito, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de depósito (más débil).

10.2.5.3 *Servicio de seguridad de no rechazo de entrega*

Este servicio de seguridad da, al originador del mensaje, garantía absoluta de que el mensaje ha sido entregado al destinatario o destinatarios originalmente especificados.

El servicio se proporciona utilizando el elemento de seguridad de prueba de entrega, de manera muy similar a como se utiliza ese elemento de seguridad para facilitar el servicio de seguridad de prueba de entrega (más débil).

10.2.6 *Servicio de seguridad del etiquetado de seguridad de mensajes*

Este servicio de seguridad permite asociar etiquetas de seguridad a todas las entidades del STM, es decir, los ATM y los usuarios del STRM. Conjuntamente con el servicio de seguridad de contexto de seguridad, facilita la ejecución de políticas de seguridad que precisen qué partes del STM pueden tratar mensajes, mediante las etiquetas de seguridad asociadas especificadas.

El servicio lo proporciona el elemento de seguridad de la etiqueta de seguridad de mensajes. Los elementos de seguridad de integridad de argumento de mensajes y de confidencialidad de argumento de mensajes aseguran la integridad y confidencialidad de la etiqueta.

10.2.7 *Servicio de gestión de la seguridad*

El STM necesita cierto número de servicios de gestión de seguridad. Los únicos servicios de gestión previstos en la Recomendación X.411 tratan del cambio de credenciales y del registro de etiquetas de seguridad de usuario del STRM.

10.2.7.1 *Servicio de seguridad de cambio de credenciales*

Este servicio de seguridad permite a una entidad del STM cambiar las credenciales que le afectan, contenidas en otra entidad del STM. Puede proporcionarse utilizando el elemento de seguridad de cambio de credenciales.

10.2.7.2 *Servicio de seguridad de registros*

Este servicio de seguridad permite el establecimiento en un ATM, de las etiquetas de seguridad autorizadas para un determinado usuario del STRM. Puede proporcionarse utilizando el elemento de seguridad de registros.

10.2.7.3 *Servicio de seguridad de registro de la MM*

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

10.3 *Elementos de seguridad*

En los puntos que siguen se describen los elementos de seguridad, disponibles en los protocolos de la Recomendación X.411, para facilitar los servicios de seguridad en el STM. Esos elementos están relacionados directamente con los argumentos de varios servicios descritos en la Recomendación X.411. Este punto tiene por objeto extraer los elementos de las definiciones de servicios de la Recomendación X.411 que tienen relación con la seguridad, y definir la función de cada uno de esos elementos de seguridad identificados.

10.3.1 *Elementos de seguridad de autenticación*

Estos elementos de seguridad se definen para facilitar los servicios de seguridad de autenticación e integridad.

10.3.1.1 *Elementos de seguridad de intercambio de autenticación*

El elemento de seguridad de intercambio de autenticación está concebido para autenticar, posiblemente de manera mutua, la identidad de un usuario del STRM a un ATM, de un ATM a un ATM, de un ATM a un usuario del STRM de una MM a un AU o de un AU a una MM. Se basa en la utilización o el intercambio de datos secretos, tales como contraseñas o testigos cifrados asimétricamente o simétricamente. El resultado del intercambio es la confirmación de la identidad de la otra parte y, facultativamente, la transferencia de datos confidenciales que pueden utilizarse para la provisión del servicio de seguridad de confidencialidad de conexiones y/o de integridad de conexiones, en capas subyacentes. Dicha autenticación sólo es válida en el instante en que se produce, dependiendo la continuidad de la validez de la identidad autenticada de si se utiliza o no intercambio de datos confidenciales, o algún otro mecanismo, para establecer un trayecto de comunicación seguro. El establecimiento y uso de un trayecto de comunicación seguro está fuera del alcance de la presente Recomendación.

Este elemento de seguridad emplea el argumento de credenciales de iniciador y el resultado de credenciales de contestador de los servicios vinculados al STRM, a la MM y a un ATM. Las credenciales transferidas son contraseñas o testigos.

10.3.1.2 *Elementos de seguridad de autenticación de origen de datos*

Estos elementos de seguridad están concebidos de manera específica para facilitar los servicios de autenticación de origen de datos, aunque también se les puede emplear para proporcionar determinados servicios de integridad de datos.

10.3.1.2.1 *Elemento de seguridad de autenticación de origen de mensajes*

El elemento de seguridad de autenticación de origen de mensajes permite, a cualquiera que reciba o transfiera un mensaje, autenticar la identidad del usuario del STRM que originó el mensaje. Esto puede significar la prestación del servicio de seguridad de autenticación de origen de mensajes o del de no rechazo de origen.

El elemento de seguridad implica la transmisión, como parte de mensaje, de una verificación de autenticación de origen de mensajes, computada como una función del contenido del mensaje, del identificador de contenido de mensajes y de la etiqueta de seguridad de mensajes. Si también hace falta el servicio de seguridad de confidencialidad de contenido, el control de verificación se computa como una función del contenido del mensaje cifrado, en vez de una función del no cifrado. Actuando sobre el contenido del mensaje según es transportado en el mensaje global (es decir, después del elemento de seguridad facultativo de confidencialidad de contenido), cualquier entidad del STM puede verificar la integridad del mensaje global sin necesidad de ver el texto en claro del contenido del mensaje. No obstante, si se hace uso del servicio de seguridad de confidencialidad de contenido, no puede emplearse el elemento de seguridad de autenticación de origen de mensajes para proporcionar el servicio de seguridad de no rechazo de origen.

El elemento de seguridad utiliza la verificación de autenticación de origen de mensajes, que es uno de los argumentos de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.1.2.2 *Elemento de seguridad de autenticación de origen de sondas*

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de sondas permite a cualquier ATM autenticar la identidad del usuario del STRM que originó una determinada sonda.

Este elemento de seguridad utiliza la verificación de autenticación de origen de sondas, que es uno de los 5 argumentos del servicio de depósito de sondas.

10.3.1.2.3 *Elemento de seguridad de autenticación de origen de informes*

De manera similar al elemento de seguridad de autenticación de origen de mensajes, el de origen de informes permite, a cualquier ATM o usuario del STRM que recibe un informe, autenticar la identidad del ATM que lo originó.

Este elemento de seguridad utiliza la verificación de autenticación de origen de informes, que es uno de los argumentos del servicio de entrega de informes.

10.3.1.3 *Elemento de seguridad de prueba de depósito*

Este elemento de seguridad proporciona al originador de un mensaje los medios para establecer que el mensaje fue aceptado por el STM para su transmisión.

El elemento de seguridad está constituido por dos argumentos: una petición de prueba de depósito enviada con un mensaje en el momento del depósito, y la prueba de depósito devuelta al usuario del STRM como parte de los resultados del depósito de mensajes. El STRM genera la prueba de depósito, que es computada como una función de todos los argumentos del mensaje depositado, del identificador de depósito de mensajes y del momento en que se produce el depósito de mensajes.

Puede utilizarse el argumento de prueba de depósito para facilitar el servicio de seguridad de prueba de depósitos. Dependiendo de cuál sea la política de seguridad en vigor, puede también facilitar el servicio de seguridad de no rechazo de depósito (más fuerte).

La petición de prueba de depósito es un argumento del servicio de depósito de mensajes. La prueba de depósito es uno de los resultados del servicio de depósito de mensajes.

10.3.1.4 *Elemento de seguridad de prueba de entrega*

Este elemento de seguridad proporciona al originador de un mensaje medios para establecer que el mensaje fue entregado en destino por el STM.

El elemento de seguridad está constituido por varios argumentos. El originador del mensaje incluye una petición de prueba de entrega en el mensaje depositado, y esta petición se entrega a cada destinatario con el mensaje. Un destinatario puede entonces computar la prueba de entrega como una función de un cierto número de argumentos asociados al mensaje. El STRM devuelve la prueba de entrega al originador del mensaje, como parte de un informe sobre los resultados del depósito de mensajes original.

Es posible utilizar la prueba de entrega para facilitar el servicio de seguridad de prueba de entrega. Dependiendo de cuál sea la política de seguridad en vigor, podría también facilitar el servicio de seguridad de no rechazo de entrega (más fuerte).

La petición de prueba de entrega es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes. La prueba de entrega es a la vez uno de los resultados del servicio de entrega de mensajes y uno de los argumentos de los servicios de transferencia de informes y de entrega de informes.

Nota – La no recepción de una prueba de entrega no implica la no entrega.

10.3.2 *Elementos de seguridad de gestión de acceso seguro*

Estos elementos de seguridad se definen para facilitar el servicio de seguridad de acceso seguro y los servicios de gestión de la seguridad.

10.3.2.1 *Elemento de seguridad de contexto de seguridad*

Cuando un usuario del STRM o un ATM se vincula a un ATM o a un usuario del STRM, la operación de vinculación especifica el contexto de seguridad de la conexión. Esto limita el alcance del paso de mensaje por referencia a las etiquetas asociadas a los mensajes. Además, el contexto de seguridad de la conexión puede ser alterado temporalmente para mensajes depositados o entregados.

El propio contexto de seguridad consta de una o más etiquetas de seguridad, que definen la sensibilidad de interacciones que pueden producirse, en línea con la política de seguridad en vigor.

El contexto de seguridad es un argumento de los servicios vinculados al STRM y a un ATM.

10.3.2.2 *Elemento de seguridad de registros*

El elemento de seguridad de registros permite el establecimiento en un ATM de etiquetas de seguridad autorizadas de un usuario del STRM.

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

10.3.2.3 *Elemento de seguridad de registro de la MM*

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

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

10.3.3 *Elementos de seguridad de confidencialidad de datos*

A todos estos elementos de seguridad, basados en la utilización del cifrado, les afecta la provisión de la confidencialidad de los datos que pasan de una entidad del STM a otra.

10.3.3.1 *Elemento de seguridad de confidencialidad de contenidos*

El elemento de seguridad de confidencialidad de contenidos garantiza la protección del mensaje contra indiscreciones durante la transmisión, mediante un elemento de seguridad cifrado. El elemento de seguridad funciona de modo tal que solo el destinatario y el emisor del mensaje pueden conocer el texto en claro del contenido del mensaje.

La especificación del algoritmo de cifrado, la clave empleada y cualquier otro dato de inicialización, se transportan utilizando los elementos de seguridad de confidencialidad de argumento de mensajes y de integridad de argumento de mensajes. El algoritmo y la clave se emplean entonces para cifrar o descifrar los contenidos de los mensajes.

Este elemento de seguridad hace uso del identificador de algoritmo de confidencialidad de contenidos, que es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.3.2 *Elemento de seguridad de confidencialidad de argumento de mensajes*

El elemento de seguridad de confidencialidad de argumento de mensajes proporciona la confidencialidad, la integridad y, si hace falta, la irrevocabilidad de los datos de destinatario asociados a un mensaje. De manera específica, estos datos incluirán cuantas claves criptográficas y datos conexos hagan falta para el funcionamiento adecuado de los elementos de seguridad de confidencialidad e integridad, caso de que se invoquen esos elementos.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de confidencialidad de argumento de mensajes constituyen los datos cifrados, dentro del testigo de mensajes. Los datos cifrados del testigo de mensajes resultan ininteligibles para todos los ATM.

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

10.3.4 *Elementos de seguridad de integridad de datos*

Estos elementos se proporcionan para facilitar la prestación de los servicios de integridad de datos, autenticación de datos y no rechazo.

10.3.4.1 *Elemento de seguridad de integridad de contenidos*

El elemento de seguridad de integridad de contenidos protege el contenido de un mensaje contra posibles modificaciones durante la transmisión.

Este elemento emplea uno o más algoritmos de criptografía. La especificación del algoritmo o algoritmos, la clave o claves utilizadas y cualquier otro dato de inicialización se transportan utilizando los elementos de seguridad de confidencialidad e integridad de argumento de mensajes. El resultado de la aplicación de los algoritmos y de la clave es la verificación de integridad de contenidos, que se envía en el sobre del mensaje. El elemento de seguridad sólo está disponible para el destinatario o destinatarios del mensaje, puesto que actúa en el texto en claro de los contenidos de los mensajes.

Si se protegiera el control de verificación de integridad de contenidos utilizando el elemento de seguridad de integridad de argumentos de mensajes, se le podría emplear, dependiendo de cuál fuese la política de seguridad en vigor, para facilitar la prestación del servicio de seguridad de no rechazo de origen.

El control de verificación de integridad de contenido es un argumento de los servicios de depósito de mensajes, transferencia de mensajes y entrega de mensajes.

10.3.4.2 *Elemento de seguridad de integridad de argumento de mensajes*

El elemento de seguridad de integridad de argumento de mensajes proporciona la integridad y, si hace falta, la irrevocabilidad de determinados argumentos asociados a un mensaje. De manera específica, estos argumentos pueden comprender cualquier selección del identificador de algoritmo de confidencialidad de contenidos, del control de verificación de integridad de contenidos, de la etiqueta de seguridad de mensajes, de la petición de prueba de entrega y del número de secuencia de mensajes.

El elemento de seguridad funciona mediante el testigo de mensajes. Los datos a proteger por el elemento de seguridad de integridad de argumento de mensajes constituyen los datos firmados, dentro del testigo de mensajes.

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

10.3.4.3 *Elemento de seguridad de integridad de secuencia de mensajes*

El elemento de seguridad de integridad de secuencia de mensajes protege al emisor y al destinatario de un mensaje contra la recepción de mensajes desordenados o duplicados.

Cada mensaje tiene asociado un número de secuencia de mensajes. Este número identifica la posición de un mensaje en una secuencia, desde el originador al destinatario. Así pues, cada pareja originador-destinatario que necesite utilizar este elemento de seguridad deberá mantener una secuencia precisa de números de mensajes. Este elemento de seguridad no facilita la inicialización o sincronización de números de secuencia de mensajes.

10.3.5 *Elementos de seguridad de no rechazo*

En la Recomendación X.411 no se definen, de manera específica, los elementos de seguridad de no rechazo. Los servicios de no rechazo pueden proporcionarse mediante una combinación de otros elementos de seguridad.

10.3.6 *Elementos de seguridad de la etiqueta de seguridad*

La finalidad de estos elementos de seguridad es facilitar el etiquetado de seguridad en el STM.

10.3.6.1 *Elemento de seguridad de etiqueta de seguridad de mensajes*

Se pueden etiquetar los mensajes con datos según se especifique en la política de seguridad vigente. La etiqueta de seguridad de mensajes está a disposición de los ATM intermedios, como parte de la política de seguridad global del sistema.

