



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

X.802

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/95)

**REDES DE DATOS Y COMUNICACIÓN
ENTRE SISTEMAS ABIERTOS**

SEGURIDAD

**TECNOLOGÍA DE LA INFORMACIÓN –
MODELO DE SEGURIDAD
DE CAPAS INFERIORES**

Recomendación UIT-T X.802

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.º 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.802 se aprobó el 10 de abril de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 13594.

NOTA

En esta Recomendación, la expresión «Administración» se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

© UIT 1996

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

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Página

1	Alcance.....	1
2	Referencias normativas.....	1
	2.1 Recomendaciones Normas internacionales idénticas.....	1
	2.2 Pares de Recomendaciones Normas Internacionales de contenido técnico equivalente.....	2
	2.3 Referencias adicionales.....	2
3	Definiciones.....	3
	3.1 Definiciones del modelo de referencia de OSI.....	3
	3.2 Definiciones de marcos de seguridad de sistemas abiertos.....	3
	3.3 Organización interna de las definiciones de la capa de red.....	3
	3.4 Definiciones adicionales.....	3
4	Abreviaturas.....	3
5	Asociaciones de seguridad.....	4
	5.1 Visión general.....	4
	5.2 Establecimiento de asociaciones de seguridad para las capas inferiores.....	5
	5.3 Cierre de la asociación de seguridad.....	6
	5.4 Modificación de atributos en una conexión.....	6
6	Repercusión en los protocolos existentes.....	7
	6.1 Principio general.....	7
	6.2 Tamaño de SDU sin conexión.....	7
	6.3 Concatenación de las PDU.....	7
	6.4 Independencia con respecto al algoritmo y a los mecanismos.....	7
7	Estructura de PDU de seguridad común.....	7
8	Determinación de los servicios y mecanismos de seguridad.....	8
9	QOS de protección.....	8
10	Reglas de seguridad.....	8
11	Colocación de seguridad en las capas inferiores.....	8
12	Utilización de capa(s) (N-1) para mejorar la seguridad de capa (N).....	14
13	Etiquetado de seguridad.....	15
14	Dominios de seguridad.....	15
15	Seguridad de encaminamiento.....	15
16	Gestión de seguridad.....	16
	16.1 Política de seguridad.....	16
	16.2 Gestión de asociaciones de seguridad.....	16
	16.3 Gestión de claves.....	16
	16.4 Auditoría de seguridad.....	16
17	Confidencialidad del flujo de tráfico.....	16
18	Directrices para la definición de atributos de SA.....	16
19	Tratamiento de errores.....	17
	Anexo A – Ejemplo ilustrativo de un conjunto convenido de reglas de seguridad.....	18

Resumen

La presente Recomendación | Informe técnico describe los aspectos de la prestación de servicios de seguridad en las capas más bajas del modelo de referencia de OSI (capas de transporte, red, enlace de datos, física) y describe los conceptos arquitecturales comunes a estas capas, la base para las interacciones en relación con la seguridad entre capas y la ubicación de protocolos de seguridad en las capas más bajas.

INFORME TÉCNICO**RECOMENDACIÓN UIT-T****TECNOLOGÍA DE LA INFORMACIÓN – MODELO DE SEGURIDAD DE CAPAS INFERIORES****1 Alcance**

La presente Recomendación | Informe técnico describe los aspectos de la prestación de servicios de seguridad en las capas más bajas del modelo de referencia de OSI (capas de transporte, de red, de enlace de datos y física).

La presente Recomendación | Informe técnico describe:

- a) los conceptos arquitecturales comunes a las capas más bajas basados en los definidos en la Rec. X.800 del CCITT | ISO 7498-2;
- b) la base para las interacciones relacionadas con la seguridad entre protocolos en las capas inferiores;
- c) la base para cualquier interacción relacionada con la seguridad entre las capas más bajas y las capas más altas de OSI;
- d) la ubicación de los protocolos de seguridad en relación con otros protocolos de seguridad de capas más bajas y el cometido relativo de tales ubicaciones.

No debe haber conflicto entre los protocolos de seguridad para las capas más bajas y el modelo descrito en esta Recomendación | Informe técnico.

La Rec. X.500 del CCITT | ISO/CEI 9594-1 identifica los servicios de seguridad pertinentes a cada una de las capas más bajas del modelo de referencia de OSI.

2 Referencias normativas

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

2.1 Recomendaciones | Normas internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- Recomendación UIT-T X.233 (1993) | ISO/CEI 8473-1:1994, *Tecnología de la información – Protocolo para proporcionar el servicio de red sin conexión de interconexión de sistemas abiertos: Especificación del protocolo.*
- Recomendación UIT-T X.234 (1994) | ISO/CEI 8602:1995, *Tecnología de la información – Protocolo para proporcionar el servicio de transporte en modo sin conexión de interconexión de sistemas abiertos.*
- Recomendación UIT-T X.273 (1994) | ISO/CEI 11577:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de seguridad de la capa de red.*
- Recomendación UIT-T X.274 (1994) | ISO/CEI 10736:1995, *Tecnología de la información – Intercambio de telecomunicaciones e información entre sistemas – Protocolo de seguridad de la capa de transporte.*

- Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores.*
- Recomendación UIT-T X.8101¹⁾ | ISO/CEI 10181-1...¹⁾, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: visión de marcos de seguridad.*
- Recomendación UIT-T X.812¹⁾ | ISO/CEI 10181-3...¹⁾, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: marco de control de acceso.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de interconexión de sistemas abiertos para aplicaciones del CCITT.*
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*
- Recomendación UIT-T X.224 (1993), *Protocolo para proporcionar el servicio de transporte en modo conexión para la interconexión de sistemas abiertos.*
ISO/CEI 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service.*
- Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno (NSA.1).*
ISO/CEI 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*
- Recomendación X.209 del CCITT (1988), *Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (NSA.1).*
Norma ISO/CEI 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

2.3 Referencias adicionales

- ISO/CEI 8208:1995, *Information technology – Data Communications – X.25 Packet Layer Protocol For Data Terminal Equipment.*
- Recomendación UIT-T X.25 (1993), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos dedicados.*
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organisation of the Network Layer.*
- ISO 9542:1988²⁾, *Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode Network Service (ISO 8473).*
- ISO/CEI 10589:1992, *Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain routing exchange protocol for use in conjunction with the protocol providing the connectionless-mode Network Service (ISO 8473).*
- ISO/CEI 10747:1994, *Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO 8473 PDUs.*

1) Actualmente en estado de proyecto.

2) Actualmente en revisión.

3 Definiciones

3.1 Definiciones del modelo de referencia de OSI

En la presente Recomendación | Informe técnico se utiliza el siguiente término definido en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

- calidad de servicio

3.2 Definiciones de marcos de seguridad de sistemas abiertos

En la presente Recomendación | Informe técnico se utiliza el siguiente término definido en la Rec. UIT-T X.810 | ISO/CEI 10181-1:

- dominio de seguridad

3.3 Organización interna de las definiciones de la capa de red

En la presente Recomendación | Informe técnico se utilizan los siguientes términos definidos en ISO 8648.

- a) protocolo de acceso de subred;
- b) sistema de extremo;
- c) sistema intermedio.

3.4 Definiciones adicionales

A los efectos de la presente Recomendación | Informe técnico se aplican las siguientes definiciones:

3.4.1 protección de reflexión: Mecanismo de protección para detectar cuándo una unidad de datos de protocolo ha sido devuelta al originador.

3.4.2 atributos de asociación de seguridad: Conjunto de informaciones requeridas para controlar la seguridad de las comunicaciones entre una entidad y su par o pares distantes.

3.4.3 asociación de seguridad: Relación entre las entidades comunicantes de capas inferiores para las cuales existen atributos de asociación de seguridad correspondientes.

3.4.4 reglas de seguridad: Información local que, dados los servicios de seguridad seleccionados, especifica los mecanismos de seguridad subyacentes que se han de emplear, incluidos todos los parámetros necesarios para el funcionamiento del mecanismo.