Es posible enviar una etiqueta de seguridad de mensajes como un argumento de mensajes y que sea protegida por el elemento de seguridad de integridad de argumento de mensajes o el de autenticación de origen de mensajes, del mismo modo que otros argumentos de mensajes.

Si son necesarias, tanto la confidencialidad como la integridad, se puede proteger la etiqueta de seguridad de mensajes, de manera alternativa, utilizando el elemento de seguridad de confidencialidad de argumento de mensajes. En este caso, la etiqueta así protegida es un argumento de originador-destinatario, y puede diferir de la etiqueta de seguridad de mensajes en la 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 STRM o de un ATM.

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

10.3.8 *Técnica del sobre doble*

Es posible dar protección adicional a un mensaje completo, incluidos los parámetros del sobre, especificando que el contenido de un mensaje es, en sí mismo, un mensaje completo, es decir, que se dispone de una técnica de doble sobre.

Se puede recurrir a esta técnica aunque se utilice el argumento del tipo de contenido, que permite especificar que el contenido de un mensaje es un sobre interno. Ese tipo de contenido significa que el contenido es, por sí mismo, un mensaje (sobre y contenido) que el destinatario indicado en el sobre externo debe reexpedir al destinatario indicado en el sobre interno.

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

11 Visión de conjunto

En esta sección se especifica cómo configurar el STM para satisfacer cualquiera de los diversos requisitos de tipo funcional, físico y organizativo.

La sección abarca los siguientes temas:

- a) configuraciones funcionales;
- b) configuraciones físicas;
- c) configuraciones organizativas;
- d) *el STM global*.

12 Configuraciones funcionales

Se especifican en este punto las posibles configuraciones funcionales del STM. La variedad de tales configuraciones está en relación directa con la presencia o ausencia de la guía y con la utilización o no, por parte de un usuario directo, de una MM.

12.1 *Respecto a la guía*

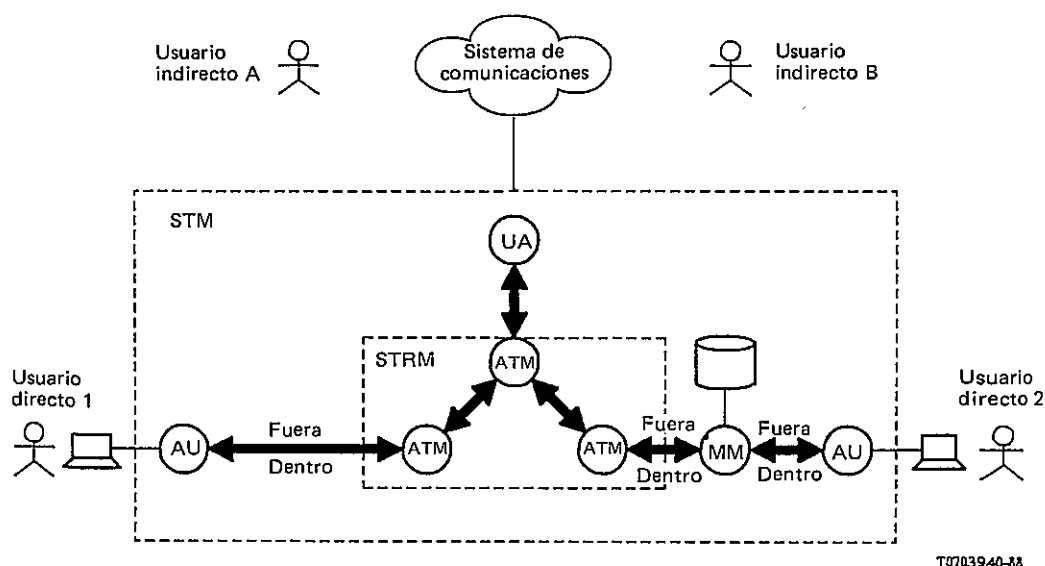
Con respecto a la guía, el STM puede configurarse para un usuario, o colectivo de usuarios (véase por ejemplo, el § 14.1), de dos maneras distintas: con la guía o sin ella. Un usuario sin acceso a la guía carecerá de las capacidades descritas en la sección cinco.

Nota – Es posible que durante un cierto periodo de tiempo exista una guía no plenamente interconectada, sino sólo parcialmente, mientras se elabora la guía (global) que hacen posible las Recomendaciones sobre guías.

12.2 *Respecto a la memoria de mensajes*

Con respecto a la MM, el STM puede configurarse, para un usuario directo particular, de dos maneras distintas: con MM o sin ella. Un usuario sin acceso a una MM no tiene capacidad de almacenar mensajes. En tal circunstancia, dependerá de su AU para el almacenamiento de objetos de información, con una capacidad que será un asunto local.

Las dos configuraciones funcionales identificadas anteriormente, se representan de manera esquemática en la figura 7/X.402, que ilustra además una posible configuración del STRM y su vinculación a otro sistema de comunicaciones a través de un AU. En esta figura, el usuario 2 está equipado con una MM, mientras que el usuario 1 no lo está.



Nota — Aunque los usuarios representados en esta figura son personas, ésta es aplicable con igual vigencia y validez a otras clases de usuarios.

FIGURA 7/X.402
Configuraciones funcionales respecto a la MM

13 Configuraciones físicas

En este punto se especifican las posibles configuraciones físicas del STM, es decir, cómo puede realizarse el STM como un conjunto de sistemas de computadores interconectados. Puesto que el número de configuraciones es ilimitado, los *sistemas de mensajería* se describen a partir de los cuales se construye el STM, y se identifican unas cuantas configuraciones representativas importantes.

13.1 Sistemas de mensajería

A las unidades elementales utilizadas en la construcción física del STM se les denomina *sistemas de mensajería*. Un **sistema de mensajería** es un sistema por computador (posiblemente, aunque no necesariamente, un sistema abierto) que contiene, o realiza, uno o más objetos funcionales.

Los sistemas de mensajería son de los tipos que se representan de manera esquemática en la figura 8/X.402.

En la primera columna del cuadro 8/X.402 se da una relación de los tipos de sistemas de mensajería representados en la figura 8/X.402. Para cada tipo de esa relación, la segunda columna indica las clases de objetos funcionales – AU, MM, ATM y UA – que pueden estar presentes en dicho sistema de mensajería, si su presencia es obligatoria o facultativa y si el sistema de mensajería consta simplemente de uno o posiblemente de múltiples objetos.

El cuadro 8/X.402 está dividido en dos secciones. Los sistemas de mensajería de los tipos de la primera sección prestan servicio a un solo usuario, mientras que los de la segunda pueden prestar servicio a un solo usuario o a varios usuarios.

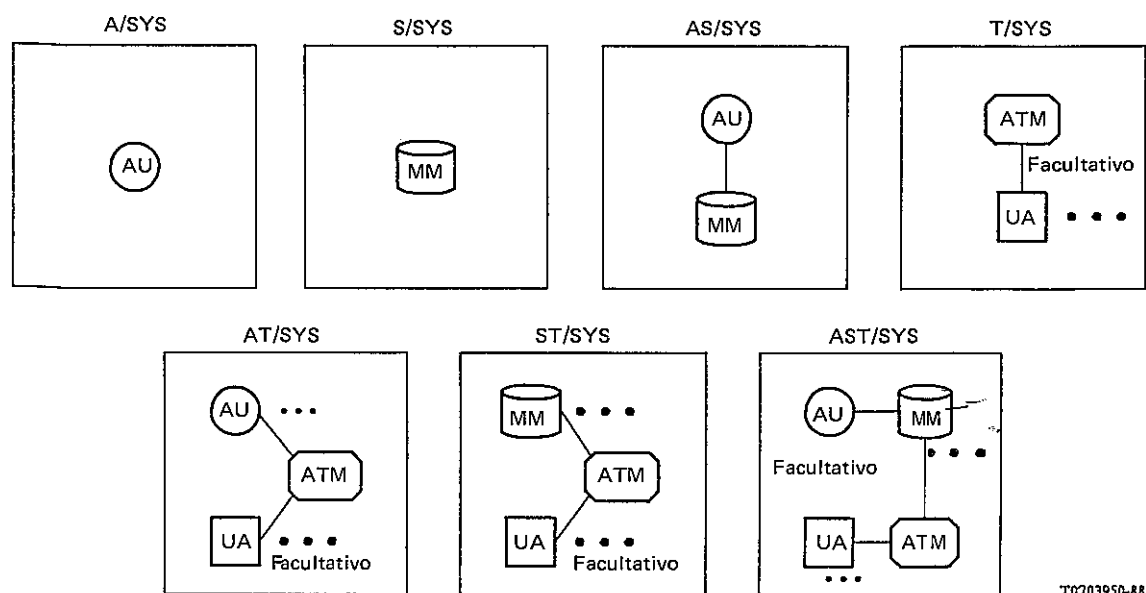
Nota — Para la admisión de tipos de sistemas de mensajería se han tenido en cuenta los siguientes principios fundamentales:

- Una UA y el ATM con el que interactúa se hallan típicamente ubicados en la misma posición, puesto que no se ha normalizado ningún protocolo que gobierne su interacción.
- Un ATM se halla típicamente coubicado con múltiples AU o MM, porque, de los protocolos normalizados, sólo el de transferencia lleva un mensaje simultáneamente a destinatarios múltiples. La entrega en serie de un mensaje a destinatarios múltiples servidos por un sistema de mensajería, tal como exigiría el protocolo de entrega, resultaría ineficaz.
- Nada se consigue ubicando varios ATM en el mismo emplazamiento, en un sistema de mensajería, puesto que un solo ATM presta servicio a múltiples usuarios, y la finalidad de un ATM es transportar objetos

funcionales entre sistemas y no dentro de tales sistemas (con esto no se pretende excluir la posibilidad de que varios procesos relacionados con un ATM coexistan en un único sistema por computador).

- d) La coubicación de una UA con un ATM no afecta al comportamiento del sistema con respecto al resto del STM. Un solo tipo de sistema de mensajería abarca, por tanto, la presencia y la ausencia de la UA.

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



T0703950-88

FIGURA 8/X.402

Tipos de sistemas de mensajería

CUADRO 8/X.402

Sistemas de mensajería

Sistema de mensajería	Objetos funcionales			
	AU	MM	ATM	UA
A/SYS	1	—	—	—
S/SYS	—	1	—	—
AS/SYS	1	1	—	—
T/SYS	—	—	1	[M]
AT/SYS	M	—	1	[M]
ST/SYS	—	M	1	[M]
AST/SYS	M	M	1	[M]

M Múltiple

[...] Facultativo

13.1.1 Sistemas de acceso

Un **sistema de acceso (A/SYS)** contiene un AU, pero no una MM ni un ATM ni una UA.

Un A/SYS se dedica a un único usuario.

13.1.2 *Sistemas de almacenamiento*

Un **sistema de almacenamiento (S/SYS)** contiene una MM, pero no un AU ni un ATM ni una UA.

Un S/SYS se dedica a un único usuario.

13.1.3 *Sistemas de acceso y almacenamiento*

Un **sistema de acceso y almacenamiento (AS/SYS)** contiene un AU, y una MM, pero no un ATM ni una UA.

Un AS/SYS se dedica a un único usuario.

13.1.4 *Sistemas de transferencia*

Un **sistema de transferencia (T/SYS)** contiene un ATM, facultativamente, una o más UA, pero no un AU ni una MM.

Un T/SYS puede prestar servicio a múltiples usuarios.

13.1.5 *Sistemas de acceso y transferencia*

Un **sistema de acceso y transferencia (AT/SYS)** contiene uno o más AU, un ATM y, facultativamente, una o más UA, pero no una MM.

Un AT/SYS puede prestar servicio a múltiples usuarios.

13.1.6 *Sistemas de almacenamiento y transferencia*

Un **sistema de almacenamiento y transferencia (ST/SYS)** contiene una o más MM, un ATM y facultativamente, una o más UA, pero no AU.

Un 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)** contiene uno o más AU, una o más MM, un ATM y facultativamente, una o más UA.

Un AST/SYS puede prestar servicio a múltiples usuarios.

13.2 *Configuraciones representativas*

Los sistemas de mensajería pueden combinarse de diversas maneras para constituir el STM. Las configuraciones físicas posibles son ilimitadas, y por ello no pueden ser enumeradas. De todos modos, en la figura 9/X.402 y en los puntos que siguen, se describen varias configuraciones representativas importantes.

13.2.1 *Totalmente centralizada*

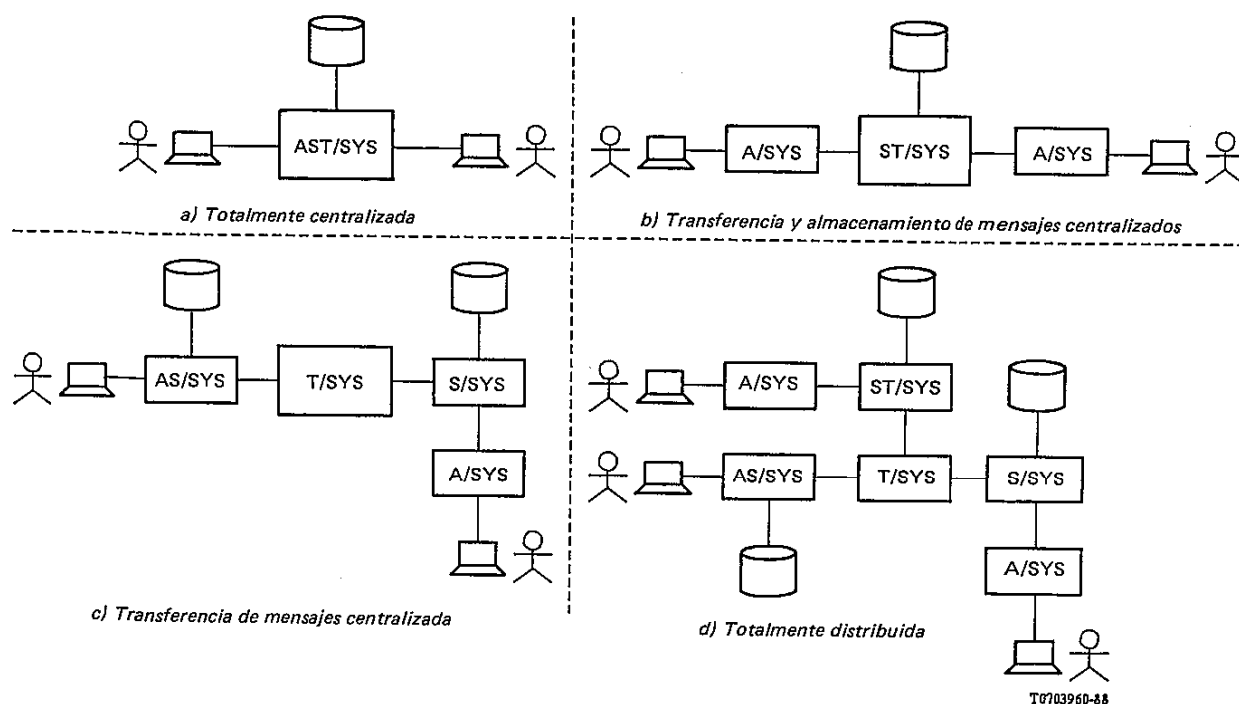
El STM puede estar totalmente centralizado [caso a) de la figura 9/X.402]. Este diseño se realiza mediante un único AST/SYS que contiene objetos funcionales de todas clases y que puede prestar servicio a múltiples usuarios.