NOTA – Las reglas de seguridad constituyen una forma de reglas de interacción seguras como se define en el modelo de seguridad de capas superiores (Rec. UIT-T X.803 | ISO/CEI 10745).

4 Abreviaturas

ISN	Número secuencial para la integridad (<i>integrity sequence number</i>)
SSAA	Conjunto de atributos de SA (<i>set of SA attributes</i>)
NLSP	Protocolo de seguridad de capa de red (<i>network layer security protocol</i>)
NLSP-CO	NLSP para el modo con conexión (<i>NLSP connection mode</i>)
NLSP-CL	NLSP para el modo sin conexión (<i>NLSP connectionless mode</i>)
QOS	Calidad de servicio (<i>quality of service</i>) (definido en la Rec. X.200 del CCITT ISO 7498-1)
SA	Asociación de seguridad (<i>security association</i>)
SA-ID	Identificador de asociación de seguridad (<i>security association identifier</i>)
SNAcP	Protocolo de acceso de subred (<i>subnetwork access protocol</i>) (definido en ISO 8648)
SNISP	Protocolo de seguridad independiente de subred (<i>subnetwork independent security protocol</i>)
TLSP	Protocolo de seguridad de capa de transporte (<i>transport layer security protocol</i>)

5 Asociaciones de seguridad

5.1 Visión general

5.1.1 Todo protocolo de seguridad utiliza varios mecanismos de seguridad para suministrar servicios de seguridad a la capa inmediata superior. Los servicios de seguridad requeridos por la capa superior pueden ser indicados a las capas inferiores utilizando las funciones de gestión de seguridad local. El protocolo de seguridad y cada uno de sus mecanismos de seguridad requieren información, además de la información codificada en las PDU, para permitir una comunicación segura. Como ejemplos de esta información adicional cabe citar la especificación de los mecanismos que han de ser utilizados por el protocolo y, para cada mecanismo, la información específica tal como la clave requerida por un mecanismo de cifrado. Cada información adicional se denomina un atributo de asociación de seguridad.

5.1.2 Los atributos de asociación de seguridad pueden estar colocados en una entidad de protocolo que utiliza varios mecanismos. Algunos ejemplos de mecanismos de colocación son:

- a) colocación durante la fabricación de un dispositivo;
- b) colocación durante la inicialización de un dispositivo;
- c) colocación a través de una interfaz manual, por ejemplo controles en el panel frontal;
- d) colocación por la gestión de seguridad de sistemas de OSI;
- e) colocación por la gestión de seguridad de capas de OSI;
- f) colocación por la gestión de seguridad de operaciones de OSI.

5.1.3 Los atributos de SA se pueden colocar en cualquier momento antes de la comunicación con la cual se relacionan. Cuando hay conjuntos de atributos de SA (SSAA) compatibles en cada entidad de protocolo, se dice que existe una asociación de seguridad entre las entidades de protocolo.

5.1.4 Los SSAA (y asociaciones de seguridad) pueden tener diferente granularidad. A veces es útil poder referirse a los SSAA con diferente granularidad. Por ejemplo, el SSAA definido por un conjunto convenido de reglas de seguridad (ASSR) se podría denotar mediante SSAA ASSR, o se puede establecer un par de claves correspondientes entre dos entidades de protocolo para utilizarlas en varios casos de un par de direcciones origen-destino común. De manera similar, el SSAA para un caso de comunicación se podría indicar como SSAA-caso de comunicación, y el SSAA para una PDU con conexión se podría indicar como SSAA CO PDU.

5.1.5 En general, los atributos de SA deben ser colocados en la entidad de protocolo por medios seguros para mantener la seguridad. Esto supone que los atributos de SA se colocan empleando un medio físicamente seguro o que se pueden colocar utilizando una asociación de seguridad existente que ha sido colocada previamente para este fin.

5.1.6 El SSAA que forma parte de una asociación de seguridad es a menudo señalado por un identificador que tiene significado local y se conoce como SA-ID. En cualquier momento, algunos miembros del conjunto de atributos de SA pueden no estar definidos. Típicamente, durante la inicialización de una comunicación de seguridad, el SSAA no estará totalmente preparado y los intercambios iniciales se utilizarán para preparar completamente el SSAA antes que se intercambien datos de usuario.

5.1.7 Con el fin de proporcionar protección contra reproducción, se deben aplicar restricciones a la utilización de los SA-ID, sus SSAA referenciados y atributos de SA.

- a) Los SA-ID no pueden ser reutilizados con la misma clave de cifrado.
- b) Después que algún atributo de SA ha sido introducido en un SSAA que es referenciado por un SA-ID, ese atributo de SA no debe cambiarse nunca, a menos que el protocolo de seguridad posea un medio para señalar el cambio entre las entidades comunicantes. Esto entraña que para poder cambiar la clave, se debe utilizar un nuevo SA-ID con copias de los antiguos atributos de SA y una nueva clave, a menos que el protocolo de seguridad posea un medio alternativo de señalar el cambio de clave (por ejemplo, soportado por la PDU de NLSP-CO CSC).

5.1.8 La supresión de cualquier atributo de SA del SSAA cierra efectivamente la asociación de seguridad.

5.1.9 Algunos atributos de SA tienen significado para un caso de comunicación (una PDU sin conexión o una conexión). Otros atributos de SA tienen significado para una sola PDU en una conexión. Los números de secuencia para integridad y las etiquetas de seguridad constituyen ejemplos de tales atributos de SA. Puede suceder que el cambio de estos atributos de SA viole la restricción indicada en 5.1.7, b). No obstante, lógicamente la asociación de seguridad,

incluidos estos atributos de SA, sólo es válida para la duración de una PDU. El ISN actúa como una ampliación lógica del SA-ID, cambiando así el SA-ID efectivo. La etiqueta sólo es válida para este caso del SA-ID ampliado. De este modo, se mantienen las restricciones. Estos atributos de SA se denominan a veces atributos de SA «dinámicos».

5.1.10 Una parte de una política de seguridad restringirá el funcionamiento de la entidad de protocolo. Esta parte de la política de seguridad se denomina el conjunto de reglas de seguridad para la entidad de protocolo. El conjunto de reglas de seguridad para una entidad de protocolo puede restringir, por ejemplo, los mecanismos de seguridad que se han de utilizar y los valores y mecanismos de ubicación para los atributos de SA. El conjunto de reglas de seguridad también definirá la correspondencia de los servicios de seguridad seleccionados con los mecanismos de seguridad utilizados por el protocolo de seguridad. El conjunto de reglas de seguridad es una forma de reglas de interacciones seguras.

5.1.11 Cuando se utiliza para funcionamiento dentro de dominios o entre ellos, es necesario establecer un identificador único para tales conjuntos de reglas de seguridad y se denomina un conjunto convenido de reglas de seguridad (ASSR, *agreed set of security rules*). El identificador ASSR puede ser intercambiado como parte del establecimiento de asociación de seguridad para definir o restringir el SSAA ASSR definido en ese conjunto de reglas de seguridad. Los atributos de SA restantes, si los hubiere, se deben establecer utilizando otros medios, tales como los enumerados en 5.1.2.

5.2 Establecimiento de asociaciones de seguridad para las capas inferiores

5.2.1 Para proteger una comunicación (una SDU sin conexión o una conexión) se debe establecer una asociación de seguridad entre las entidades comunicantes.

5.2.2 La información que forma una SA es una información estática, que puede ser «negociada» cuando se establece la SA y queda fijada mientras dura la asociación, o una información dinámica que puede ser actualizada en una comunicación.

5.2.3 Una SA se puede establecer como un protocolo de capas 1 a 4 de OSI mediante el intercambio de unidades de datos de protocolo (PDU) de asociación de seguridad, o por mecanismos fuera del alcance de las capas inferiores de OSI.

5.2.4 Antes de establecer una SA, cada entidad debe haber preestablecido un conjunto de reglas de seguridad comunes, mutuamente acordadas e inequívocamente identificadas, así como los servicios de seguridad que pueden ser seleccionados.