13.2.2 *Transferencia y almacenamiento de mensajes centralizados*

El STM puede proporcionar transferencia y almacenamiento de mensajes centralmente, pero con acceso distribuido de los usuarios [caso b) de la figura 9/X.402]. Este diseño se realiza mediante un único ST/SYS y, por cada usuario, un A/SYS.

13.2.3 *Transferencia de mensajes centralizada*

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



Nota 1 – Aunque los usuarios representados en esta figura son personas, ésta es aplicable con igual vigencia y validez a otras clases de usuarios.

Nota 2 – Además de las configuraciones físicas resultantes de los planteamientos «puros» que a continuación se indican, pueden construirse muchas configuraciones de carácter «híbrido».

FIGURA 9/X.402
Configuraciones físicas representativas

13.2.4 Totalmente distribuida

El STM puede proporcionar transferencia de mensajes incluso de manera distribuida [caso d) de la figura 9/X.402]. Este diseño implica múltiples ST/SYS o T/SYS.

14 Configuraciones organizativas

En este punto se especifican las configuraciones organizativas posibles del STM, es decir, cómo puede realizarse el STM en forma de conjuntos de sistemas de mensajería interconectados, pero gestionados independientemente (estando los propios sistemas conectados entre sí). Como el número de configuraciones es ilimitado, se describen los tipos de *dominios de gestión* a partir de los cuales se construye el STM, y se identifican unas cuantas configuraciones representativas importantes.

14.1 Dominios de gestión

A los bloques primarios, utilizados en la construcción de STM, se les denomina *dominios de gestión*. Un **dominio de gestión (DG)** (o **dominio**) es un conjunto de sistemas de mensajería – por lo menos uno, que contenga o realice un ATM – gestionado por una única organización.

Lo anterior no impide que una organización gestione un conjunto de sistemas de mensajería (por ejemplo, un solo A/SYS) que no tiene categoría de DG por falta de un ATM. Ese grupo de sistemas de mensajería, bloque secundario utilizado en la construcción del STM, son de la «incumbencia» de un DG.

Los DG son de varios tipos, cada uno de los cuales se define y describe en los puntos que siguen.

14.1.1 Dominio de gestión de administración

Un **dominio de gestión de administración (DGAD)** comprende varios sistemas de mensajería gestionados por una Administración. La distinción técnica principal entre un DGAD y un DGPR es que el primero se halla por

encima del segundo en los regímenes jerárquicos de direccionamiento (véase el § 18) y encaminamiento (véase el § 19) del STM.

Nota – Un DGAD proporciona tratamiento de mensajes al público.

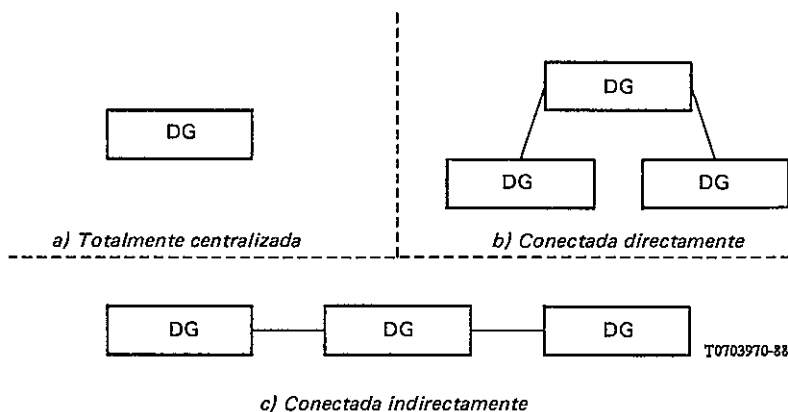
14.1.2 Dominio de gestión privado

Un **dominio de gestión privado (DGPR)** comprende sistemas de mensajería gestionados por una organización distinta de una Administración. La distinción técnica principal entre un DGPR y un DGAD es que el primero se halla por debajo del segundo en los regímenes jerárquicos de direccionamiento (véase el § 18) y encaminamiento (véase el § 19) del STM.

Nota – Un DGPR proporciona tratamiento de mensajes, por ejemplo, a los empleados de una compañía, o a esos empleados en un determinado emplazamiento de la compañía.

14.2 Configuraciones representativas

Los DG pueden combinarse de diversas maneras para constituir el STM. Las configuraciones organizativas posibles son ilimitadas, y por ello no pueden enumerarse. De todos modos, en la figura 10/X.402 y en los puntos que siguen se describen varias configuraciones representativas importantes.



Nota – Además de las configuraciones organizativas resultantes de los planteamientos «puros» que a continuación se indican, pueden construirse muchas otras organizaciones de carácter «híbrido».

FIGURA 10/X.402

Configuraciones organizativas representativas

14.2.1 Totalmente centralizada

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

14.2.2 Conectada directamente

El STM puede ser gestionado por varias organizaciones, estando los sistemas de mensajería de cada una de ellas conectados a los sistemas de mensajería de todas las demás [caso b) de la figura 10/X.402]. Este diseño se realiza mediante múltiples DG interconectados por pares.

14.2.3 Conectada indirectamente

El STM puede ser gestionado por varias organizaciones, actuando los sistemas de mensajería de una como intermediarios entre los sistemas de mensajería de las otras [caso c) de la figura 10/X.402]. Este diseño se realiza mediante múltiples DG uno de los cuales está interconectado con todos los demás.

15 El STM global

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

El STM global abarca, casi con toda seguridad, la gama completa de configuraciones funcionales especificadas en el § 12.

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

La configuración organizativa del STM global es una combinación híbrida de las configuraciones puras especificadas en el § 14, sumamente compleja y con un alto grado de distribución organizativa.

En la figura 11/X.402 se da un ejemplo de posibles interconexiones, que no pretende identificar todas las configuraciones posibles. Tal como se indica en la figura 11/X.402 los DGAD juegan un papel central en el STM global. Mediante su interconexión internacional se constituye la columna vertebral de la transferencia de mensajes. Interconectándolos a nivel nacional, y dependiendo de cuáles sean los reglamentos nacionales, pueden también proporcionar entramados básicos, a ese mismo nivel, unidos al entramado internacional. Los DGAD sirven también como primera autoridad de denominación, en la *asignación de direcciones O/D* a usuarios y LD.

Los DGPR desempeñan un contenido más bien periférico en el STM global, estando conectados al eje central de los DGAD, que actúa de intermediario entre ellos.

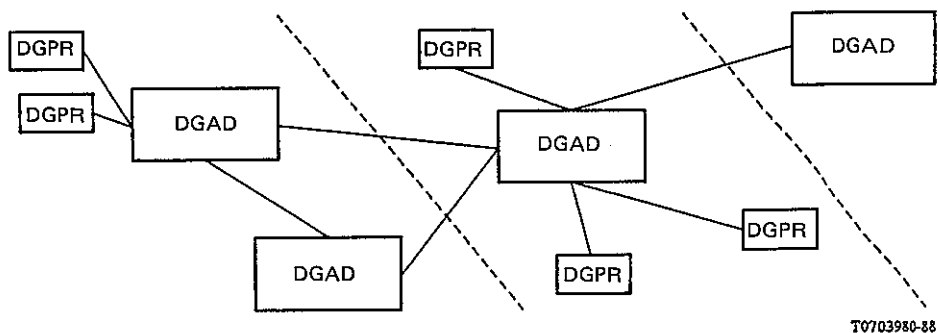


FIGURA 11/X.402

El STM global

SECCIÓN 4 – DENOMINACIÓN, DIRECCIONAMIENTO Y ENCAMINAMIENTO

16 Vision de conjunto

En esta sección se describen la denominación y el direccionamiento de usuarios y LD, y el encaminamiento hacia ellos de objetos de información.

La sección comprende los siguientes temas:

- a) denominación;
- b) direccionamiento;
- c) encaminamiento.

17 Denominación

En este punto se especifica cómo se denomina a los usuarios y LD a efectos de tratamiento de mensajes en general y transferencia de mensajes en particular. Se definen los *nombres O/D* y se describe el papel que desempeñan en ellos los nombres de guía.

Cuando un AU o una MM depositan un mensaje o una sonda, identifican al STRM los destinatarios potenciales. Cuando el STRM entrega un mensaje, identifica el originador a cada AU o MM del destinatario potencial. Los *nombres O/D* son las estructuras de datos por medio de las cuales se realiza esa identificación.

17.1 Nombres de guía

Un nombre de guía es un componente de un *nombre O/D*. El nombre de guía identifica un objeto a la guía. Presentando ese nombre a la guía, el STM puede acceder la inscripción en la guía de un usuario o una LD. El STRM obtiene de esa inscripción, por ejemplo, la *dirección O/D* del usuario o de la LD.

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

Nota 1 – Muchos usuarios y LD carecerán de nombre de guía mientras no se generalice la difusión de ésta, como elemento auxiliar del STM. Gran número de usuarios indirectos (por ejemplo, patrones postales) no tendrán tales nombres mientras no se disponga ampliamente de la guía, como un adjunto a otros sistemas de comunicación.

Nota 2 – A los usuarios y a las LD se les puede asignar nombres de guía incluso antes de que se ponga en marcha una guía interconectada y distribuida, preestableciendo las autoridades de denominación, de las que dependerá la guía en su momento.

Nota 3 – El nombre de guía típico le resulta más cómodo y estable al usuario que la *dirección O/D* típica porque la segunda está expresada necesariamente desde el punto de vista de la estructura organizativa o física del STM, mientras que el primero no lo está. Se pretende por ello que, con el tiempo, los nombres de guía se conviertan necesariamente en el principal medio de identificación de los usuarios y las LD fuera del STM (es decir, por otros usuarios), y que el empleo de las *direcciones O/D* se limite en gran medida al STRM (es decir, por los ATM).

17.2 Nombres O/D

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

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

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

En entrega, el STRM incluye una *dirección O/D* y posiblemente un nombre de guía en cada nombre O/D que suministra al destinatario de un mensaje o al originador de un mensaje o sonda objeto de un informe. El nombre de guía se incluye si el originador lo ha suministrado, o si se identificó como miembro de una LD ampliada.

Nota – La redirección o la ampliación de LD pueden dar lugar a que el STRM lleve a un AU o a una MM en entrega, nombres O/D que el AU o la MM no suministraron en depósito directo.

18 Direccionamiento

En este punto se especifica la manera de direccionar a usuarios y LD. Se definen las *direcciones O/D*, se describe la estructura de las *listas de atributos* a partir de las que se elaboran, se examinan los conjuntos de caracteres con los que se componen los *atributos* individuales, se dan reglas para determinar si dos *listas de atributos* son equivalentes y para la inclusión de *atributos* condicionales en tales listas y se definen los *atributos normalizados* que pueden figurar en ellas.

Para transportar un mensaje, una sonda o un informe a un usuario, o para ampliar una LD especificada como destinatario potencial de un mensaje o una sonda, el STRM debe localizar el usuario o la LD relativos a sus propias estructuras física y organizativa. Las *direcciones O/D* son las estructuras de datos mediante las cuales se realizan todas estas localizaciones.

18.1 *Lista de atributos*

Las *direcciones O/D* de usuarios y LD son listas de atributos. Una **lista de atributos** es un conjunto ordenado de *atributos*.

Un **atributo** es un elemento de información que describe a un usuario o LD y que puede también ubicarlo en relación con la estructura física y organizativa del STM (o la red inherente al mismo).

Un atributo consta de las siguientes partes:

- a) **tipo de atributo (o tipo)**: Identificador que indica una clase de información (por ejemplo, nombres personales).
- b) **valor de atributo (o valor)**: Ejemplo de la clase de información indicada por el tipo de atributo (por ejemplo, un nombre personal).

Los atributos son de las dos clases siguientes:

- a) **atributo normalizado**: Atributo cuyo tipo está vinculado a una clase de información por esta Recomendación.

El valor de cada atributo normalizado, excepto el del *tipo-terminal*, es una cadena o bien un grupo de cadenas.

- b) **atributo definido por el dominio**: Atributo cuyo tipo está vinculado a una clase de información por un DG.

Tanto el tipo como el valor de cada atributo definido por el dominio son cadenas o grupos de cadenas.

Nota – El uso generalizado de atributos normalizados genera direcciones O/D más uniformes y por tanto más cómodas para el usuario. No obstante, es de prever que no todos los DG serán capaces de emplear tales atributos inmediatamente. La finalidad de los atributos definidos por el dominio es permitir a un DG que retenga durante cierto tiempo los convenios primitivos de direccionamiento existentes. Se pretende sin embargo, que todos los DG tiendan al empleo de atributos normalizados, y que los atributos definidos por el dominio se utilicen sólo con carácter provisional.

18.2 *Juegos de caracteres*

Los valores de atributos normalizados y los tipos y valores de atributos definidos por el dominio se elaboran a partir de cadenas numéricas, imprimibles y teletex, según los siguientes criterios:

- a) El tipo o valor de un determinado atributo definido por el dominio puede ser una cadena imprimible, una cadena teletex o ambas. Se elegirá lo mismo para el tipo y para el valor.
- b) Las clases de cadenas con las que pueden elaborarse valores de atributos normalizados y la manera de elaborarlos (por ejemplo, como una sola cadena o varias) difiere de un atributo a otro (véase el § 18.3).