5.2.5 Si la SA se ha de establecer a través del intercambio de las PDU de asociación de seguridad, se deberá preestablecer también lo siguiente:

- a) una selección inicial de servicios de seguridad, y por consiguiente los mecanismos de seguridad, que se han de aplicar en el establecimiento de una SA;
- b) la información de claves básica necesaria para establecer una SA.

5.2.6 En el establecimiento de una SA, una entidad establece la siguiente información compartida con su par distante que debe permanecer inalterada (es decir estática) mientras dura la asociación:

- a) las SA-ID local y distante;
- b) los servicios de seguridad seleccionados para uso entre las entidades asociadas para las comunicaciones;

NOTA – Los servicios de seguridad que se han de utilizar pueden ser seleccionados entre los servicios de seguridad preestablecidos.
- c) los mecanismos y sus propiedades que se utilizarán como se deduce de los servicios de seguridad seleccionados;
- d) las claves compartidas iniciales para mecanismos de integridad, cifrado y autenticación de una comunicación;
- e) el conjunto de etiquetas de seguridad y direcciones que se pueden utilizar en esta asociación para control de acceso.

5.2.7 Los SA-ID y las claves compartidas [incisos a) y d) anteriores] se deben establecer asociación por asociación. La otra información puede estar preestablecida. Además, como parte del establecimiento de una SA, se debe autenticar la identidad del par distante para proporcionar autenticación de entidad par.

5.2.8 La siguiente información se puede actualizar dinámicamente para cada comunicación:

- a) número(s) secuencial(es) para integridad necesario(s) para datos normales y acelerados en cada sentido;
- b) una etiqueta de seguridad que se selecciona dinámicamente del conjunto estático de etiquetas de seguridad;
- c) la información de nueva clave para los mecanismos de cifrado/integridad en protocolos de seguridad que admiten nuevas claves dentro de una asociación (por ejemplo, el protocolo de seguridad de capa de red en modo conexión).

5.2.9 Para efectuar la autenticación de entidad par o de origen de los datos, es necesario aplicar mecanismos de autenticación para cada comunicación.

5.2.10 En la Figura 1 se ilustran los diferentes atributos de SA que pueden ser establecidos en las distintas etapas de una asociación de seguridad. Los términos preestablecida, estática y dinámica se utilizan en relación con una asociación de seguridad como se describe en los párrafos precedentes del mismo modo. Los términos utilizados y la forma de autenticación son los descritos en los párrafos anteriores.

Preestablecida	Estática	Dinámica
Conjunto convenido de reglas de seguridad Servicios de seguridad posibles Servicios de seguridad iniciales Información de claves básica	SA-ID Claves iniciales Autenticación	ISN Etiqueta de seguridad Información de nueva clave Información de claves básica
Nivel seleccionado de QOS de protección Mecanismo seleccionado Conjunto etiqueta de seguridad/dirección		

Figura 1 – Ilustración de atributos de una asociación de seguridad

5.2.11 Una entidad debe identificar los atributos de SA necesarios utilizando el SA-ID.

5.2.12 Se deberá establecer la SA antes de proteger una comunicación.

5.3 Cierre de la asociación de seguridad

Una SA indicada por un SA-ID se cierra cuando la SA ya no es válida.

Una asociación de seguridad se puede cerrar por los siguientes métodos:

- a) como un protocolo de capas 1 a 4 de OSI mediante el intercambio de unidades de datos de protocolo (PDU) de asociación de seguridad;
- b) mediante mecanismos externos fuera del alcance de las capas inferiores de OSI;
- c) implícitamente, cerrando una conexión (esto se aplica sólo al modo conexión);
- d) implícitamente, cuando expira una clave dentro de la SA.

NOTA – Se ha de tener cuidado en utilizar el método d) mientras dura una clave definida por el número de paquetes enviados/recibidos entre entidades pares, pues en cada par pueden resultar valores significativamente distintos.

Antes de utilizar el método c) anterior, un atributo de la asociación de seguridad debe indicar que la asociación ha de ser cerrada cuando se cierra una conexión que utiliza esa asociación.

5.4 Modificación de atributos en una conexión

Para cada comunicación (una PDU sin conexión o una conexión), sólo se puede establecer una SA.

Durante la existencia de una conexión, los servicios y mecanismos de seguridad utilizados en esa conexión no pueden ser modificados (sin embargo, esto no impide el cambio de claves).

La indicación de utilización de nuevas claves será descrita por el protocolo de seguridad.

6 Repercusión en los protocolos existentes

6.1 Principio general

En principio la influencia de los protocolos de seguridad en los protocolos existentes debe ser mínima.

6.2 Tamaño de SDU sin conexión

Durante la transferencia de datos, según los mecanismos de seguridad seleccionados, la seguridad repercute en el protocolo de capa (N) como sigue:

- a) los datos de usuario (N), y en algunos casos, partes de la información de control de protocolo (N), funcionan por transformaciones criptográficas antes y después de la transmisión. Esto puede cambiar la longitud de los datos de usuario (N).
- b) la información de control de protocolo relacionada con datos de usuario (N) (por ejemplo, identificador de asociación de seguridad, código de comprobación criptográfico) puede necesitar ser transportada por el protocolo (N).

NOTA – Esto tendrá repercusión en el tamaño de datos de usuario máximo definido en 15.2.3 de la Rec. X.213 del CCITT | ISO/CEI 8348 y en la Rec. X.214 del CCITT | ISO/CEI 8072.

6.3 Concatenación de las PDU

Sólo pueden ser concatenadas las PDU que han de ser protegidas en la misma asociación de seguridad.

6.4 Independencia con respecto al algoritmo y a los mecanismos

Los protocolos de seguridad de capa inferior se especifican para que sean independientes del algoritmo. Asimismo, el NLSIP ha adoptado el método de separar las partes del protocolo de seguridad que son dependientes del mecanismo e independientes del mecanismo. Se prevé que los futuros protocolos de seguridad de capa inferior podrán lograr esto utilizando servicios abstractos genéricos para seguridad comunes a las capas superiores e inferiores de OSI.

7 Estructura de PDU de seguridad común

7.1 Se utilizará una estructura de PDU general común para las PDU de datos protegidas en los protocolos de seguridad de capa inferior. Aunque la estructura de PDU general es la misma para todos los protocolos de seguridad de capas inferiores, naturalmente no será idéntica por varias razones, siendo la más obvia las restricciones de formato impuestas por una determinada capa de protocolo.

7.2 Los aspectos comunes de las estructuras de PDU en los protocolos de seguridad de capas inferiores pueden ser:

- a) un valor de comprobación de integridad (ICV, *integrity check value*) en el extremo de la PDU (salvo para cualquier relleno de cifrado, véase más abajo);
- b) el relleno para los mecanismos de cifrado, integridad y confidencialidad del flujo de tráfico puede ser ubicado en campos separados;
- c) un número de longitud variable utilizado para la integridad de la secuencia;

- d) un método flexible para la codificación de los campos que utiliza tipo/longitud/valor para permitir una extensibilidad fácil e imponer restricciones mínimas en el ordenamiento de campos;
- e) la protección de reflexión proporcionada por una bandera en el sentido iniciador a responder de SA protegida.

8 Determinación de los servicios y mecanismos de seguridad

Los servicios de seguridad que serán aplicados por un protocolo de seguridad se determinan como se describe en la cláusula 9. Los mecanismos de seguridad que se aplicarán se determinan, dados los servicios de seguridad seleccionados, mediante la utilización de reglas de seguridad como se describe en la cláusula 10.

9 QOS de protección

La QOS de protección es el grado al cual un proveedor de servicios intenta contrarrestar las amenazas de seguridad utilizando servicios de seguridad aplicados en las capas inferiores.

El tratamiento de los parámetros de servicio de la QOS de protección es un asunto local controlado conforme a la política de seguridad en vigor. La QOS de protección no es negociada entre los usuarios de servicio. Para una comunicación, un usuario de servicio puede indicar al proveedor del servicio sus necesidades de QOS de protección. El proveedor de servicio puede indicar la QOS de protección suministrada al usuario del servicio en una comunicación. La QOS de protección suministrada por el proveedor del servicio no necesita ser igual que la solicitada por el usuario del servicio.

Cualquier intercambio de protocolos de capas inferiores entre sistemas abiertos (denominados intercambios de protocolos «dentro de banda») para transmitir información sobre los servicios de seguridad que se han de seleccionar se transporta en un protocolo de asociación de seguridad que es independiente de la comunicación. Puede ser transportada implícitamente por una etiqueta de seguridad o explícitamente por otros medios.

10 Reglas de seguridad

Habida cuenta de los servicios de seguridad seleccionados, las reglas de seguridad especifican los mecanismos de seguridad que se han de utilizar incluidos todos los parámetros necesarios para el funcionamiento de los mecanismos. En el Anexo A figura un ejemplo ilustrativo de las reglas de seguridad que se pueden considerar convenientes para uso por una comunidad.

Cuando los servicios de seguridad seleccionados son indicados por una etiqueta de seguridad, las reglas de seguridad especifican también la correspondencia de una etiqueta de seguridad con los requisitos de protección indicados.

NOTA – Actualmente, las reglas de seguridad no están normalizadas por el UIT-T | ISO/CEI.

11 Colocación de seguridad en las capas inferiores

Actualmente se definen protocolos de seguridad para utilización en la capa de transporte y en la capa de red [protocolo de seguridad de capa de transporte (TLSP) y protocolo de seguridad de capa de red (NLSP)].

Para comunicaciones en modo conexión, el TLSP funciona conforme a la Rec. UIT-T X.224 | ISO/CEI 8073 (véase la Figura 2). Para comunicaciones en el modo sin conexión, el TLSP funciona conforme a la Rec. UIT-T X.234 | ISO/CEI 8602 (véase la Figura 3).

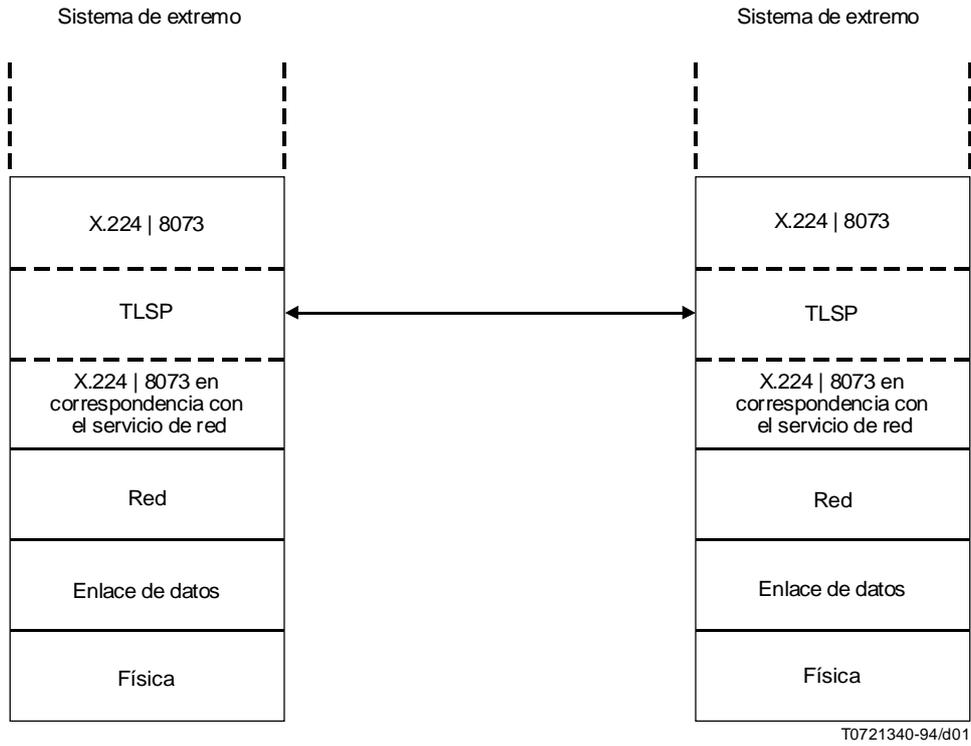


Figura 2 – Ilustración de TLSP que funciona con la Rec. UIT-T X.224 | ISO/CEI 8073

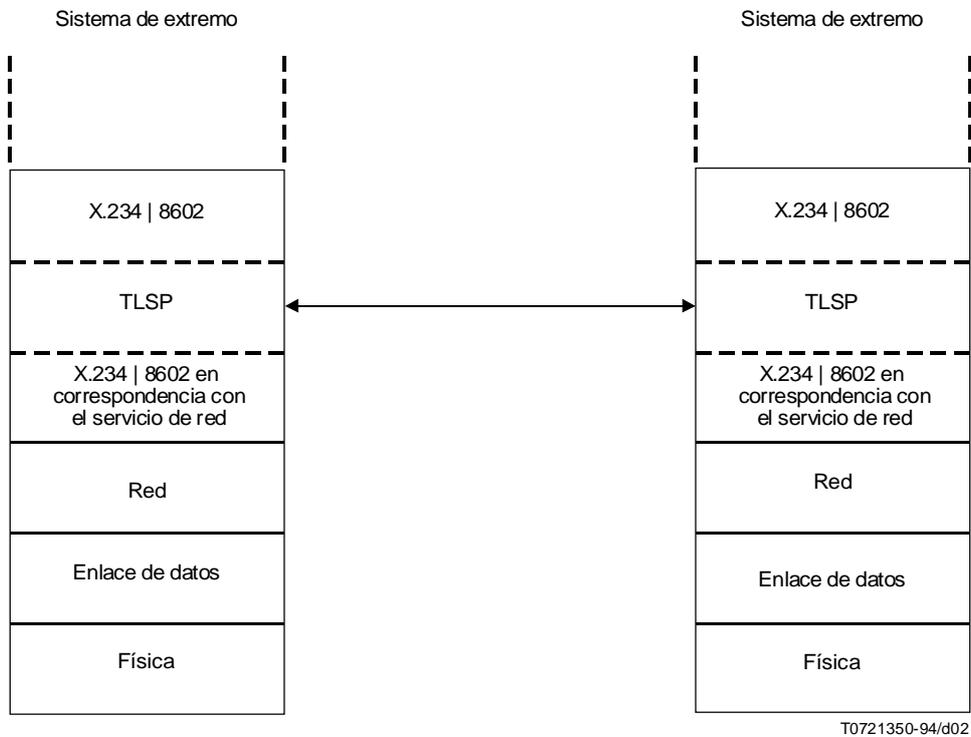


Figura 3 – Ilustración de TLSP que funciona con la Rec. UIT-T X.234 | ISO/CEI 8602

La seguridad en la capa de red puede ser suministrada por un protocolo de seguridad independiente de subred (SNISP) que desempeña un cometido de seguridad independiente de subred además de los cometidos identificados en ISO 8648. Como se describe más adelante, existen varias opciones para las diversas relaciones entre un SNISP como el NLSP y los protocolos que proporcionan los otros cometidos de protocolo de capa de red identificados en ISO 8648.

Para comunicaciones en el modo sin conexión entre sistemas de extremo, el NLSP puede funcionar por encima de protocolos de capa de red «normales». Esto se ilustra en la Figura 4. Se protege así a las unidades de datos de servicio de red.