El valor de un atributo consta de cadenas de una de las siguientes variedades, dependiendo de su tipo: numérico sólo, imprimible sólo, numérico e imprimible e imprimible y teletex. En relación con esto, las siguientes reglas gobiernan cada caso de comunicación:

- a) Donde se permitan cadenas tanto numéricas como imprimibles, podrán suministrarse indistintamente cadenas de una u otra variedad (pero no de ambas).
- b) Donde se permitan cadenas tanto imprimibles como teletex, podrán suministrarse cadenas de una u otra variedad, o de ambas, pero las cadenas imprimibles se suministrarán lo menos posible cuando se transporten los atributos internacionalmente. Si se suministran cadenas tanto imprimibles como teletex, ambas deberán transportar la misma información, de tal modo que en la recepción pueda ignorarse una de las dos sin pérdida de seguridad.

La longitud de cada cadena y de cada secuencia de cadenas en un atributo se limitará tal como se indica en la especificación más detallada de atributos (por ejemplo, NSA.1) de la Recomendación X.411.

Nota 1 – Se permiten las cadenas teletex en valores de atributos para facilitar la inclusión, por ejemplo, de caracteres acentuados, utilizados normalmente en muchos países.

Nota 2 – No todos los dispositivos de entrada/salida permiten la introducción y visualización, por ejemplo, de caracteres acentuados. Las cadenas imprimibles son necesarias, a nivel internacional, para asegurar que esas limitaciones de los dispositivos no impiden la comunicación.

18.3 Atributo normalizados

En la primera columna del cuadro 9/X.402 figura la lista de tipos de atributos normalizados. Para cada tipo enumerado se indican en la segunda columna los conjuntos de caracteres - numéricos, imprimibles y teletex - con los que está permitido elaborar valores de atributos.

El cuadro 9/X.402 tiene tres secciones. Los tipos de atributos de la primera son de naturaleza general, los de la segunda están relacionados con el *encaminamiento* a un SEF y los de la tercera, con el *direccionamiento dentro de* un SEF.

CUADRO 9/X.402

Atributos normalizados

Tipo de atributo normalizado	Juego de caracteres		
	NUM	IMP	TTX
<i>General</i>			
Nombre-dominio-administración	x	x	—
Nombre-común	—	x	x
Nombre-país	x	x	—
Dirección-red	x ^{a)}	—	—
Identificador-usuario-numérico	x	—	—
Nombre-organización	—	x	x
Nombre-unidades-organización	—	x	x
Nombre-personal	—	x	x
Nombre-dominio-privado	x	x	—
Identificador-terminal	—	x	—
Tipo-terminal	—	—	—
<i>Encaminamiento postal</i>			
Nombre-servicio-entrega-física	—	x	—
Nombre-país-entrega-física	x	x	—
Código-postal	x	x	—
<i>Direccionamiento postal</i>			
Componentes-ampliación-dirección-O/D postal	—	x	x
Componentes-ampliación-entrega-física	—	x	x
Atributos-postales-locales	—	x	x
Nombre-oficina-entrega-física	—	x	x
Número-oficina-entrega-física	—	x	x
Nombre-organización-entrega-física	—	x	x
Nombre-personal-entrega-física	—	x	x
Dirección-apartado-correos	—	x	x
Dirección-lista-correos	—	x	x
Dirección-calle	—	x	x
Dirección-postal-no-formatizada	—	x	x
Nombre-postal-exclusivo	—	x	x

NUM Numérico

IMP Imprimible

TTX Teletex

x Permitido

^{a)} En determinadas circunstancias, una secuencia de cadenas de octetos

Los tipos de atributos normalizados, resumidos en el cuadro 9/X.402, se definen y describen individualmente en los puntos que siguen.

18.3.1 *Nombre-dominio-administración*

Nombre-dominio-administración es un atributo normalizado que identifica un DGAD relativo al país indicado por un nombre-país.

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

Nota - El valor de atributo que consta de un único espacio (« ») se reservará para los siguientes fines. Si lo permite el país indicado por el atributo de nombre-país, un único espacio designará cualquiera (es decir, todos) los DGAD dentro del país. Esto afecta tanto a la identificación de usuarios dentro del país como al encaminamiento de mensajes, sondas e informaciones hacia y entre los DGAD de ese país. En relación con lo primero, es preciso que las direcciones O/D de los usuarios dentro del país se elijan de tal modo que se asegure su carácter inequívoco, incluso en ausencia de los nombres verdaderos de los DGAD de usuarios. En relación con lo segundo, ello permite que los DGPR de dentro y los DGAD de fuera del país encaminen mensajes, sondas e informes a cualquiera de DGAD de dentro del país indiscriminadamente, y exige que estos últimos se interconecten de manera tal que los mensajes, las sondas y los informes sean llevados a sus destinos.

18.3.2 *Nombre-común*

Nombre común es un atributo normalizado que identifica a una LD o a un usuario relativo a la entidad indicada por otro atributo (por ejemplo, un nombre-organización).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas. Sea imprimible o teletex, la cadena se elige de entre un conjunto de tales cadenas administrado para este fin (y quizá para otros) por la entidad aludida anteriormente.

Nota – Entre otras muchas posibilidades, un nombre-común podría identificar un cometido organizativo (por ejemplo, «Director de mercadotecnia»).

18.3.3 *Nombre-país*

Nombre-país es un atributo normalizado que identifica a un país.

El valor de este atributo es una cadena numérica que da uno de los números asignados al país por la Recomendación X.121, o una cadena imprimible que da el par de caracteres asignados al país por la norma ISO 3166.

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

Componentes-ampliación-dirección-O/D-postal es un atributo normalizado que proporciona, en una dirección postal, información adicional necesaria para identificar al destinatario (por ejemplo, una unidad organizativa).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.5 *Componentes-ampliación-dirección-entrega-física*

Componentes-ampliación-dirección-entrega-física es un atributo normalizado que especifica, en una dirección postal, información adicional necesaria para identificar el punto exacto de entrega (por ejemplo, número de piso y despacho en un gran edificio).

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.6 *Atributos-postales-locales*

Atributos-postales-locales es un atributo normalizado que especifica el lugar de distribución, distinto del indicado por un atributo de nombre-oficina-entrega-física (por ejemplo, una zona geográfica) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.7 *Dirección-red*

Dirección-red es un atributo normalizado que da la dirección de red de un terminal.

Este atributo tiene algunos de los siguientes valores:

- a) una cadena numérica de conformidad con la Recomendación X.121;
- b) dos cadenas numéricas tal como se especifican en las Recomendaciones E.163 y E.164;

- c) una dirección de punto de acceso al servicio de presentación (PASP).

Nota – Entre las cadenas admitidas por la Recomendación X.121 se encuentra un número télex precedido por la cifra de escape télex (8).

18.3.8 *Identificador-usuario-numérico*

Identificador-usuario-numérico es un atributo normalizado que identifica numéricamente a un usuario relativo al DGAD, indicado por un nombre-dominio-administración.

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

18.3.9 *Nombre-organización*

Nombre-organización es un atributo normalizado que identifica una organización. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre-organización identifique una única entidad dentro del país) o referirse al DG indentificado por un nombre-dominio-privado, por un nombre-dominio-administración, o por ambos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas. Sea imprimible o teletex, la cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por el país o el DG aludido anteriormente.

Nota – En los países en que cada atributo nombre-organización debe corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos atributos.

18.3.10 *Nombres-unidades-organizativas*

Nombre-unidades-organizativas es un atributo normalizado que identifica una o más unidades (por ejemplo, divisiones o departamentos) de la organización indicada por un nombre-organización, siendo cada unidad, excepto la primera, una subunidad de las unidades cuyos nombres le preceden en el atributo.

El valor de este atributo es una secuencia ordenada de cadenas imprimibles, una secuencia ordenada de cadenas teletex o ambas. Sea imprimible o teletex, cada cadena se elige de entre un conjunto de tales cadenas, administrado para este fin (y quizá para otros) por la organización (o unidad abarcadora) aludida anteriormente.

18.3.11 *Nombre-servicio-entrega-física*

Nombre-servicio-entrega-física es un atributo normalizado que identifica a un servicio de entrega física relativo al DGAD indicado por un nombre-dominio-administración.

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

18.3.12 *Nombre-personal*

Nombre-personal es un atributo normalizado que identifica una persona con respecto a la entidad indicada por otro atributo (por ejemplo, un nombre-organización).

El valor de este atributo comprende los siguientes cuatro elementos de información, de las que la primera es obligatoria y las otras facultativas:

- a) el apellido de la persona;
- b) el nombre de la persona;
- c) las iniciales de todos sus apelativos, excepto la del apellido;
- d) su generación (por ejemplo «hijo»).

La información anterior se proporciona en forma de cadenas imprimibles, cadenas teletex o ambas.

18.3.13 *Nombre-país-entrega-física*

Nombre-país-entrega-física es un atributo normalizado que identifica el país en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo está sometido a las mismas limitaciones que el de un nombre-país.

18.3.14 *Nombre-oficina-entrega-física*

Nombre-oficina-entrega-física es un atributo normalizado que identifica la ciudad, el pueblo, etc. en el que se halla la oficina postal a través de la cual un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.15 *Número-oficina-entrega-física*

Número-oficina-entrega-física es un atributo normalizado que distingue entre varias oficinas postales indicadas por un único nombre-oficina-entrega-física.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.16 *Nombre-organización-entrega-física*

Nombre-organización-entrega-física es un atributo normalizado que identifica una organización patrón postal.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.17 *Nombre-personal-entrega-física*

Nombre-personal-entrega-física es un atributo normalizado que identifica un patrón postal.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.18 *Dirección-apartado-correos*

Dirección-apartado-correos es un atributo normalizado que especifica el número del casillero de la oficina postal en el que un usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas, a elegir entre el conjunto de tales cadenas asignadas para este fin por la oficina postal indicada por un atributo de nombre-oficina-entrega-física.

18.3.19 *Código-postal*

Código-postal es un atributo normalizado que especifica el código postal para la zona geográfica en la que el usuario recibe la entrega de los mensajes físicos.

El valor de este atributo es una cadena imprimible o numérica, elegida de entre el conjunto de tales cadenas, mantenido y normalizado para este fin por la Administración del país identificado por un atributo de nombre-país-entrega-física.

18.3.20 *Dirección-lista-correos*

Dirección-lista-correos es un atributo normalizado que identifica el código que un usuario da a la oficina postal para que acopie los mensajes físicos que se le deben entregar.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas, elegida de entre el conjunto de tales cadenas asignadas a este fin por la oficina postal indicada por un atributo de nombre-oficina-entrega-física.

18.3.21 *Nombre-dominio-privado*

Nombre-dominio-privado es un atributo normalizado que identifica un DGPR relativo al DGAD. Como asunto nacional, esta identificación puede referirse al país indicado por un nombre-país (de tal modo que cada nombre de DGPR identifique una única entidad dentro del país) o referirse al DGAD identificado por un nombre-dominio-administración.

El valor de este atributo es una cadena numérica o imprimible elegida de entre un conjunto de tales cadenas administradas para este fin por el país o el DGAD aludido anteriormente.

Nota – En los países en que cada nombre de DGPR debe corresponder a una entidad única a escala nacional, se precisa una autoridad nacional para el registro de dichos nombres.

18.3.22 *Dirección-calle*

Dirección-calle es un atributo normalizado que especifica la dirección de calle [por ejemplo, número de la casa y nombre de la calle y tipo (por ejemplo, «camino»)] en la que el usuario recibe la entrega de mensajes físicos.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.3.23 *Identificador-terminal*

Identificador-terminal es un atributo normalizado que da el identificador terminal de un terminal (por ejemplo, un distintivo télex o un identificador de terminal de teletex).

El valor de este atributo es una cadena imprimible.

18.3.24 *Tipo-terminal*

Tipo-terminal es un atributo normalizado que da el tipo de un terminal.

El valor de este atributo es uno cualquiera de los siguientes: *télex*, *teletex*, *facsimilar G3*, *facsimilar G4*, *terminal AI5* o *videotex*.

18.3.25 *Dirección-postal-no-formatizada*

Dirección-postal-no-formatizada es un atributo normalizado que especifica una dirección postal de usuario de forma libre.

El valor de este atributo es una secuencia de cadenas imprimibles, representando cada una una línea de texto, o bien una única cadena teletex, estando las líneas separadas tal como se especifica para tales cadenas, o bien ambas.

18.3.26 *Nombre-postal-exclusivo*

Nombre-postal-exclusivo es un atributo normalizado que identifica el punto de entrega, distinto del indicado por un dirección-calle, un dirección-apartado-correos o un dirección-lista-correos, (por ejemplo, un edificio o un caserío) de los mensajes físicos de un usuario.

El valor de este atributo es una cadena imprimible, una cadena teletex o ambas.

18.4 *Equivalencia de listas de atributos*

Varias direcciones O/D, y por tanto varias listas de atributos, pueden indicar el mismo usuario o la misma LD. Esta multiplicidad de direcciones O/D se debe en parte (pero sólo en parte) a las siguientes reglas de equivalencia de listas de atributos:

- a) El orden relativo de atributos normalizados es intrascendente.
- b) Cuando el valor de un atributo normalizado pueda ser una cadena numérica o una cadena imprimible equivalente, la elección entre ellas se considerará intrascendente.

Nota – Esta regla se aplica incluso al atributo normalizado nombre-país cuando la elección entre las formas Rec. X.121 o ISO 3166 se considere irrelevante. Cuando en la Rec. X.121 se asignen a un país más de un número, la relevancia del número utilizado no ha sido normalizada en esta Recomendación.

- c) Cuando el valor de un atributo normalizado pueda ser una cadena imprimible, una cadena teletex equivalente o ambas, la elección entre las tres posibilidades se considerará intrascendente.
- d) Cuando el valor de un atributo normalizado puede contener letras, los tipos de esas letras se considerarán intrascendentes.
- e) En un tipo o valor de atributo definido por el dominio o en un valor de atributo normalizado, todos los espacios precedentes, todos los espacios subsiguientes y todos los intermedios consecutivos menos uno, se considerarán intrascendentes.

Nota 1 – Un DG puede imponer reglas de equivalencia adicionales a los atributos que asigna a sus propios usuarios y LD. Podría definir, por ejemplo, reglas relativas a los caracteres de puntuación en los valores de atributos, el tipo de las letras de tales atributos o el orden relativo de los atributos definidos por el dominio.

Nota 2 – En el plano nacional, los DG pueden imponer reglas de equivalencia adicionales respecto a los atributos normalizados cuyos valores se dan como cadenas teletex, en particular las reglas para la deducción de las cadenas imprimibles equivalentes.

18.5 *Formas de direcciones O/D*

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

Una dirección O/D puede tomar alguna de las formas que, de manera resumida, se indican en el cuadro 10/X.402. En la primera columna del cuadro se da una relación de los atributos disponibles para la elaboración de direcciones O/D. Para cada forma de dirección O/D, la segunda columna indica los atributos que pueden aparecer en estas direcciones O/D y sus grados (véase también el § 18.6).