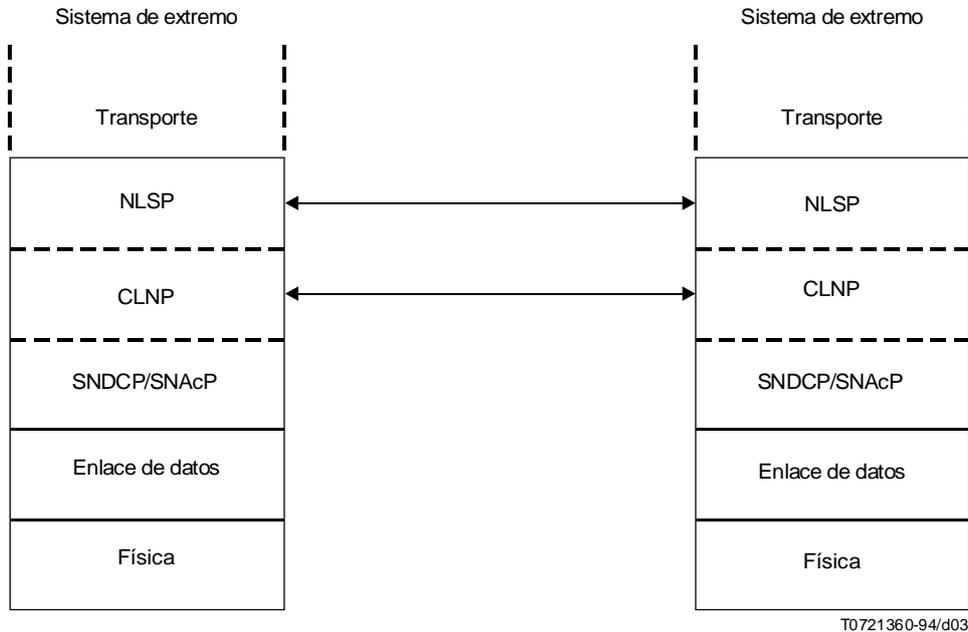


Figura 4 – Ilustración de NLSP-CL entre sistemas de extremo

Alternativamente, para comunicaciones en el modo sin conexión entre dos sistemas de extremo, un sistema de extremo y un sistema intermedio o entre dos sistemas intermedios, el NLSP funciona por debajo del protocolo de red sin conexión (véase la Rec. UIT-T X.233 | ISO/CEI 8473-1) y por encima de un protocolo de convergencia de subred o de un protocolo según la Rec. UIT-T X.233 | ISO/CEI 8473-1. Esto se ilustra en las Figuras 5 y 6. La representación de dos capas de la Rec. UIT-T X.233 | ISO/CEI 8473-1 y una capa NLSP no supone necesariamente máquinas de protocolo separadas. Esto depende de la política de realización local. Se protege así a las unidades de datos de protocolo de red.

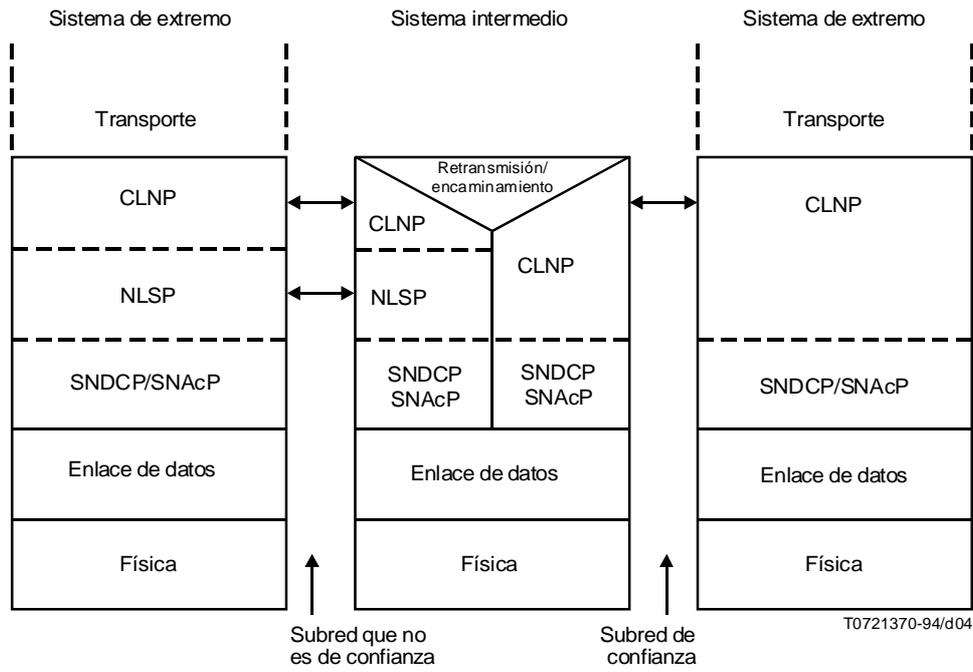


Figura 5 – Ilustración de NLSP-CL con subred que no es de confianza

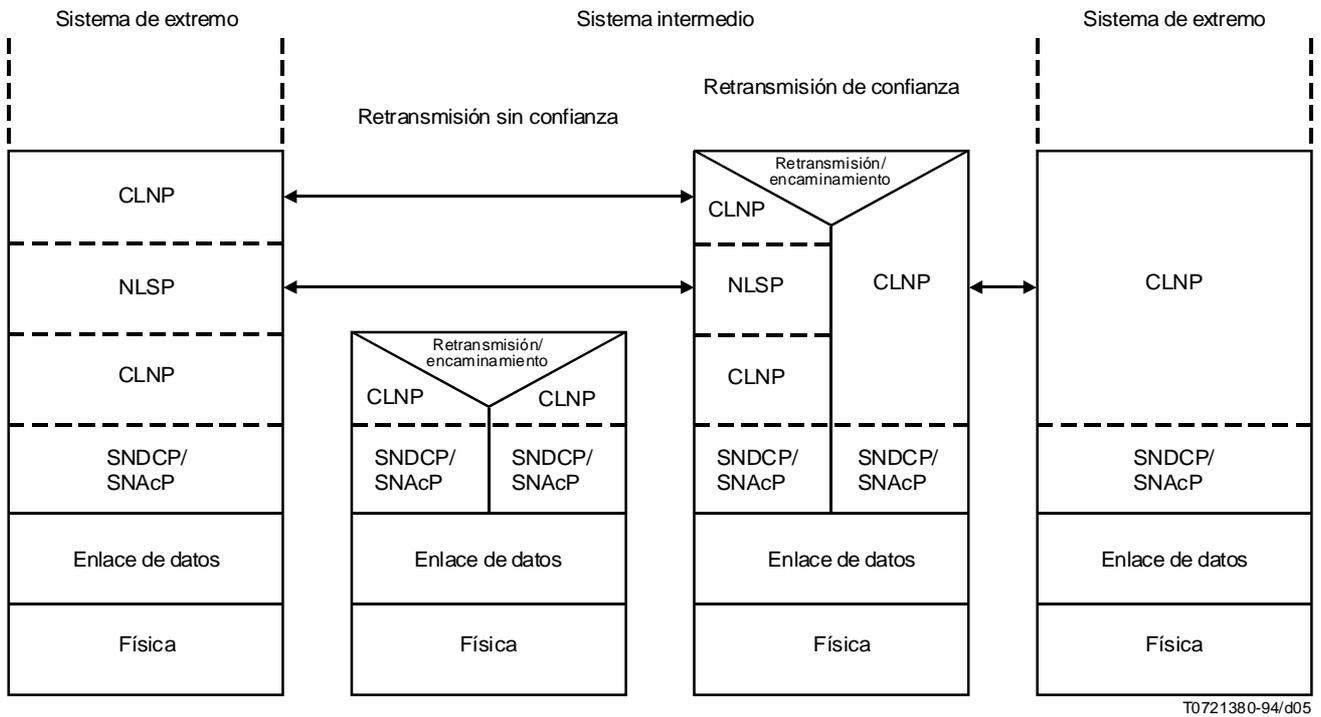


Figura 6 – Ilustración de NLSP-CL con un sistema de retransmisión que no es de confianza

Para comunicaciones en el modo con conexión, el NLSP siempre funciona por encima de un protocolo independiente de subred o de un protocolo de acceso de subred según ISO/CEI 8208. Esto se ilustra en las Figuras 7, 8 y 9. Se protege así a las unidades de datos de servicio de red. El NLSP no tiene que estar ubicado necesariamente en la parte superior de la capa de red.