El cuadro 10/X.402 tiene cuatro secciones. Los tipos de atributos de la primera son los de carácter general, los de la segunda y la tercera son específicos de la entrega física. La cuarta sección comprende los atributos definidos por el dominio.

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

18.5.1 *Dirección O/D nemotécnica*

Dirección O/D nemotécnica es una dirección que identifica nemotécnicamente a un usuario o una LD. Identifica a un DGAD y a un usuario o una LD relativos a éste.

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

- a) un nombre-país y un nombre-dominio-administración, que juntos identifican a un DGAD;
- b) un nombre-dominio-privado, un nombre-organización, un nombres-unidades-organizativas, un nombre-personal o nombre-común o una combinación de los anteriores; y facultativamente uno o más atributos definidos por el dominio, que, conjuntamente, identifican a un usuario o una LD relativos al DGAD mencionado en a).

18.5.2 *Dirección O/D numérica*

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

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

- a) un nombre-país y un nombre-dominio-administración, que conjuntamente identifican a un DGAD;
- b) un identificador-usuario-numérico y, de manera condicional, un nombre-dominio-privado, que juntos identifican al usuario relativo al DGAD mencionado en a);
- c) de manera condicional, uno o más atributos definidos por el dominio que proporcionan información adicional a la de identificación del usuario.

18.5.3 *Dirección O/D postal*

Dirección O/D postal es una dirección que identifica a un usuario por su dirección postal. Identifica al servicio de entrega física a través del cual ha de accederse al usuario y da la dirección postal del mismo.

Se distinguen las siguientes clases de direcciones O/D postales:

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

CUADRO 10/X.402

Formas de direcciones O/D

Tipos de atributos	Formas de direcciones O/D				
	NEM	NUM	Postal		TERM
			F	NF	
<i>General</i>					
Nombre-dominio-administración	O	O	O	O	C
Nombre-común	C	—	—	—	—
Nombre-país	O	O	O	O	C
Dirección-red	—	—	—	—	O
Identificador-usuario-numérico	—	O	—	—	—
Nombre-organización	C	—	—	—	—
Nombre-unidades-organizativas	C	—	—	—	—
Nombre-personal	C	—	—	—	—
Nombre-dominio-privado	C	C	C	C	C
Identificador	—	—	—	—	C
Tipo-terminal	—	—	—	—	C
<i>Encaminamiento postal</i>					
Nombre-servicio-entrega-física	—	—	C	C	—
Nombre-país-entrega-física	—	—	O	O	—
Código-postal	—	—	O	O	—
<i>Direccionamiento postal</i>					
Componentes-ampliación-dirección-O/D postal	—	—	C	—	—
Componentes-ampliación-entrega-física	—	—	C	—	—
Atributos-postales-locales	—	—	C	—	—
Nombre-oficina-entrega-física	—	—	C	—	—
Número-oficina-entrega-física	—	—	C	—	—
Nombre-organización-entrega-física	—	—	C	—	—
Nombre-personal-entrega-física	—	—	C	—	—
Dirección-apartado-correos	—	—	C	—	—
Dirección-lista-correos	—	—	C	—	—
Dirección-calle	—	—	C	—	—
Dirección-postal-no-formatizada	—	—	—	O	—
Nombre-postal-exclusivo	—	—	C	—	—
<i>Definido por el dominio</i>					
Definido por el dominio (uno o más)	C	C	—	—	C

NEM	Nemotécnica	NF	No formatizada
NUM	Númerica	O	Obligatoria
TERM	Terminal	C	Condicional
F	Formatizada		

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

- a) un nombre-país y un nombre-país-administración, que juntos identifican a un DGAD;
- b) de manera condicional, un nombre-dominio-privado, un nombre-servicio-entrega-física o ambos, que juntos identifican al servicio de entrega física mediante el cual se accede al usuario;
- c) un nombre-país-entrega-física y un código-postal que juntos identifican la zona geográfica en la que el usuario recibe la entrega de mensajes físicos.

Una dirección O/D postal formatizada comprende, además, uno de cada uno de los atributos de direccionamiento postal (véase el cuadro 9/X.402) excepto el de dirección-postal-no-formatizada, que necesita el SEF para identificar el patrón postal.

Una dirección O/D postal no formatizada incluye, adicionalmente, un atributo de dirección-postal-no-formatizada.

Nota – El número total de caracteres de los valores de todos los atributos, excepto nombre-país, nombre-dominio-administración y nombre-servicio-entrega-física, en una dirección O/D postal, deberá ser lo bastante reducido para permitir su reproducción en 6 líneas de 30 caracteres, que es el tamaño de una ventanilla de sobre típica. El algoritmo de reproducción es específico de la UAEF, pero es probable que incluya delimitadores de inserción (por ejemplo, espacios) entre algunos de los valores de atributos.

18.5.4 Dirección O/D terminal

Dirección O/D terminal es una dirección que identifica un usuario mediante el número de red y, si es preciso, el tipo de su terminal. También puede identificar el DGAD a través del cual se accede a ese terminal. En el caso de un terminal telemático, da la dirección de red del terminal y, posiblemente, su identificador y tipo de terminal. En el caso de un terminal télex, da su número de télex.

Una dirección O/D terminal consta de los siguientes atributos:

- a) una dirección-red;
- b) de manera condicional, un identificador-terminal;
- c) de manera condicional, un tipo-terminal;
- d) de manera condicional, un nombre-país y un nombre-dominio-administración que juntos identifican un DGAD;
- e) de manera condicional, un nombre-dominio-privado y, condicionalmente asimismo, uno o más atributos definidos por el dominio, todos los cuales proporcionan información adicional a la que identifica al usuario.

Los atributos de nombre-dominio-privado y definido por el dominio sólo estarán presentes si también lo están los de nombre-dominio-administración y nombre-país.

18.6 Atributos condicionales

La presencia o ausencia en una dirección O/D particular, de los atributos señalados como condicionales en el cuadro 10/X.402, se determina según los criterios que a continuación se exponen.

Si se accede a un usuario o LD a través de un DGPR, los atributos utilizados para encaminar mensajes al DGPR están presentes en la dirección O/D, a discreción del DGAD indicado por los atributos nombre-país y nombre-dominio-administración de la dirección O/D y de acuerdo con las reglas establecidas por él. El DGAD no impone más limitaciones a los atributos de la dirección O/D. Si no se accede a un usuario a través de un DGPR, todos los atributos condicionales, excepto los específicos de las direcciones O/D postales, figuran en una dirección O/D a discreción del DGAD indicado por los atributos nombre-país y nombre-dominio-administración y de acuerdo con las reglas establecidas por él.

Todos los atributos condicionales específicos de las direcciones O/D postales están presentes o ausentes en tales direcciones O/D, de modo que se satisfagan las exigencias de direccionamiento postal de los usuarios a los que identifican.

19 Encaminamiento

Para transportar un mensaje, sonda o informe a un usuario o al punto de ampliación de una LD, un ATM debe, no sólo localizar el usuario o la LD (es decir obtener su dirección O/D), sino también seleccionar un encaminamiento hacia esa ubicación.

El encaminamiento externo es un proceso incremental y sólo vagamente normalizado. A continuación se sugieren algunos principios para el encaminamiento externo. El interno queda fuera del alcance de esta Recomendación.

Estos principios son ilustrativos, y no son definitivos.

- a) En un STM que conste de un único DG, la cuestión del encaminamiento, naturalmente, no se plantea.
- b) Un DGPR puede estar conectado a un único DGAD. Cuando esto ocurre, el encaminamiento implica necesariamente al DGAD.
- c) Un DGAD puede estar conectado a múltiples DGPR. Si este es el caso, el encaminamiento puede basarse en atributos de dirección O/D condicionales, incluyendo el de nombre-dominio-privado, pero sin limitarse a él.
- d) Un DG puede estar conectado directamente a algunos otros DG, pero no a todos. Cuando la dirección O/D identifica a un DG con el que no existe conexión directa, el encaminamiento se puede basar en *acuerdos bilaterales* con los DG con los que sí existen conexiones directas, y en otras reglas locales.
- e) Cuando el DG está conectado directamente al DG identificado por la dirección O/D, el objeto es encaminado, por sistema, directamente a ese DG.
- f) Por *acuerdo bilateral*, un DG podría encaminar un objeto a otro DG a efectos de, por ejemplo, conversión.
- g) Un DG puede encaminar a una dirección O/D mal formada siempre que, naturalmente, contenga por lo menos los atributos requeridos para ello.

Nota – Los acuerdos bilaterales y las reglas locales a que se ha aludido anteriormente, quedan fuera del alcance de esta Recomendación, y pueden estar basados en consideraciones de tipo técnico, político o económico, o de otra clase.

SECCIÓN 5 – USO DE LA GUÍA

20 Visión de conjunto

En esta sección se describen los usos que el STM puede hacer de la guía, cuando se dispone de ella. Si el STM no dispone de guía, la manera según la cual realiza las mismas tareas, si es que las realiza, es un asunto local.

La sección comprende los siguientes temas:

- a) autenticación;
- b) resolución de nombres;
- c) ampliación de LD;
- d) evaluación de capacidades.

21 Autenticación

Un objeto funcional puede efectuar la autenticación utilizando información almacenada en la guía.

22 Resolución de nombres

Un objeto funcional puede llevar a cabo la resolución de nombres utilizando la guía.

Un objeto que posee el nombre de guía de un usuario o de una LD y cuya dirección o direcciones O/D desea obtener, presenta ese nombre a la guía y pide los siguientes atributos de la inscripción en la guía del objeto:

- a) *Direcciones O/D del STM;*
- b) *Métodos de entrega preferidos del STM.*

Para hacerlo de manera satisfactoria, el objeto debe primero autenticarse él mismo a la guía, y tener derechos de acceso a la información solicitada.

23 Ampliación de LD

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

Para obtener los miembros de una LD cuyo nombre de guía posee, el objeto presenta ese nombre a la guía y pide los siguientes atributos de la inscripción en la guía del objeto:

- a) *miembros de LD del STM;*
- b) *permisos de depósito de LD del STM;*
- c) *métodos de entrega preferidos del STM.*

Para hacerlo de manera satisfactoria, el ATM debe primero autenticarse él mismo a la guía, y tener derechos de acceso a la información solicitada.

24 Evaluación de capacidades

Un objeto funcional puede evaluar las capacidades de un usuario o LD utilizando la guía.

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

- a) *longitud de contenido entregable del STM;*
- b) *tipos de contenido entregables del STM;*
- c) *TIC entregables del STM*
- d) *métodos de entrega preferidos del STM.*

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

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

Para evaluar determinada capacidad de un usuario o MM cuyo nombre de guía posee, el objeto presenta ese nombre a la guía y pide los atributos asociados a esa capacidad, que figuran en la inscripción en la guía del objeto.

Para hacerlo de manera satisfactoria, el ATM debe primero autenticarse él mismo a la guía y tener derechos de acceso a la información solicitada.

SECCIÓN 6 – REALIZACIÓN POR ISA

25 Visión de conjunto

En esta sección se describe cómo se realiza el STM por medio de la ISA.

La sección comprende los siguientes temas:

- a) elementos de servicio de aplicación;
- b) contextos de aplicación.

26 Elementos de servicio de aplicación

En este punto se identifican los elementos de servicio de aplicación (ESA) que figuran en la realización mediante ISA del tratamiento de mensajes.

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

Nota – El STM depende no sólo de los ESA examinados, sino también del elemento de servicio de acceso a la guía, definido en la Recomendación X.519. Sin embargo, como este ESA no figura en los CA para tratamiento de mensajes (véase la Recomendación X.419), no se analiza aquí.

26.1 El concepto de ESA

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

A la relación entre dos EA en sistemas abiertos diferentes se le llama asociación de aplicación. Los ESA de un sistema abierto se comunican con sus ESA pares del otro a través de una conexión de presentación entre ellos. Esa comunicación es la que crea y mantiene la relación inherente a la asociación de aplicación. Para que varios ESA se combinen de manera satisfactoria en una única EA, deben estar diseñados de manera que coordinen su utilización de la asociación de aplicación.

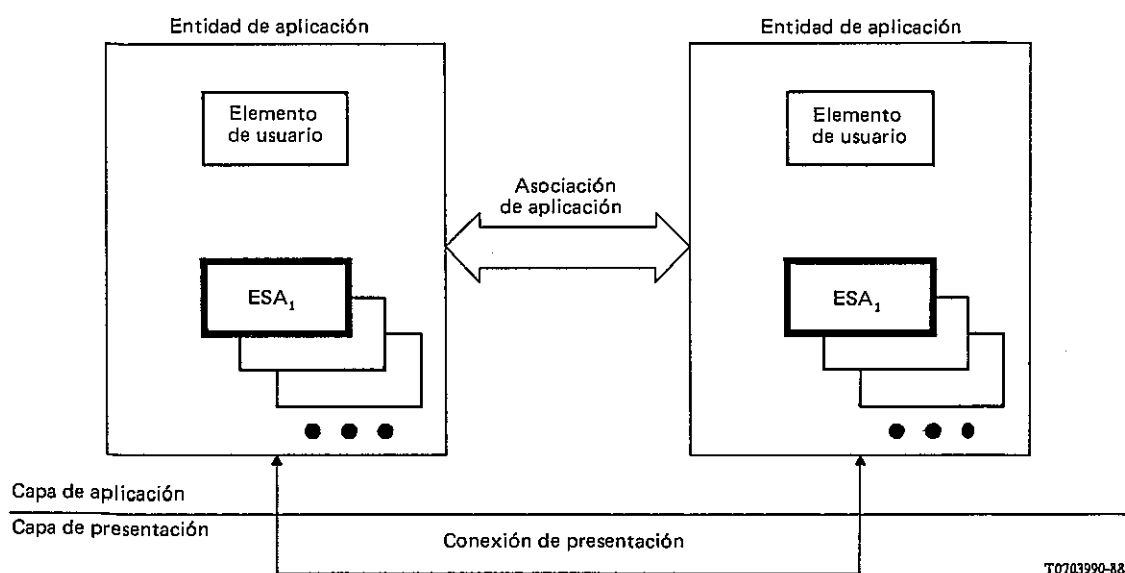


FIGURA 12/X.402

El concepto de ESA

Un ESA desempeña el papel, en gran medida mecánico, de trasladar las peticiones formuladas por su EU, y las respuestas, a y desde la forma dictada por el protocolo de aplicación que gobierna la interacción del ESA con su ESA par del sistema abierto al que la asociación le conecta. El ESA efectúa un servicio, o una parte del mismo, abstracto, a efectos de comunicación de la ISA (véase la Recomendación X.407).