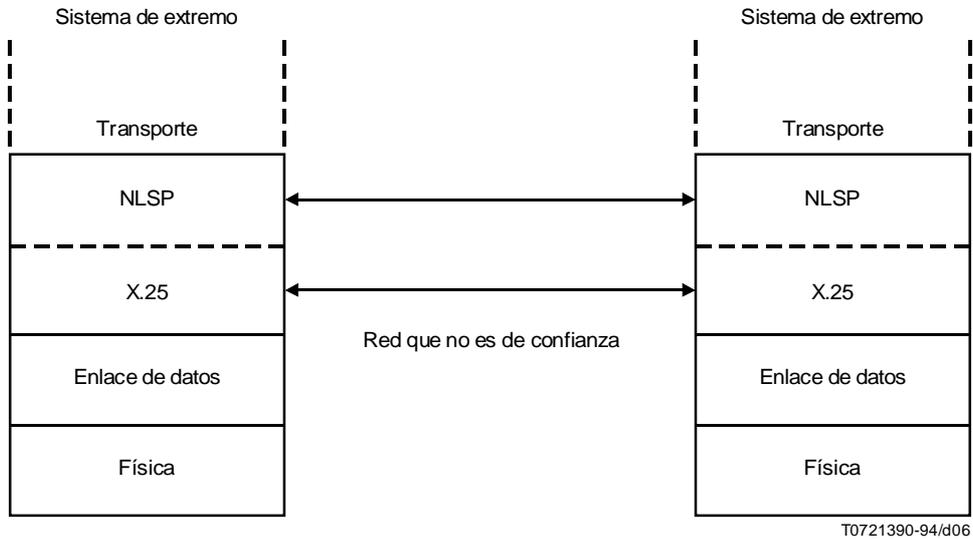


Figura 7 – Ilustración de NLSP-CO entre sistemas de extremo

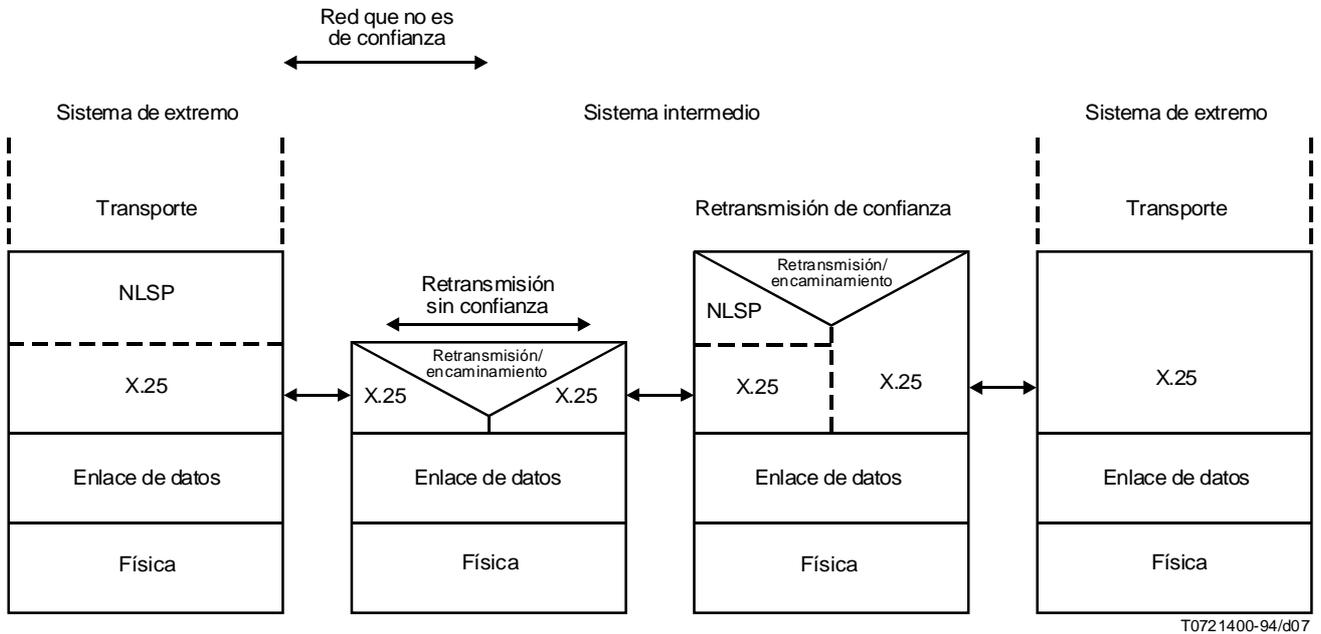
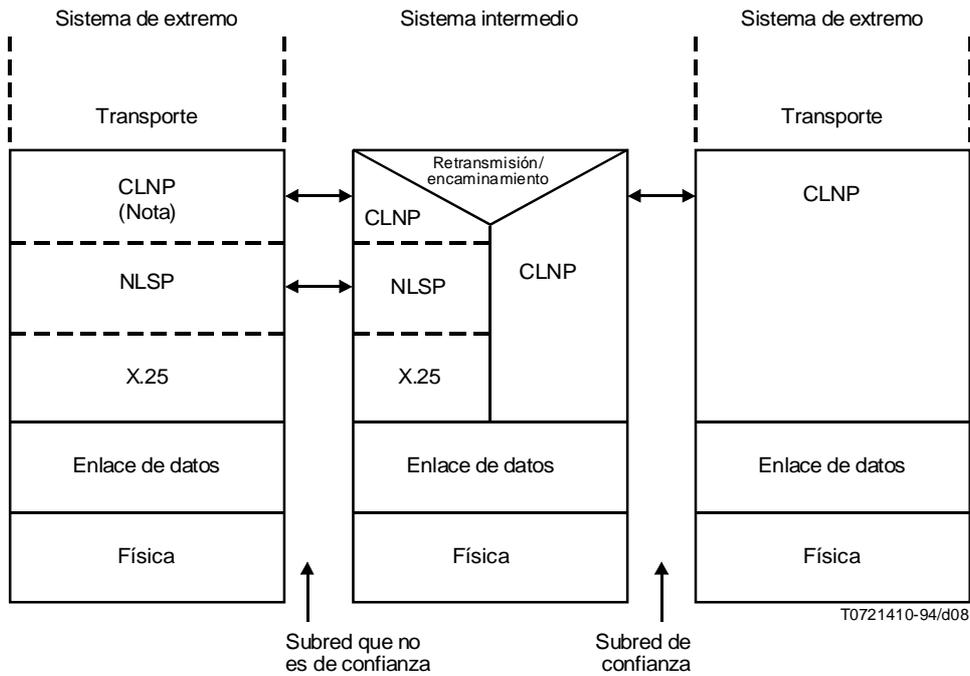


Figura 8 – Ilustración de NLSP-CO con sistema de retransmisión que no es de confianza



NOTA – Incluye una función de convergencia al modo conexión.

Figura 9 – Ilustración de NLSP en un entorno con múltiples redes

Es posible utilizar otras colocaciones no incluidas en este modelo.

Los intercambios del protocolo de encaminamiento entre dominios (IDRP) (*interdomain routing protocol*) (ISO/CEI 10747) se pueden proteger utilizando un NLSP que funciona por debajo del IDRP y por encima del protocolo conforme a la Rec. UIT-T X.233 | ISO/CEI 8473-1 (véase la Figura 10). Esto protege a las unidades de datos de protocolo IDRP.