Nota – En sentido estricto, el papel de un sistema abierto viene determinado por el comportamiento de sus procesos de aplicación. En el contexto del tratamiento de mensajes, un proceso de aplicación realiza un objeto funcional de uno de los tipos definidos en el § 7. A su vez, un EU es una parte de un proceso de aplicación.

26.2 ESA simétricos y asimétricos

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

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

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

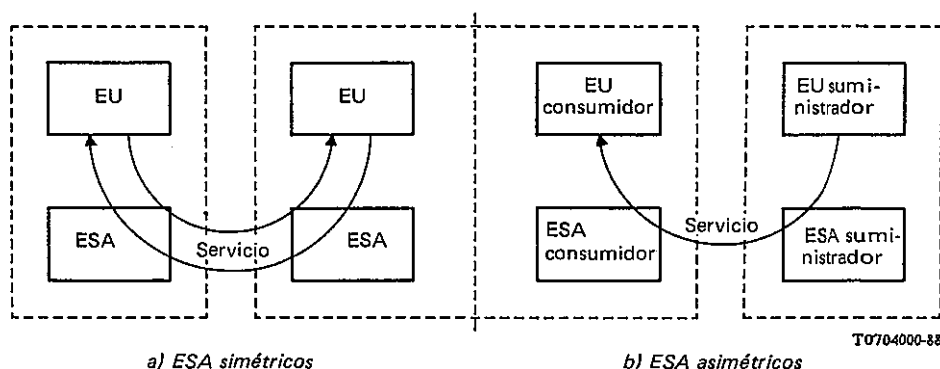


FIGURA 13/X.402

ESA simétricos y asimétricos

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

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

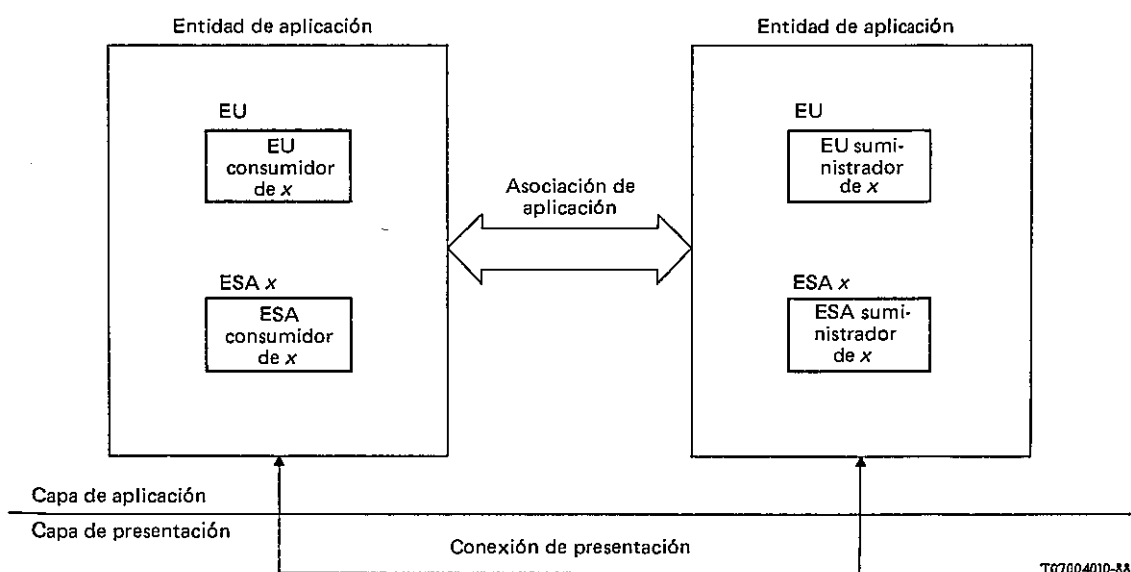


FIGURA 14/X.402

Terminología para ESA asimétricos

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

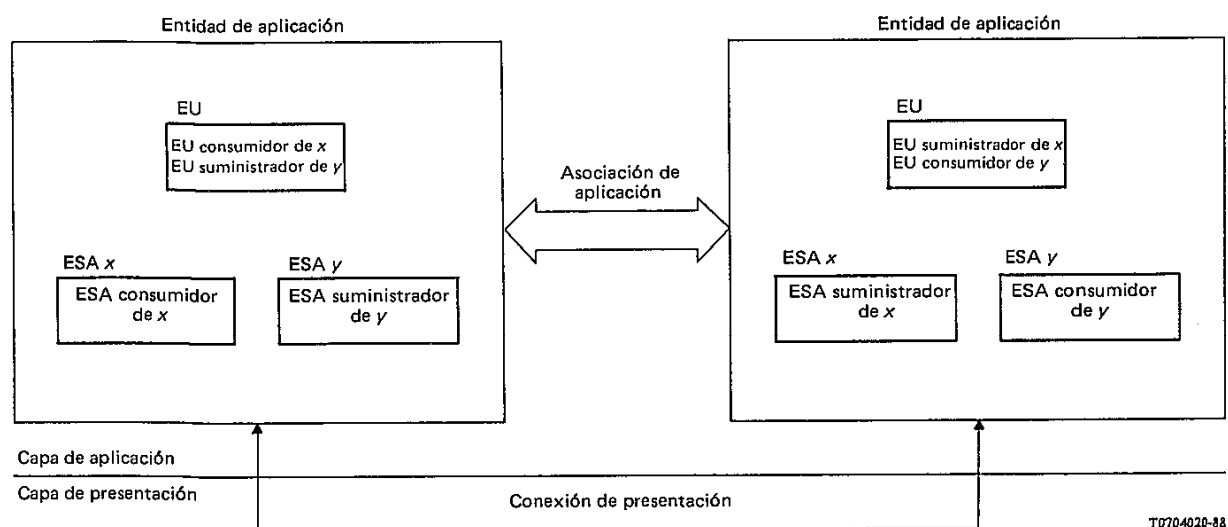


FIGURA 15/X.402
ESA asimétricos múltiples

26.3 ESA de tratamiento de mensajes

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

CUADRO 11/X.402
ESA de tratamiento de mensajes

ESA	Forma	Objetos funcionales			
		AU	MM	ATM	UA
ESTM	SIM	–	–	CS	–
ESDM	ASIM	C	CS	S	–
ESEM	ASIM	C	C	S	–
ESRM	ASIM	C	S	–	–
ESAM	ASIM	C	CS	S	–

SIM Simétrico
ASIM Asimétrico
C Consumidor
S Suministrador

Los ESA de tratamiento de mensajes, resumidos en el cuadro 11/X.402, se presentan por separado en los puntos que siguen. En la Recomendación X.419 figuran sus definiciones.

26.3.1 *Transferencia de mensajes*

El elemento de servicio transferencia de mensajes (ESTM) es el medio por el cual se efectúa el paso de transmisión de transferencia.

26.3.2 *Depósito de mensajes*

El elemento de servicio depósito de mensajes (ESDM) es el medio por el cual se efectúa el paso de transmisión de depósito.

26.3.3 *Entrega de mensajes*

El elemento de servicio entrega de mensajes (ESEM) es el medio por el cual se efectúa el paso de transmisión de entrega.

26.3.4 *Recuperación de mensajes*

El elemento de servicio recuperación de mensajes (ESRM) es el medio por el cual se efectúa el paso de transmisión de extracción.

26.3.5 *Administración de mensajes*

El elemento de servicio de administración de mensajes (ESAM) es el medio por el cual un AU, una MM o ATM archiva, en cada uno de los otros dos la información que facilita y controla su interacción subsiguiente, mediante el ESDM, ESM, el ESRM y el ESAM.

26.4 *ESA de apoyo*

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

CUADRO 12/X.402

ESA de apoyo

ESA	Forma
ESOD	SIM
ESTF	SIM
ESCA	SIM

SIM Simétrico

Los ESA de apoyo, resumidos en el cuadro 12/X.402 se presentan por separado en los puntos que siguen.

26.4.1 *Operaciones distantes*

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

El ESOD se define en la Recomendación X.219.

26.4.2 *Transferencia fiable*

El elemento de servicio transferencia fiable (ESTF) es el medio por el cual diversos ESA de tratamiento de mensajes, simétricos y asimétricos, transportan objetos de información - especialmente grandes, (por ejemplo, mensajes facsímil) - entre sistemas abiertos, de modo que se garantice su almacenamiento seguro en sus destinos.

El ESTF se define en la Recomendación X.218.

26.4.3 *Control de asociación*

El elemento de servicio control de asociación (ESCA) es el medio por el cual se establecen, se liberan y, en otros aspectos, se gestionan todas las asociaciones de aplicación entre sistemas abiertos.

El ESCA se define en la Recomendación X.217.

27 **Contextos de aplicación**

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

Un CA especifica cómo debe establecerse la asociación (por ejemplo, qué parámetros de inicialización se deben intercambiar), qué ESA deben participar en una comunicación entre pares a través de la asociación, qué limitaciones han de imponerse (si es que se impone alguna) a su utilización individual de la asociación, si el consumidor de cada ESA asimétrico es el iniciador o el contestador y cómo puede liberarse la asociación (por ejemplo, qué parámetros de finalización se deben intercambiar).

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

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

Las sintaxis abstractas de una UDPA es su estructura como objeto de información (por ejemplo, un conjunto NSA.1 que comprenda un código de instrucción entero y un argumento de instrucción cadena AI5). Se diferencia de la sintaxis de transferencia de la UDPA, que es como se representa el objeto de información para transmisión entre dos sistemas abiertos (por ejemplo, un octeto indicando un conjunto NSA.1, seguido por un octeto que dé la longitud del conjunto, etc.).

Los CA, por medio de los cuales se proporcionan los diversos servicios de tratamiento de mensajes, se especifican en la Recomendación X.419. A estos protocolos se les conoce por P1, P3 y P7.

Nota – La naturaleza del contenido de un mensaje no entra en la definición del CA de tratamiento de mensajes, porque el contenido queda englobado (como una cadena de octetos) en los protocolos que lo transportan.

ANEXO A
(a la Recomendación R.402)

Clases de objetos de guía y atributos

Este anexo forma parte integrante de la presente Recomendación.

Varias clases de objetos de guía, atributos y sintaxis de atributos son específicos del tratamiento de mensajes. Se definen en el presente anexo utilizando los macros OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE-SYNTAX respectivamente, de la Recomendación X.501.

A.1 *Clases de objetos*

A continuación se especifican las clases de objetos del tratamiento de mensajes.

Nota - Las clases de objetos de guía descritos en este anexo pueden combinarse con otras clases de objetos, por ejemplo, los definidos en la Recomendación X.521. En el § 9 de la Recomendación X.501 figura una explicación del modo en que pueden combinarse las clases de objetos de guía en una inscripción de guía. El anexo B de la Recomendación X.521 da más información sobre las formas de nombres de guía y posibles estructuras de árboles de informaciones de guía.

A.1.1 *Lista de distribución del STM*

Un objeto **lista de distribución del STM** es una LD. Los atributos de su inscripción identifican su nombre común, permisos de depósito y direcciones O/D y, en la medida en que estén presentes los atributos pertinentes, describen la LD, identifican su organización, sus unidades organizativas y su propietario, mencionan objetos relacionados e identifican sus tipos de contenido entregable, TIC entregables, miembros y métodos de entrega preferidos.

```
mhs-distribution-list OBJECT-CLASS
  SUBCLASS OF top
  MUST CONTAIN {
    commonName,
    mhs-dl-submit-permissions,
    mhs-or-addresses }
  MAY CONTAIN {
    description,
    organization,
    organizationalUnitName,
    owner
    seeAlso,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-dl-members,
    mhs-preferred-delivery-methods }
  ::= id-oc-mhn-distribution-list
```

A.1.2 *Memoria de mensajes del STM*

Un objeto **memoria de mensajes del STM** es una EA que realiza una MM. Los atributos de su inscripción, en la medida en que estén presentes, describen la MM, identifican a su propietario y enumeran los atributos facultativos, las acciones automáticas y los tipos de contenido que facilita.

```
mhs-message-store OBJECT-CLASS
  SUBCLASS OF applicationEntity
  MAY CONTAIN {
    description,
    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 STM*

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

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

A.1.4 *Usuario del STM*

Un objeto **usuario del STM** es un usuario genérico del STM (el usuario genérico del STM puede tener, por ejemplo, una dirección comercial, o una dirección privada, o ambas). Los atributos de su inscripción identifican la dirección O/D del usuario y, en la medida en que estén presentes, los atributos pertinentes identifican la longitud del contenido entregable del usuario, tipos de contenido y TIC, su MM y sus métodos de entrega preferidos.

```
mhs-user OBJECT-CLASS
  SUBCLASS OF top
  MUST CONTAIN {
    mhs-or-adresses },
  MAY CONTAIN {
    mhs-deliverable-content-length,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-message-store,
    mhs-preferred-delivery-methods }
::= id-oc-mhs-user
```

A.1.5 *Agente de usuario del STM*

Un objeto **agente de usuario del STM** es una EA que realiza un AU. Los atributos de su inscripción, en la medida en que estén presentes, identifican al propietario del AU, la longitud de su contenido entregable, tipos de contenido y TIC, y su dirección O/D.

```
mhs-user-agent OBJECT-CLASS
  SUBCLASS OF applicationEntity
  MAY CONTAIN {
    owner,
    mhs-deliverable-content-length,
    mhs-deliverable-content-types,
    mhs-deliverable-eits,
    mhs-or-adresses }
::= id-oc-mhs-user-agent
```

A.2 *Atributos*

Los atributos específicos del tratamiento de mensajes son los que se indican a continuación.

A.2.1 *Longitud de contenido entregable del STM*

El atributo **longitud del contenido entregable del STM** identifica la longitud máxima del contenido de los mensajes cuya entrega aceptará un usuario.

Un valor de este atributo es un entero.

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

A.2.2 *Tipos de contenido entregable del STM*

El atributo **tipos de contenido entregable del STM** identifica los tipos de contenido de los mensajes cuya entrega aceptará el usuario.

Un valor de este atributo es un identificador de objeto.

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

A.2.3 *TIC entregables del STM*

El atributo **TIC entregables del STM** identifica los TIC de los mensajes cuya entrega aceptará el usuario.

Un valor de este atributo es un identificador de objeto.

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

A.2.4 *Miembros de LD del STM*

El atributo **miembros de LD del STM** identifica los miembros de una LD.

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

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

A.2.5 *Permisos de depósito de LD del STM*

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

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

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

A.2.6 *Memoria de mensajes del STM*

El atributo **memoria de mensajes del STM** identifica una MM de usuario por un nombre.

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

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

A.2.7 *Direcciones O/D del STM*

El atributo **direcciones O/D del STM** especifica las direcciones O/D de un usuario o de una LD.

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

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

A.2.8 *Métodos de entrega preferidos del STM*

El atributo **métodos de entrega preferidos del STM** identifica, en orden decreciente de preferencias, los métodos de entrega que prefiere un usuario.

Un valor de este atributo es un método de entrega preferido.

```
mhs-preferred-delivery-methods ATTRIBUTE
  WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
  MATCHES FOR EQUALITY
  SINGLE VALUE
::= id-at-mhs-preferred-delivery-methods
```

A.2.9 Acciones automáticas permitidas por el STM

El atributo **acciones automáticas permitidas por el STM** identifica las acciones automáticas que un AM admite totalmente.

Un valor de este atributo es un identificador de objeto.

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

A.2.10 Tipos de contenido permitidos por el STM

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

Un valor de este atributo es un identificador de objeto.

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

A.2.11 Atributos facultativos permitidos por el STM

El atributo **atributos facultativos permitidos por el STM** identifica los atributos facultativos que permite totalmente una MM.

Un valor de este atributo es un identificador de objeto.

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

A.3 Sintaxis de atributos

Las sintaxis de atributos específicos del tratamiento de mensajes son las que se indican a continuación.

A.3.1 Permiso de depósito de LD del STM

La sintaxis de atributo **permiso de depósito de LD del STM** caracteriza un atributo, cada uno de cuyos valores es un permiso de depósito.

```
mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
  SYNTAX DLSubmitPermission
  MATCHES FOR EQUALITY
::= id-as-mhs-dl-submit-permission
```

```
DLSubmitPermission ::= CHOICE {
  individual          [0] ORName,
  member-of-dl        [1] ORName,
  pattern-match        [2] ORNamePattern,
  member-of-group      [3] Name }
```

El valor de un permiso de depósito de LD presentado será del tipo *individual*.

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

- a) *Individual*: Usuario o LD (no ampliada) alguno de cuyos nombres O/D es igual al nombre O/D especificado.
- b) *Miembro-de-ld*: Cada miembro de la LD, o de cada LD jerarquizada de manera recurrente, alguno de cuyos nombres O/D es igual al nombre O/D especificado.
- c) *Concordancia-de-esquemas*: Cada usuario o LD (no ampliada) alguno de cuyos nombres O/D satisface el esquema de nombres O/D especificado.
ORNamePattern ::= ORName
- d) *Miembro-de-grupo*: Cada miembro de grupo-de-nombres, o de cada grupo-de-nombres jerarquizado, de manera recurrente, cuyo nombre está especificado.

Se considera que un valor presentado es igual a un valor objetivo de este tipo si los dos son idénticos, atributo por atributo. Además, se puede declarar igualado en otras condiciones, que son asunto local.

A.3.2 Dirección O/D del STM

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

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

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

A.3.3 Nombre O/D del STM

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

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

Un valor de nombre O/D presentado es igual a un valor de nombre O/D objetivo si los dos son idénticos, atributo por atributo. Puede además declararse igualdad bajo otras condiciones, que son asunto local.

ANEXO B

(a la Recomendación X.402)

Definiciones de referencia de identificadores de objetos

Este anexo forma parte integrante de la presente Recomendación.

En él se definen, a efectos de referencia, diversos identificadores de objetos mencionados en el módulo NSA.1 del anexo C. Se utiliza NSA.1.

Todos los identificadores de objetos asignados por esta Recomendación lo son en el presente anexo. El anexo B es definitivo para todos, excepto para los de los módulos del NSA.1 y del propio STM. Las asignaciones definitivas para el primero se producen en los mismos módulos; en los párrafos IMPORT aparecen otras referencias a los mismos. El segundo es fijo.

```

MHSubjectIdentifiers {joint-iso-ccitt
    mhs-motis(6) arch(5) modules(0) object-identifiers(0)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
    -- Prólogo
    -- Exporta todo.

IMPORTS -- nada -- ;

ID ::= OBJECT IDENTIFIER

-- Aspectos del STM

id-mhsac      ID ::= { joint-iso-ccitt mhs-motis(6) mhsac(0) }
    -- Contexto de aplicación del STM
    -- Véase la Recomendación X.419

id-ipms       ID ::= { joint-iso-ccitt mhs-motis(6) ipms(1) }
    -- Mensajería interpersonal
    -- Véase la Recomendación X.420

id-asdc       ID ::= { joint-iso-ccitt mhs-motis(6) asdc (2) }
    -- Convenios de definición de servicio abstracto
    -- Véase la Recomendación X.407

id-mts ID ::= { joint-iso-ccitt mhs-motis(6) mts (3) }
    -- Sistema de transferencia de mensajes
    -- Véase la Recomendación X.411

id-ms ID ::= { joint-iso-ccitt mhs-motis(6) ms (4) }
    -- Memoria de mensajes
    -- Véase la Recomendación X.413

id-arch       ID ::= { joint-iso-ccitt mhs-motis(6) arch (5) }
    -- Arquitectura global
    -- Véase esta Recomendación

id-group      ID ::= { joint-iso-ccitt mhs-motis(6) group(6) }
    -- Reservado

-- Categorías

id-mod        ID ::= { id-arch 0 } -- módulos, no definitivo
id-oc         ID ::= { id-arch 1 } -- clases de objetos
id-at         ID ::= { id-arch 2 } -- tipos de atributos
id-as         ID ::= { id-arch 3 } -- sintaxis de atributos

-- Módulos

id-object-identifiers      ID ::= {id-mod 0} -- no definitivo
id-directory-objects-and-attributes; ID ::= {id-mod 1}
    --no definitivo

-- Clases de objetos

id-oc-mhs-distribution-list      ID ::= {id-oc 0 }
id-oc-mhs-message-store          ID ::= {id-oc 1 }
id-oc-mhs-message-transfer-agent ID ::= { id-oc 2 }
id-oc-mhs-user                   ID ::= { id-oc 3 }
id-oc-mhs-user-agent             ID ::= { id-oc 4 }

-- Atributos

id-at-mhs-deliverable-content-length      ID ::= { id-at 0 }
id-at-mhs-deliverable-content-types       ID ::= { id-at 1 }
id-at-mhs-deliverable-eits                ID ::= { id-at 2 }
id-at-mhs-dl-members                      ID ::= { id-at 3 }
id-at-mhs-dl-submit-permissions           ID ::= { id-at 4 }
id-at-mhs-message-store                   ID ::= { id-at 5 }
id-at-mhs-or-addresses                    ID ::= { id-at 6 }

```

id-at-mhs-preferred-delivery-methods	ID ::= { id-at 7 }
id-at-mhs-supported-automatic-actions	ID ::= { id-at 8 }
id-at-mhs-supported-content-types	ID ::= { id-at 9 }
id-at-mhs-supported-optional-attributes	ID ::= { id-at 10 }

-- *Sintaxis de atributos*

id-as-mhs-dl-submit-permission	ID ::= { id-as 0 }
id-as-mhs-or-address	ID ::= { id-as 1 }
id-as-mhs-or-name	ID ::= { id-as 2 }

END -- *final de los identificadores de objetos de STM*

ANEXO C

(a la Recomendación R.402)

Definición de referencia de clases de objetos de guía y atributos

Este anexo forma parte integrante de la presente Recomendación.

Este anexo, que complementa el anexo A define a efectos de referencia las clases de objetos, los atributos y las sintaxis de atributos específicos del tratamiento de mensajes. Para ello, se hace uso de las macro OBJECT-CLASS, ATTRIBUTE y ATTRIBUTE SYNTAX de la Recomendación X.501.

```
MHSDirectoryObjectsAndAttributes { joint-iso-ccitt
    mhs-motis(6) arch(5) modules(0) directory(1) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
-- Prólogo
-- Exporta todo
```

```
IMPORTS
```

```
-- Identificadores de objetos del STM
```

```
    id-as-mhs-dl-submit-permission, id-as-mhs-or-address,
    id-as-mhs-or-name-, id-at-mhs-deliverable-content-length,
    id-at-mhs-deliverable-content-types,
    id-at-mhs-deliverable-eits, id-at-mhs-dl-members,
    id-at-mhs-dl-submit-permissions, id-at-mhs-message-store,
    id-at-mhs-or-addresses, id-at-mhs-preferred-delivery-methods,
    id-at-mhs-supported-automatic-actions,
    id-at-mhs-supported-content-types,
    id-at-mhs-supported-optional-attributes,
    id-oc-mhs-distribution-list, id-oc-mhs-message-store,
    id-oc-mhs-message-transfer-agent,
    id-oc-mhs-user,
    id-oc-mhs-user-agent
```

```
    ----
    FROM MHSObjectIdentifiers { joint-iso-ccitt
        mhs-motis(6) arch(5) modules(0) object-identifiers(0) }
```

```
-- Servicio abstracto del STM
```

```
    ORAddress, ORName, RequestedDeliveryMethod
```

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

```

-- Marco de información
    ATTRIBUTE, ATTRIBUTE-SYNTAX, Name, OBJECT-CLASS
    ----
    FROM InformationFramework { joint-iso-ccitt
        ds(5) modules(1) informationFramework(a) }

-- Clases de objeto seleccionadas
    applicationEntity
    top
    ----
    FROM SelectedObjectClasses { joint-iso-ccitt
        ds(5) modules(1) selectedObjectClasses(6) }

-- Tipos de atributo seleccionados
    commonName, description, distinguishedNameSyntax,
    integerSyntax, objectIdentifierSyntax, organization,
    organizationalUnitName, owner, seeAlso
    ----
    FROM SelectedAttributeTypes { joint-iso-ccitt
        ds(5) modules(1) selectedAttributeTypes(5) };

-- CLASES DE OBJETOS

-- Lista de distribución del STM
    mhs-distribution-list OBJECT-CLASS
        SUBCLASS OF top
        MUST CONTAIN {
            commonName,
            mhs-dl-submit-permissions,
            mhs-or-addresses }
        MAY CONTAIN {
            description,
            organization,
            organizationalUnitName,
            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 STM
    mhs-message-store OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
            description,
            owner,
            mhs-supported-optional-attributes,
            mhs-supported-automatic-actions,
            mhs-supported-content-types }
        ::= id-oc-mhs-message-store

-- Agente de transferencia de mensajes del STM
    mhs-message-transfer-agent OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
            description,
            owner,
            mhs-deliverable-content-length }
        ::= id-oc-mhs-message-transfer-agent

-- Usuario del STM
    mhs-user OBJECT-CLASS
        SUBCLASS OF TOP

```

```

    MUST CONTAIN {
        mhs-or-addresses }
    MAY CONTAIN {
        mhs-deliverable-content-length,
        mhs-deliverable-content-types,
        mhs-deliverable-eits,
        mhs-message-store,
        mhs-preferred-delivery-methods }
    ::= id-oc-mhs-user

-- Agente de usuario del STM
mhs-user-agent OBJECT-CLASS
    SUBCLASS OF applicationEntity
    MAY CONTAIN {
        owner,
        mhs-deliverable-content-length,
        mhs-deliverable-content-types,
        mhs-deliverable-eits,
        mhs-or-addresses }
    ::= id-oc-mhs-user-agent

-- ATRIBUTOS

-- Longitud de contenido entregable del STM
mhs-deliverable-content-length ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX integerSyntax
    SINGLE VALUE
    ::= id-at-mhs-deliverable-content-length

-- Tipos de contenido entregable del STM
mhs-deliverable-content-types ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-deliverable-content-types

-- TIC entregables del STM
mhs-deliverable-eits ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-deliverable-eits

-- Miembros de LD del STM
mhs-dl-members ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
    MULTI VALUE
    ::= id-at-mhs-dl-members

-- Permisos de depósito de LD del STM
mhs-dl-submit-permissions ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
    MULTI VALUE
    ::= id-at-mhs-dl-submit-permissions

-- Direcciones O/D del STM
mhs-or-addresses ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX mhs-or-address-syntax
    MULTI VALUE
    ::= id-at-mhs-or-addresses

-- Memoria de mensajes del STM
mhs-message-store ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX distinguishedNameSyntax
    SINGLE VALUE
    ::= id-at-mhs-message-store

```

```

-- Métodos de entrega preferidos del STM
mhs-preferred-delivery-methods ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX RequestedDeliveryMethod
    MATCHES FOR EQUALITY
    SINGLE VALUE
    ::= id-at-mhs-preferred-delivery-methods

-- Acciones automáticas admitidas por el STM
mhs-supported-automatic-actions ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-supported-automatic-actions

-- Tipos de contenido admitidos por el STM
mhs-supported-content-types ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-supported-content-types

-- Atributos facultativos admitidos por el STM
mhs-supported-optional-attributes ATTRIBUTE
    WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
    MULTI VALUE
    ::= id-at-mhs-supported-optional-attributes

-- SINTAXIS DE ATRIBUTO

-- Permiso de presentación de LD de STM
mhs-dl-submit-permission-syntax ATTRIBUTE-SYNTAX
    SYNTAX DLSubmitPermission
    MATCHES FOR EQUALITY
    ::= id-as-mhs-dl-submit-permission

DLSubmitPermission ::= CHOICE {
    individual          [0] ORName,
    member-of-dl [1] ORName,
    pattern-match [2] ORNamePattern,
    member-of-group    [3] Name }

ORNamePattern ::= ORName

-- Dirección O/D del STM
mhs-or-address-syntax ATTRIBUTE-SYNTAX
    SYNTAX ORAddress
    MATCHES FOR EQUALITY
    ::= id-as-mhs-or-address

-- Nombre O/D del STM
mhs-or-syntax ATTRIBUTE-SYNTAX
    SYNTAX ORName
    MATCHES FOR EQUALITY
    ::= id-as-mhs-or-name