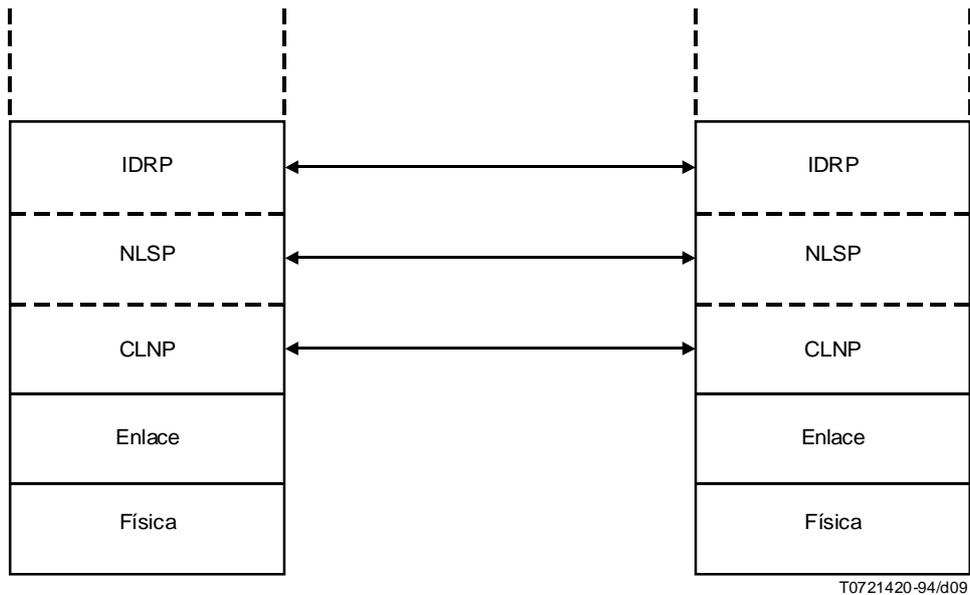


Figura 10 – Ilustración de NLSP que funciona con IDRP

Se puede definir una correspondencia para las primitivas de servicio de red subyacentes del NLSP con el servicio de enlace de datos para emplear un protocolo de capa de enlace como un protocolo de red de zona local (LAN) (*local area network*) definido en ISO/CEI 8802 (véase la Figura 11).

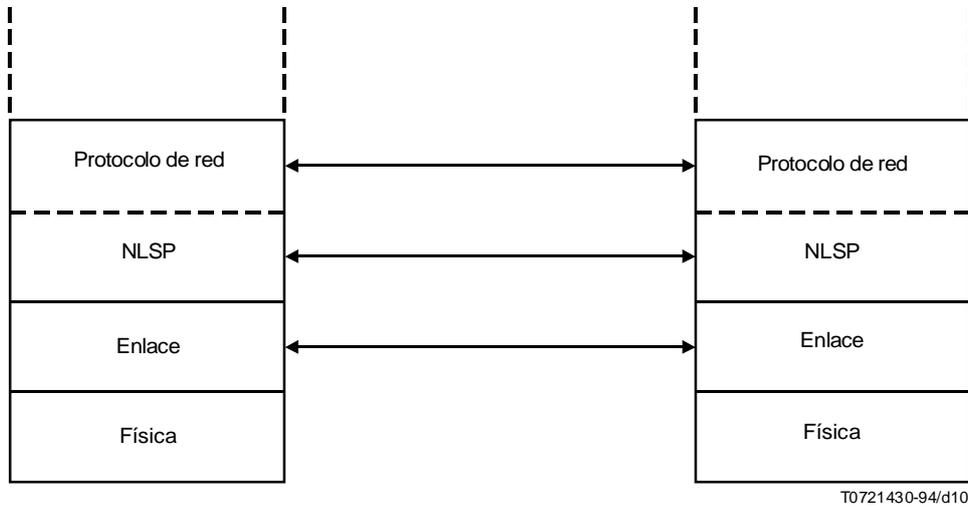


Figura 11 – Ilustración de NLSP que funciona a través de una capa de enlace

La Rec. X.800 del CCITT | ISO 7498-2 requiere la confidencialidad en la capa de enlace de datos. Se necesita un protocolo de seguridad de enlace de datos para proteger las comunicaciones entre puentes de capa 2 en un entorno LAN (véase la Figura 12).

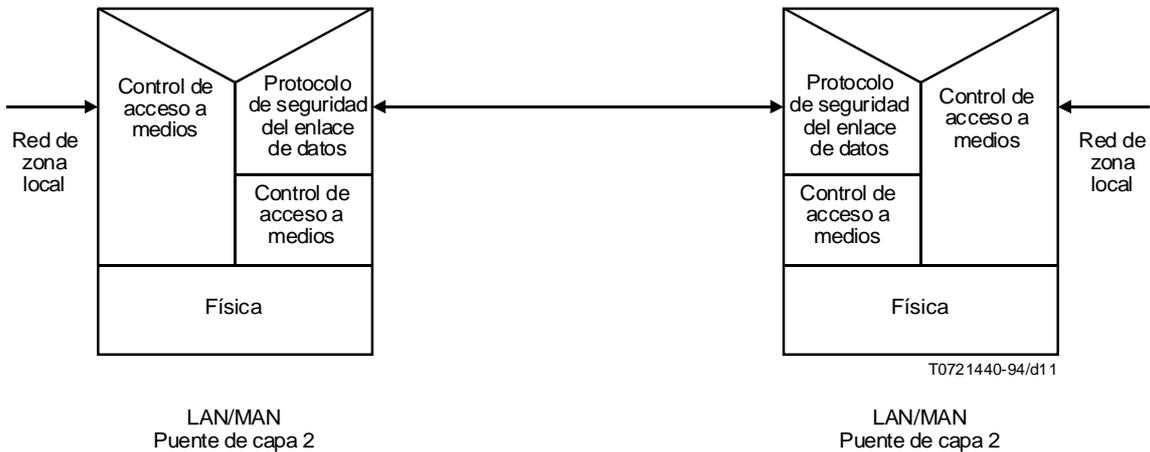


Figura 12 – Ilustración de protocolo de seguridad de la capa de enlace de datos utilizado para proteger la comunicación entre dos puentes

12 Utilización de capa(s) (N-1) para mejorar la seguridad de capa (N)

Al proporcionar funciones de seguridad en una determinada capa, es posible utilizar los servicios de seguridad suministrados por capa(s) de abajo. Los servicios de seguridad globales suministrados al usuario de capa (N) se pueden establecer mediante mecanismos en las capas subyacentes.

13 Etiquetado de seguridad

Se puede utilizar una etiqueta de seguridad para indicar los requisitos de los servicios de seguridad seleccionados (véase la cláusula 9), así como el control de acceso y encaminamiento.

En una asociación de seguridad un par de entidades puede preestablecer un conjunto de etiquetas de seguridad que pueden ser asignadas a unidades de datos de protocolo con conexión/sin conexión entre ellas.

La utilización de etiquetas de seguridad se define como parte de una política de seguridad.

En marcos de seguridad: Parte 3 – Control de acceso, se describe la aplicación de las etiquetas de seguridad para el control de acceso.

El primer campo de una etiqueta de seguridad identificará a la autoridad de seguridad que define la etiqueta. Este identificador será un identificador de objeto (definido en la Rec. X.208 del CCITT | ISO/CEI 8824 sobre ASN.1), codificado con las reglas de codificación básica (véase la Rec. X.208 del CCITT | ISO/CEI 8824).

La estructura general de las etiquetas de seguridad debe estar de acuerdo con el trabajo del SC27 sobre objetos de información de seguridad.

14 Dominios de seguridad

Los dominios de seguridad, definidos en la Rec. UIT-T X.810 | ISO/CEI 10181-1 (visión de conjunto de los marcos de seguridad), no se relacionan directamente con los protocolos entre pares. La utilización de dominios ha de ser considerada en el contexto de la gestión de seguridad.

15 Seguridad de encaminamiento

15.1 El protocolo de seguridad de la capa de red (NLSP) (véase la Rec. UIT-T X.273 | ISO/CEI 11577) se puede utilizar para proteger los intercambios de unidades de datos de protocolo de encaminamiento entre dominios (ISO/CEI 10747) (véase también la cláusula 11 sobre la colocación del IDRP).

15.2 El NLSP (definido en la Rec. X.273 del CCITT | ISO/CEI 11577) no se puede utilizar para soportar la seguridad de intercambios de encaminamiento entre dominios basados en ISO/CEI 10589 (sistema intermedio a sistema intermedio, IS-IS) y en ISO/CEI 9542 (sistema de extremo a sistema intermedio, ES-IS) y no admite comunicaciones multipares. Se puede definir un protocolo normalizado basado en una ampliación de NLSP para la seguridad de los protocolos de intercambio de encaminamiento dentro de dominios IS-IS y ES-IS. Cualquiera de estos protocolos normalizados para la seguridad del intercambio de encaminamiento dentro de dominios IS-IS y ES-IS debe ser independiente de estos protocolos de encaminamiento.

15.3 Se debe señalar que los controles de acceso aplicados a las comunicaciones (por ejemplo, grupos cerrados de usuarios de la Rec. UIT-T X.25 | ISO/CEI 8208, etiquetas de seguridad, NLSP de la Rec. UIT-T X.233 | ISO/CEI 8473-1), pueden hacer las rutas disponibles. Se puede requerir información sobre el estado de seguridad de las rutas para que la información de encaminamiento sea útil en entornos de seguridad.

15.4 Asimismo, se debe considerar las necesidades de encaminamiento para soportar el control de acceso/control de encaminamiento.

NOTA – En la Rec. X.800 del CCITT | ISO 7498-2 se define el control de encaminamiento como: «La aplicación de reglas durante el proceso de encaminamiento con el fin de evitar redes, enlaces o relevadores específicos». El control de encaminamiento podría basarse, por ejemplo, en direcciones, e impedir el encaminamiento de todos los datos en una subred con excepción de determinadas direcciones autorizadas. Como alternativa, el control de encaminamiento se podría basar en etiquetas de seguridad; por ejemplo, los paquetes identificados como «comercial confidencial» no serán encaminados por la red pública.

16 Gestión de seguridad

16.1 Política de seguridad

La siguiente información se establece como parte de los criterios de política de seguridad para seleccionar el servicio y los mecanismos de seguridad en una capa (N) para una entidad (N) dada:

- criterios para establecer los servicios de seguridad seleccionados para una capa (N) incluidos los niveles máximo y mínimo aceptables;
- criterios para la correspondencia de servicios de seguridad seleccionados con los mecanismos y los requisitos de protección subyacentes (es decir, las reglas de seguridad que se describen en la cláusula 10).

Cuando se utilizan etiquetas de seguridad la información se establece como parte de la política de seguridad para la utilización de etiquetas de seguridad (véase la cláusula 13).

La información se establece como parte de la política de seguridad para auditoría de los aspectos de seguridad pertinentes de los protocolos de capa y para suministrar el restablecimiento.

16.2 Gestión de asociaciones de seguridad

La gestión de asociaciones de seguridad se trata en la cláusula 5.

16.3 Gestión de claves

La distribución y selección de claves se puede hacer de una de las siguientes maneras (*métodos*):

- a) como parte del establecimiento de SA;
- b) dentro de un protocolo de seguridad; o
- c) a través de mecanismos fuera del alcance de las capas inferiores de OSI.

16.4 Auditoría de seguridad

La recopilación y análisis de información de auditoría de seguridad se describe en los marcos de seguridad, Parte 7: Auditoría de seguridad (futura Norma ISO/CEI 10181-7).

17 Confidencialidad del flujo de tráfico

El tratamiento de relleno de tráfico no se comprende bien. Se puede proporcionar tres tipos de relleno asociados con la confidencialidad del flujo de tráfico en el entorno del servicio de red con conexión como sigue:

- a) rellenando las PDU de datos de seguridad existentes;
- b) generando PDU de datos de seguridad ficticias;
- c) generando conexiones ficticias con otras entidades pares del NLSP.

Con cada tipo de relleno hay parámetros posibles que deben ser definidos (por ejemplo, todas las PDU deben tener una longitud de 1024 octetos; debe haber una PDU en la conexión cada 500 milisegundos; cuando esta entidad NLSP efectúa una conexión con una determinada entidad NLSP par, estas seis entidades NLSP también deben estar conectadas y se debe intercambiar el mismo volumen de tráfico con ellas). Estos parámetros no son bien comprendidos pero, en los dos primeros casos de relleno, se deben incluir como parte de la asociación de seguridad. Por consiguiente, no es adecuado un atributo booleano. Los tipos de parámetros necesarios requieren ulterior estudio.

18 Directrices para la definición de atributos de SA

Un atributo de SA es un ítem de información requerido para controlar la seguridad de las comunicaciones y su par distante. En la cláusula 5 se describen tres clases diferentes de atributos de SA.

Los atributos de SA requeridos para controlar un protocolo de seguridad se definen como parte del protocolo de seguridad. Esta definición debe incluir:

- a) un término mnemónico utilizado para referirse al atributo en el protocolo de seguridad;
- b) el tipo de datos del atributo;

- c) una descripción de la semántica del atributo;
- d) una descripción de cómo se establece el valor de este atributo.

Muchos de los atributos requeridos para un protocolo de seguridad dependerán de los mecanismos soportados.

Ejemplos de definiciones de atributos de SA son:

- Encipher: Booleano.
 El cifrado se utiliza para suministrar confidencialidad.
 El valor de este atributo está definido por un conjunto convenido de reglas de seguridad dados los servicios de seguridad seleccionados.
- Enc_Alg: Identificador de objeto atribuido según ISO 9979.
 Algoritmo de cifrado.
 El valor de este atributo está definido por un conjunto convenido de reglas de seguridad dados los servicios de seguridad seleccionados.
- Enc_key Forma definida por el conjunto convenido de reglas de seguridad.
 Clave de cifrado.
 Valor establecido por establecimiento de asociaciones de seguridad.

19 Tratamiento de errores

Las acciones que se han de ejecutar cuando se produce un error en un protocolo de seguridad serán determinadas por la política de seguridad local. Las opciones pueden ser:

- descartar la PDU con error;
- emitir PDU de error;
- aplicar procedimientos de reiniciación o de desconexión;
- rellenar un informe de auditoría.

Anexo A

Ejemplo ilustrativo de un conjunto convenido de reglas de seguridad

(Este anexo es parte integrante de la presente Recomendación | Informe técnico)

An Agreed Set of Security Rules (ASSR) establishes the security mechanisms to be used including all parameters needed to define the operation of the mechanism for given Security Services Selected.

ASSR-ID OBJECT IDENTIFIER

SA-ID_Length 4

Services Selected Definition Module

PE Auth: none, low, high
 AC: none, low, high
 Confid: none, low, high
 Integ: none, low, high

Security Label Mapping

Label_Def_Auth XYZ

Label->Sensitivity = Unclass
 implies

PE Auth none, AC none, Confid none, Integ none

Label-Sensitivity = Confidential
 implies

PE Auth low, AC low, Confid low, Integ none

Label-Sensitivity = Secret
 implies

PE Auth high, AC high, Confid high, Integ high

Protection of All Service Parameters

For Security Services Selected: Integ = high or Conf = high

Mechanism Module – Security labels for Access Control

For Security Services Selected: AC = high or Conf = high

Label_Def_Auth XYZ

Explicit indication Yes

Mechanism Module – Integrity Check Value

For Security Services Selected: Integ > none or PE Auth = High
 or Mechanism Security Labels

ICV_Alg_Id XYZ

ICV_Block_size 8 octets

Re-key after 10,000 PDUs

Key distribution mechanism Asymmetric

Mechanism Module – Integrity Sequence Number

For Security Services Selected: Integ = high or Auth = High

ISN_Len 4 octets

Mechanism Module – Encipherment

For Security Services Selected: Conf > low

Enc_Alg_ID XYZ

Mode Chained

Enc_Block_Size 8 octets

Re-key after	1,000 PDUs
Key distribution mechanism	Asymmetric

Mechanism Module – No Header

For Security Services Selected: Conf = low and Integ = none and not Label mechanism

Mechanism Module – Connection Authentication

For Security Services Selected: AC > Low or PE Auth > Low

Enc_Alg_ID	XYZ
------------	-----

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

PKC_Alg_ID	RSA
------------	-----