END -- final de la guía del STM

```

ANEXO D

Amenazas contra la seguridad

Este anexo no forma parte de la presente Recomendación.

En el § 15.1 de la Recomendación X.400 se da una visión general de las amenazas contra la seguridad del STM. En esta Recomendación se consideran las amenazas tal como se plantean en el STM: amenazas en el acceso, amenazas entre mensajes, amenazas en los propios mensajes y amenazas en su almacenamiento. Todas estas amenazas pueden aparecer en las diversas formas siguientes:

- a) suplantación;
- b) secuenciamiento de mensajes;
- c) modificación de información
- d) denegación de servicio;
- e) fuga de información;
- f) rechazo;
- g) otras amenazas del STM.

Además, las amenazas pueden surgir por accidente o intento doloroso, y pueden tener un carácter activo o pasivo. Las agresiones al STM se dirigirán hacia sus debilidades potenciales, y pueden comprender un cierto número de amenazas. Este anexo se ocupa de amenazas individuales, examinándose varios tipos amplios de amenazas, que de todos modos no constituyen una relación exhaustiva de las mismas.

En el cuadro D-1/X.402 se indica cómo hacer frente a esas amenazas utilizando los servicios de seguridad del STM. La lista de amenazas que aquí se da es indicativa, no definitiva.

CUADRO D-1/X.402

Utilización de los servicios de seguridad del STM

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

D.1 *Suplantación*

El fenómeno llamado suplantación ocurre cuando una entidad finge, con éxito, ser una entidad distinta de la que es, y puede tener lugar de diferentes maneras. Un usuario no autorizado del STRM puede simular a otro para acceder sin permiso a las facilidades del STRM, o actuar en detrimento de un usuario válido, por ejemplo, desechando sus mensajes. Un usuario del STRM puede suplantar a otro y acusar recibo, falsamente, de un mensaje en nombre del receptor «válido». Un mensaje puede ser introducido en el STRM por un usuario que utilice falsamente la identidad de otro. Un usuario del STRM, un AM o un ATM se pueden enmascarar como si fuesen un usuario, un AM o un ATM distintos.

Entre las amenazas de tipo suplantación figuran las siguientes:

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

Una suplantación incluye normalmente otras formas de agresión y, en un sistema seguro, puede implicar series de autenticaciones de usuarios válidos, por ejemplo, en la reactuación o modificación de mensajes.

D.2 *Secuenciamiento de mensajes*

Las amenazas contra la secuenciación de mensajes se producen cuando un mensaje se repite, entero o en parte, se le desplaza en el tiempo o se reordena. Puede recurrirse a esto para aprovecharse de la información de autenticación de un mensaje válido o reordenar o desplazar en el tiempo mensajes válidos. Si bien con los servicios de seguridad del STM es imposible evitar la reactuación de mensajes, sí cabe detectarlas y eliminar los efectos de esa amenaza.

Entre las amenazas a la secuenciación de mensajes figuran las siguientes:

- a) reactuación de mensajes;
- b) reordenación de mensajes;
- c) adelanto de mensajes;
- d) retraso de mensajes.

D.3 *Modificación de información*

La información para un destinatario deseado, la información de encaminamiento y otros datos relativos a la gestión pueden perderse o modificarse sin que ello se detecte. Es algo que puede ocurrir con cualquier elemento del mensaje, por ejemplo, su etiquetado, el contenido, los atributos, el destinatario o el originador. La degradación de la información de encaminamiento o de otro tipo de información de la gestión, almacenada en los ATM o utilizada por ellos, puede dar lugar a que el STRM pierda mensajes o bien a que funcione de manera incorrecta.

Entre las amenazas de tipo modificación de información figuran las siguientes:

- a) modificación de mensajes;
- b) destrucción de mensajes;
- c) degradación del encaminamiento y de otra información de gestión.

D.4 *Denegación de servicio*

La denegación de servicio se produce cuando una entidad deja de realizar su cometido o evita que otras realicen los suyos. Puede tratarse de una denegación de acceso o de comunicaciones (que da lugar a otros problemas, como los de sobrecarga), una eliminación deliberada de mensajes dirigidos a un determinado destinatario, o una invención de tráfico extra. Se denegará el STRM si se provoca el fallo o el funcionamiento incorrecto de un ATM. Además, un usuario del STRM puede dar lugar a que dicho servicio se deniegue a otro usuario, saturándolo con mensajes que podrían sobrecargar la capacidad de conmutación de un ATM o llenar el espacio de almacenajes de mensajes de que se dispone.

Entre las amenazas de denegación de servicio figuran las siguientes:

- a) denegación de comunicaciones;
- b) fallo del ATM;
- c) saturación del STRM.

D.5 *Rechazo*

El rechazo tiene lugar cuando un usuario del STRM o el propio STRM pueden negar a posteriori el depósito, la recepción o la originación de un mensaje.

Entre las amenazas de rechazo figuran las siguientes:

- a) denegación de origen;
- b) denegación de depósito;
- c) denegación de entrega.

D.6 *Fuga de información*

Un ente no autorizado puede captar información vigilando las transmisiones o accediendo sin permiso a la información almacenada en alguna entidad del STM o por suplantación. En algunos casos, la presencia en el sistema de un usuario del STRM puede ser un asunto delicado y debe preservarse su anonimato. También es posible que un usuario del STRM distinto del destinatario deseado se haga con un mensaje enviado al segundo. Este podría ser el resultado de la simulación y del mal uso del STRM, o de haber provocado el funcionamiento incorrecto de un ATM. Además, observando el tráfico se pueden obtener otros detalles sobre la información que fluye por un STRM.

Entre las amenazas de fuga de información, figuran las siguientes:

- a) pérdida de confidencialidad;
- b) pérdida de anonimato;
- c) apropiación indebida de mensajes;
- d) análisis de tráfico.

D.7 *Otras amenazas*

En un sistema de seguridad de nivel único o de nivel múltiple, puede haber cierto número de amenazas relativas al etiquetado de seguridad, por ejemplo, el encaminamiento a través de un nodo al que no se le puede confiar información particularmente valiosa o en donde los sistemas utilizan procedimiento de etiquetado diferentes. Pueden existir amenazas a la implantación de una política de seguridad basada en la separación lógica utilizando etiquetas de seguridad. Es posible que un usuario del STRM origine un mensaje y le asigne una etiqueta para la que no está autorizado. Cabe también que un usuario del STRM o un ATM establezcan o acepten una asociación con un contexto de seguridad, para el que no tienen autorización.

Entre las «otras amenazas» aludidas en el epígrafe, figuran las siguientes:

- a) originador no autorizado para etiqueta de seguridad de mensajes (depósito inadecuado);
- b) usuario del STRM/ATM no autorizado para el contexto;
- c) encaminamiento erróneo;
- d) procedimientos de etiquetado diferentes.

ANEXO E

(a la Recomendación R.402)

Provisión de servicios de seguridad en la Recomendación X.411

Este anexo forma parte de la presente Recomendación.

En el cuadro E-1/X.402 se indica qué elementos de servicio de la Recomendación X.411 pueden utilizarse para facilitar los servicios de seguridad descritos en el § 10.2.

CUADRO E-1/X.402

Provisión de servicios de seguridad del STM

Servicio	Argumentos/servicios del STRM
<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

Diferencias entre la Recomendación del CCITT y la norma ISO

Este anexo no forma parte de la presente Recomendación.

En él se da una relación de todas las diferencias, excepto las puramente estilísticas, entre esta Recomendación y la correspondiente norma internacional de la ISO.

Entre ambas especificaciones hay las diferencias siguientes:

- a) La Norma Internacional de la ISO que corresponde a esta Recomendación muestra la conexión directa de dos DGPR situados en el mismo país, la de dos DGPR situados en países diferentes, y la de un solo DGPR conectado a dos DGAD, lo que no hace esta Recomendación (véase la figura 11/X.402).
- b) La Norma Internacional de la ISO que corresponde a esta Recomendación no requiere que los DGAD y los DGPR estén relacionados jerárquicamente para direccionamiento y encaminamiento; mientras que esta Recomendación sí lo requiere (véanse los § 14.1.1, 14.1.2, 15 y 19).
- c) Cuando un atributo de dirección O/D admite cadenas imprimibles y teletex, la Norma Internacional de la ISO que corresponde a esta Recomendación, no requiere que se proporcione la cadena imprimible, como mínimo, cuando los atributos se estén transportando internacionalmente, mientras que esta Recomendación sí lo requiere (véase el § 18.2).

ANEXO G

Índice

Este anexo no forma parte de la presente Recomendación.

Este anexo constituye el índice de esta Recomendación. Proporciona los números de los puntos donde se definen los elementos de cada categoría. El tratamiento de cada categoría es exhaustivo.

Este anexo presenta un índice de los elementos (si los hay) en las siguientes categorías:

- a) abreviaturas;
- b) términos;
- c) elementos de información;
- d) módulos NSA.1;
- e) macros NSA.1;
- f) tipos NSA.1;
- g) valores NSA.1;
- h) acuerdos bilaterales
- i) **elementos que requieren ulterior estudio;**
- j) **elementos a preparar.**

G.1 Abreviaturas

A/SYS 13.1.1

AS/SYS 13.1.3

ASG 3.2

AST/SYS 13.1.7

AT/SYS 13.1.5

ATM 7.3.1

AU 7.2.2

C 5.2

CA 3.1.3, 27

COMPUSEC 10

D 5.2

DG 14.1

DGAD 14.1.1	MM 7.2.3
DGPR 14.1.2	NSA.1 13.1.2
EA 3.1.1	O 5.2
ESA 3.1.1, 26	OD 3.1.5
ESAM 26.3.5	P1 27
ESCA 3.13, 26.4.3	P3 27
ESDM 26.3.2	P7 27
ESEM 26.3.3	S/SYS 13.1.2
ESOD 3.1.5, 26.4.1	SEF 7.4.1
ESRM 26.3.4	ST/SYS 13.1.6
ESTF 3.1.4, 26.4.2	STM 7.1.1
ESTM 26.3.1	STRM 7.2.1
ETM 7	T/SYS 13.1.4
EU 3.1.1	TF 3.1.4
F 5.2	TIC 8.1
IS	UA 7.2.4
ISA 3.1.1	UDPA 3.1.1
LD 7.1.3	UAEF 7.4.1

G.2 Términos

afirmación 9.4.9	conversión 9.4.6
agente de depósito 9.3.2	conversión explícita 9.4.6
agente de entrega 9.3.6	conversión implícita 9.4.6
agente de transferencia de mensajes 7.3.1	defectible 5.2
agente de usuario 7.2.2	depósito 9.3.2
almacenamiento de mensajes 6	depósito directo 9.3.2
ampliación de LD 9.4.4	depósito indirecto 9.3.2
asimétrico 26.2	destinatario 9.2
atributo 18.1	destinatario alternativo al destinatario asignado 9.2
atributo definido por el dominio 18.1	destinatario alternativo especificado por
atributo normalizado 18.1	el originador 9.2
atributos-postales-locales 18.3.6	destinatario deseado 9.2
código postal 18.3.19	destinatario efectivo 9.2
combinación 9.4.2	destinatario indirecto 9.2
componentes-ampliación-dirección-entrega	destinatario inmediato 9.1
física 18.3.5	destinatario miembro 9.2
componentes-ampliación-dirección-O/D	destinatario potencial 9.2
postal 18.3.4	dirección-apartado-correos 18.3.18
condicional 5.2	dirección-calle 18.3.22
contenido 8.1	dirección-lista-correos 18.3.20

dirección-postal-no-formatizada 18.3.25
 dirección O/D 18.5
 dirección O/D numérica 18.3.2
 dirección O/D nemotécnica 18.5.1
 dirección O/D postal 18.5.3
 dirección O/D terminal 18.5.4
 dirección-red 18.3.7
 división 9.4.1
 dominio 14.1
 dominio de gestión 14.1
 dominio de gestión de administración 14.1.1
 dominio de gestión privado 14.1.2
 encaminamiento 9.4.10
 encaminamiento externo 9.4.10
 encaminamiento interno 9.4.10
 entorno de tratamiento de mensajes 7
 entrega 9.3.6
 entrega física 7.4.1
 ESA consumidor 26.2
 ESA suministrador 26.2
 EU consumidor 26.2
 EU suministrador 26.2
 evento 9.1
 evento de transmisión 9.1
 exportación 9.3.5
 recuperación 9.3.7
 facultativo 5.2
 formatizado 18.5.3
 grado 5.2
 indentificador terminal 18.3.23
 indentificador-usuario-numérico 18.3.8
 importación 9.3.3
 informe 8.3
 informe de entrega 8.3
 informe de no entrega 8.3
 jerarquizado 7.1.3
 lista de atributos 18.1
 lista de distribución 7.1.3
 memoria de mensajes 7.2.3
 mensaje 8.1
 mensaje descrito 8.2
 mensaje físico 7.4.1
 mensaje objeto 8.3
 miembros 7.1.3
 no entrega 9.4.7
 no formatizado 18.5.3
 no afirmación 9.4.8
 nombre-común 18.3.2
 nombre-dominio-administración 18.3.1
 nombre-dominio-privado 18.3.21
 nombre O/D 17.2
 nombre-organización 18.3.9
 nombre-organización-entrega-física 18.3.16
 nombre-país 18.3.3
 nombre-país-entrega-física 18.3.13
 nombre-personal 18.3.12
 nombre-personal-entrega-física 18.3.17
 nombre-postal-exclusivo 18.3.26
 nombre-servicio-entrega-física 18.3.11
 nombre-unidades-organizativas 18.3.10
 número-oficina-entrega-física 18.3.14
 obligatorio 5.2
 origen 9.3.1
 originador 9.2
 paso 9.1
 paso de transmisión 9.1
 permiso de depósito 7.1.3
 punto de ampliación 9.4.4
 recepción 9.3.8
 redirección 9.4.5
 reproducción física 7.4.1
 resolución de nombre 9.4.3
 simétrico 26.2
 sistema de acceso 13.1.1
 sistema de acceso y almacenamiento 13.1.3
 sistema de acceso, almacenamiento y
 transferencia 13.1.7
 sistema de acceso y transferencia 13.1.5
 sistema de almacenamiento 13.1.2
 sistema de almacenamiento y transferencia 13.1.6
 sistema de entrega física 7.4.1
 sistema de mensajería 13.1

sistema de transferencia 13.1.4
sistema de transferencia de mensajes 7.2.1
sistema de tratamiento de mensajes 7.1.1
sonda
sonda objeto 8.3
STM global 15
tipo 18.1
tipo de atributo 18.1
tipo de contenido 8.1
tipo de información codificada 18.1
tipo-terminal 18.3.24
transferencia 9.3.4

transferencia externa 9.3.4
transferencia interna 9.3.4
transferencia de mensajes 6
transmisión 9.1
tratamiento de mensajes 6
unidad de acceso 7.2.4
unidad de acceso de entrega física 7.4.1
usuario 7.1.2
usuario directo 7.1.2
usuario indirecto 7.1.2
valor 18.1
valor de atributo 18.1

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación