UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT X.800

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

REDES DE COMUNICACIÓN DE DATOS: INTERCONEXIÓN DE SISTEMAS ABIERTOS (ISA); SEGURIDAD, ESTRUCTURA Y APLICACIONES

ARQUITECTURA DE SEGURIDAD DE LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT

Recomendación X.800

Ginebra, 1991

PREFACIO

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

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

La Recomendación X.800 ha sido preparada por la Comisión de Estudio VII y fue aprobada por el procedimiento de la Resolución N.º 2 el 22 de marzo de 1991.

NOTA DEL CCITT

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

Recomendación X.800

ARQUITECTURA DE SEGURIDAD DE LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT [1)]

0 Introducción

La Recomendación X.200 del CCITT describe el modelo de referencia básico para la interconexión de sistemas abiertos (ISA). Dicha Recomendación establece un marco para coordinar el desarrollo de Recomendaciones existentes y futuras para la interconexión de sistemas.

El objetivo de la ISA es permitir la interconexión de sistemas de computador heterogéneos de modo que puedan lograrse comunicaciones útiles entre procesos de aplicación. En distintos momentos, deben establecerse controles de seguridad para proteger la información intercambiada entre los procesos de aplicación. Estos controles deben hacer que el costo de obtener o modificar los datos de una manera indebida sea mayor que el valor potencial de esta acción, o hacer que el tiempo requerido para obtener los datos de una manera indebida sea tan largo que pierdan su valor.

Esta Recomendación define los elementos arquitecturales generales relacionados con la seguridad que pueden aplicarse adecuadamente en las circunstancias en que se requiere la protección de la comunicación entre sistemas abiertos. Establece, en el marco del modelo de referencia, directrices y restricciones para mejorar las Recomendaciones existentes o formular nuevas Recomendaciones en el contexto de ISA con el fin de permitir comunicaciones seguras y proporcionar así un enfoque coherente de la seguridad en la ISA.

Para comprender la presente Recomendación será útil una información básica sobre seguridad. Por tanto, se aconseja a los lectores que no estén muy familiarizados con la seguridad que lean primero el anexo A.

La presente Recomendación amplía el modelo de referencia (Recomendación X.200) para abarcar los aspectos de seguridad que son elementos arquitecturales generales de protocolos de comunicación, pero que no se examinan en el modelo de referencia.

1 Alcance y campo de aplicación

La presente Recomendación:

a) da una descripción general de los servicios de seguridad y mecanismos conexos, que pueden ser proporcionados por el modelo de referencia; y

b) define las posiciones, dentro del modelo de referencia, en que pueden proporcionarse los servicios y mecanismos.

La presente Recomendación amplía el campo de aplicación de la Recomendación X.200, para tratar comunicaciones seguras entre sistemas abiertos.

Se han identificado servicios y mecanismos básicos de seguridad y su ubicación apropiada para todas las capas del modelo de referencia básico. Además, se han establecido las relaciones arquitecturales entre los servicios y mecanismos de seguridad y el modelo de referencia. Pueden necesitarse otras medidas de seguridad en los sistemas extremos (o sistemas de extremo), instalaciones y organizaciones. Estas medidas se emplean en diversos contextos de aplicación. La definición de los servicios de seguridad necesarios para soportar estas medidas adicionales de seguridad está fuera del alcance de esta Recomendación.

---

1) La Recomendación X.800 y la Norma ISO 7498-2 (Information Processing Systems – Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture) están técnicamente alineadas.

Las funciones de seguridad ISA se relacionan solamente con los aspectos visibles de un trayecto de comunicación que permite a los sistemas extremos realizar una transferencia segura de información entre ellos. La seguridad de ISA no se relaciona con las medidas de seguridad necesarias en los sistemas extremos, instalaciones y organizaciones, salvo cuando dichas medidas tienen repercusiones sobre la elección y posición de servicios de seguridad visibles en ISA. Estos últimos aspectos de seguridad pueden normalizarse pero no en el ámbito de las Recomendaciones relativas a la ISA.

La presente Recomendación amplía los conceptos y principios definidos en la Recomendación X.200 sin modificarlos. No es una especificación de realización, ni una base para evaluar la conformidad de realizaciones existentes.

2 Referencias

Rec. X.200 – Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT.

ISO 7498 – Information processing systems – Open systems interconnection – Basic Reference Model (1984).

ISO 7498-4 – Information processing systems – Open systems interconnection – Basic Reference Model –Part 4: Management framework (1989).

ISO 7498/AD1 – Information processing systems – Open system interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission (1987).

ISO 8648 – Information processing systems – Open systems interconnection – Internal organization of the Network Layer (1988).

3 Definiciones y abreviaturas

3.1 La presente Recomendación se basa en los conceptos desarrollados en la Recomendación X.200 del CCITT y utiliza los siguientes términos definidos en ella:

a) conexión (N);

b) transmisión de datos (N);

c) entidad (N);

d) facilidad (N);

e) capa (N);

f) sistema abierto;

g) entidades pares;

h) protocolo (N);

j) unidad de datos de protocolo (N);

k) relevo (o retransmisión) (N);

l) encaminamiento;

m) secuenciación;

n) servicio (N);

p) unidad de datos de servicio (N);

q) datos de usuario (N);

r) subred;

s) recurso ISA; y

t) sintaxis de transferencia.

3.2 Esta Recomendación utiliza los siguientes términos de las Recomendaciones/Normas internacionales citadas en las referencias.

Transmisión en modo sin conexión (Norma ISO 7498/AD1)

Sistema extremo (Recomendación X.200/Norma ISO 7498)

Funciones de relevo y de encaminamiento (Norma ISO 8648)

Base de Información de Gestión (BIG) (Norma ISO 7498-4)

Además, se utilizan las siguientes abreviaturas:

ISA Interconexión de sistemas abiertos;

UDS Unidad de datos de servicio;

BIGS Base de información de gestión de seguridad;

BIG Base de información de gestión.

3.3 A los efectos de esta Recomendación, son aplicables las siguientes definiciones:

3.3.1 **control de acceso**

Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada.

3.3.2 **lista de control de acceso**

Lista de entidades, con sus derechos de acceso, que están autorizadas a tener acceso a un recurso.

3.3.3 **imputabilidad**

Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.

3.3.4 **amenaza activa**

Amenaza de un cambio deliberado y no autorizado del estado del sistema.

Nota – Como ejemplos de amenazas activas relativas a la seguridad cabe citar: la modificación de mensajes, la reproducción de mensajes, la inserción de mensajes espurios, la usurpación de identidad (o impostura) de una entidad autorizada y la negación (o denegación) de servicio.

3.3.5 **auditoría**

Véase «auditoría de seguridad».

3.3.6 **registro de auditoría**

Véase «registro de auditoría de seguridad».

3.3.7 **autenticación**

Véanse «autenticación de origen de los datos» y «autenticación de entidad par».

Nota – En la presente Recomendación, el término «autenticación» no se utiliza en relación con la integridad de los datos; en su lugar se utiliza el término «integridad de los datos».

3.3.8 **información de autenticación**

Información utilizada para establecer la validez de una identidad alegada.

3.3.9 **intercambio de autenticación**

Mecanismo destinado a garantizar la identidad de una entidad mediante intercambio de información.

3.3.10 **autorización**

Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.3.11 **disponibilidad**

Propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.3.12 **capacidad**

Testigo (token) utilizado como identificador de un recurso de modo que la posesión del testigo confiera derechos de acceso a ese recurso.

3.3.13 **canal**

Trayecto de transferencia de la información.

3.3.14 **criptograma** (o texto cifrado)

Datos producidos mediante cifrado. El contenido semántico de los datos resultantes no está disponible.

Nota – Un criptograma puede ser cifrado, de nuevo, para obtener un criptograma supercifrado.

3.3.15 **texto claro**

Datos inteligibles, cuyo contenido semántico está disponible.

3.3.16 **confidencialidad**

Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.3.17 **credenciales**

Datos que se transfieren para establecer la identidad alegada de una entidad.

3.3.18 **criptoanálisis** (o análisis criptográfico)

Análisis de un sistema criptográfico y/o sus entradas y salidas para derivar variables confidenciales y/o datos sensibles, incluido texto claro.

3.3.19 **valor de comprobación criptográfico**

Información que se obtiene realizando una transformación criptográfica (véase criptografía) sobre una unidad de datos.

Nota – El valor de comprobación puede obtenerse en uno o más pasos y es el resultado de una función matemática de la clave y una unidad de datos. Suele utilizarse para verificar la integridad de una unidad de datos.

3.3.20 **criptografía**

Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado.

Nota – La criptografía determina los métodos utilizados en el cifrado y descifrado. Un ataque a los principios, medios y métodos criptográficos es criptoanálisis.

3.3.21 **integridad de los datos**

Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.3.22 **autenticación del origen de los datos**

Confirmación de que la fuente de los datos recibidos es la alegada.

3.3.23 **descifrado**

Operación inversa de un cifrado reversible correspondiente.

3.3.24 **decripción**

Véase descrifrado.

3.3.25 **negación (o denegación) de servicio**

Prevención de acceso autorizado a recursos o retardo deliberado de operaciones críticas desde el punto de vista del tiempo.

3.3.26 **firma digital**

Datos añadidos a una unidad de datos, o transformación criptográfica (véase criptografía) de una unidad de datos que permite al recibiente de la unidad de datos probar la fuente y la integridad de la unidad de datos y proteger contra la falsificación (por ejemplo, por el recibiente).

3.3.27 **cifrado**

Transformación criptográfica de datos (véase criptografía) para producir un criptograma o texto cifrado.

Nota – El cifrado puede ser irreversible, en cuyo caso no puede realizarse el proceso de descifrado correspondiente.

3.3.28 **encripción**

Véase «cifrado».

3.3.29 **cifrado de extremo a extremo**

Cifrado de datos en el interior o en el sistema extremo fuente, cuyo descifrado correspondiente se produce sólo en el interior o en el sistema extremo de destino (véase también «cifrado enlace por enlace»).

3.3.30 **política de seguridad basada en la identidad**

Política de seguridad basada en las identidades y/o atributos de los usuarios, de un grupo de usuarios o entidades que actúan en nombre de los usuarios y en los recursos/objetos a que se accede.

3.3.31 **integridad**

Véase «integridad de los datos».

3.3.32 **clave**

Secuencia de símbolos que controla las operaciones de cifrado y descifrado.

3.3.33 **gestión de claves**

Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad.

3.3.34 **cifrado enlace por enlace**

Aplicación individual del cifrado a datos en cada enlace de un sistema de comunicación. (Véase también «cifrado de extremo a extremo».)

Nota – El cifrado enlace por enlace entraña que los datos estén en forma de texto claro en las entidades relevadoras.

3.3.35 **detección de manipulación**

Mecanismo que se utiliza para detectar si una unidad de datos ha sido modificada, sea accidental o intencionalmente.

3.3.36 **usurpación de identidad** (o impostura)

Pretención de una entidad de pasar por una entidad diferente.

3.3.37 **notarización**

Registro de datos por un tercero de confianza que permite la ulterior seguridad de la exactitud de sus características, tales como contenido, origen, fecha, entrega.

3.3.38 **amenaza pasiva**

Amenaza de revelación no autorizada de la información sin modificar el estado del sistema.

3.3.39 **contraseña**

Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres.

3.3.40 **autenticación de entidad par**

Corroboración de que una entidad par en una asociación es la pretendida.

3.3.41 **seguridad física**

Medidas adoptadas para proporcionar la protección física de los recursos contra amenazas deliberadas o accidentales.

3.3.42 **política**

Véase «política de seguridad».

3.3.43 **privacidad**

Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada.

Nota – Como este término se relaciona con el derecho de las personas, no puede ser muy preciso y su uso debe evitarse, salvo como un motivo para exigir seguridad.

3.3.44 **repudio**

Negación de una de las entidades implicadas en una comunicación de haber participado en toda la comunicación o en parte de ella.

3.3.45 **control de encaminamiento**

Aplicación de reglas durante el proceso de encaminamiento con el fin de elegir o evitar redes, enlaces o relevadores específicos.

3.3.46 **política de seguridad basada en reglas**

Política de seguridad basada en reglas globales impuestas a todos los usuarios. Estas reglas suelen depender de una comparación de la sensibilidad de los recursos a los que se accede con los atributos correspondientes de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios.

3.3.47 **auditoría de seguridad**

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

3.3.48 **registro de auditoría de seguridad**

Datos recogidos que pueden usarse para efectuar una auditoría de seguridad.

3.3.49 **etiqueta de seguridad**

Marca vinculada a un recurso (que puede ser una unidad de datos) que denomina o designa los atributos de seguridad de dicho recurso.

Nota – La marca y/o vinculación puede ser explícita o implícita.

3.3.50 **política de seguridad**

Conjunto de criterios para la prestación de servicios de seguridad (véanse también «política de seguridad basada en la identidad» y «política de seguridad basada en reglas»).

Nota – Una política de seguridad completa tratará necesariamente muchos aspectos que están fuera del ámbito de ISA.

3.3.51 **servicio de seguridad**

Servicio proporcionado por una capa de sistemas abiertos comunicantes, que garantiza la seguridad adecuada de los sistemas y de la transferencia de datos.

3.3.52 **protección selectiva de los campos**

Protección de ciertos campos específicos dentro de un mensaje que ha de transmitirse.

3.3.53 **sensibilidad**

Característica de un recurso relativa a su valor o importancia y eventualmente a su vulnerabilidad.

3.3.54 **firma**

Véase «firma digital».

3.3.55 **amenaza**

Violación potencial de la seguridad.

3.3.56 **análisis del tráfico**

Inferencia de información a partir de la observación de flujos de tráfico (presencia, ausencia, cantidad, sentido y frecuencia).

3.3.57 **confidencialidad del flujo de tráfico**

Servicio de confidencialidad que ofrece protección contra el análisis de tráfico.

3.3.58 **relleno de tráfico**

Generación de instancias de comunicación espurias, de unidades de datos/o datos espurios en las unidades de datos.

3.3.59 **funcionalidad de confianza**

Funcionalidad percibida como correcta con respecto a algunos criterios, por ejemplo, los establecidos por una política de seguridad.

4 Notación

La notación utilizada para designar las capas es la misma definida en la Recomendación X.200 del CCITT.

El término «servicio» cuando no tiene otra calificación, se utiliza para referirse a un servicio de seguridad.

5 Descripción general de los servicios y mecanismos de seguridad

5.1 *Visión de conjunto*

En este punto se examinan los servicios de seguridad que se incluyen en la arquitectura de seguridad de ISA y los mecanismos que realizan estos servicios. Los servicios de seguridad descritos a continuación son servicios de seguridad básicos. En la práctica, se invocarán en las capas apropiadas y en combinaciones apropiadas, usualmente con servicios y mecanismos que no son de ISA, para satisfacer la política de seguridad y/o las exigencias de los usuarios. Pueden utilizarse mecanismos de seguridad particulares para realizar combinaciones de los servicios de seguridad básicos. En las realizaciones prácticas de los sistemas pueden utilizarse combinaciones particulares de los servicios de seguridad básica invocación directa.

5.2 *Servicios de seguridad*

Se considera que los siguientes servicios de seguridad pueden proporcionarse facultativamente en el marco del modelo de referencia de ISA. Los servicios de autenticación requieren información de autenticación que comprende información almacenada localmente y datos que se transfieren (credenciales) para facilitar la autenticación.

5.2.1 *Autenticación*

Estos servicios proporcionan la autenticación de una entidad par comunicante y de la fuente de datos, según se describe a continuación.

5.2.1.1 *Autenticación de entidad par*

Cuando este servicio, es proporcionado por la capa (N), corrobora a la entidad (N + 1) que la entidad par es la entidad (N + 1) pretendida.

Este servicio se utiliza en el establecimiento de la fase de transferencia de datos de una conexión, o a veces durante ésta, para confirmar la identidad de una o varias entidades conectadas a una o varias otras entidades. Este servicio da confianza, en el momento de utilización solamente, en que una entidad no está tratando de usurpar otra identidad o la reproducción no autorizada de una conexión anterior. Son posibles esquemas de autenticación de entidad par unilaterales y mutuos, con o sin comprobación en tiempo real, y pueden proporcionar diversos grados de protección.

5.2.1.2 *Autenticación del origen de los datos*

Este servicio, cuando es prestado por la capa (N), corrobora a una entidad (N + 1) que la fuente de los datos es la entidad par (N + 1) pretendida.

El servicio de autenticación del origen de los datos confirma la fuente de una unidad de datos. Este servicio no proporciona protección contra la duplicación o modificación de las unidades de datos.

5.2.2 *Control de acceso*

Este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante ISA. Estos recursos a los que se tiene acceso mediante protocolos de ISA, pueden ser o no de ISA. Este servicio de protección puede aplicarse a diversos tipos de acceso a un recurso (por ejemplo, el uso de un recurso de comunicaciones, la lectura, la escritura, o la supresión de un recurso de información; la ejecución de un recurso de procesamiento) o a todos los accesos a un recurso.

El control de acceso se efectuará de conformidad con las diversas políticas de seguridad (véase el § 6.2.1.1).

5.2.3 *Confidencialidad de los datos*

Estos servicios proporcionan la protección de los datos contra la revelación no autorizada, según se describe a continuación.

5.2.3.1 *Confidencialidad de los datos en modo con conexión*

Este servicio proporciona la confidencialidad de todos los datos de usuario (N) en una conexión (N).

Nota – Según el uso y la capa, puede no ser apropiado proteger todos los datos, por ejemplo, los datos expeditados o los datos de una petición de conexión.

5.2.3.2 *Confidencialidad de los datos en modo sin conexión*

Este servicio proporciona la confidencialidad de todos los datos de usuario (N) en una UDS (N) en modo sin conexión.

5.2.3.3 *Confidencialidad de campos seleccionados*

Este servicio proporciona la confidencialidad de campos seleccionados en los datos de usuario (N) en el curso de una conexión (N) o en una unidad de datos de servicio (N) en modo sin conexión.

5.2.3.4 *Confidencialidad del flujo de tráfico*

Este servicio proporciona la protección de la información que pudiera derivarse de la observación de los flujos de tráfico.

5.2.4 *Integridad de los datos*

Estos servicios contrarrestan las amenazas activas y pueden ser de una de las formas descritas a continuación.

Nota – El uso del servicio de autenticación de la entidad par al comienzo de la conexión y del servicio de integridad de los datos mientras dura la conexión puede confirmar conjuntamente la fuente de todas las unidades de datos transferidas a la conexión, la integridad de estas unidades de datos y puede además proporcionar la detección de duplicación de unidades de datos, por ejemplo, mediante el uso de números de secuencia.

5.2.4.1 *Integridad en modo con conexión con recuperación*

Este servicio proporciona la integridad de todos los datos de usuario (N) en una conexión (N) y detecta cualquier modificación, inserción, supresión o reproducción de cualquier dato dentro de una secuencia completa de UDS (con tentativa de recuperación).

5.2.4.2 *Integridad en modo con conexión sin recuperación*

Igual que el § 5.2.4.1 pero sin tentativa de recuperación.

5.2.4.3 *Integridad de campos seleccionados en modo con conexión*

Este servicio proporciona la integridad de campos seleccionados en los datos de usuario (N) de una UDS (N) transferida por una conexión y adopta la forma de una indicación que permite saber si los campos seleccionados han sido modificados, insertados, suprimidos o reproducidos.

5.2.4.4 *Integridad en modo sin conexión*

Cuando este servicio es prestado por la capa (N), proporciona la seguridad de la integridad a la entidad (N + 1) solicitante.

Este servicio proporciona la integridad de una sola UDS en modo sin conexión y puede adoptar la forma de una indicación que permite saber si una UDS recibida ha sido modificada. Además, puede proporcionarse una forma limitada de detección de reproducción.

5.2.4.5 *Integridad de campos seleccionados en modo sin conexión*

Este servicio proporciona la integridad de campos seleccionados dentro de una sola UDS en modo sin conexión y adopta la forma de una indicación que permite saber si los campos seleccionados han sido modificados.

5.2.5 *No repudio*

Este servicio puede adoptar una de las formas siguientes o ambas.

5.2.5.1 *No repudio con prueba del origen*

Se proporciona al destinatario de los datos la prueba del origen de los datos. Esto lo protegerá contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.

5.2.5.2 *No repudio con prueba de la entrega*

Se proporciona al expedidor de los datos la prueba de la entrega de los datos. Esto lo protegerá contra cualquier tentativa ulterior del destinatario de negar que ha recibido los datos o su contenido.

5.3 *Mecanismos de seguridad específicos*

Los siguientes mecanismos pueden incorporarse en la capa (N) apropiada para proporcionar algunos de los servicios descritos en el § 5.2.

5.3.1 *Cifrado*

5.3.1.1 El cifrado puede proporcionar la confidencialidad de la información de datos o del flujo de tráfico y puede desempeñar una función en varios otros mecanismos de seguridad o complementarlos, según se describe en los puntos siguientes.

5.3.1.2 Los algoritmos de cifrado pueden ser reversibles o irreversibles. Los algoritmos de cifrado reversibles pueden ser de dos tipos:

a) cifrado simétrico (es decir, con clave secreta), en el cual el conocimiento de la clave del cifrado implica el conocimiento de la clave de descifrado y viceversa;

b) cifrado asimétrico (por ejemplo, con clave pública), en el cual el conocimiento de la clave del cifrado no implica el conocimiento de la clave de descifrado, o viceversa. Algunas veces las dos claves de este sistema se denominan «clave pública» y «clave privada».

Los algoritmos de cifrado irreversibles pueden utilizar o no una clave. Cuando utilizan una clave, ésta puede ser pública o secreta.

5.3.1.3 La existencia de un mecanismo de cifrado implica el uso de un mecanismo de gestión de claves, salvo en el caso de algunos algoritmos de cifrado irreversibles. En el § 8.4 figuran algunas directrices sobre metodología de gestión de claves.

5.3.2 *Mecanismos de firma digital*

Estos mecanismos definen dos procedimientos:

a) firma de una unidad de datos; y

b) verificación de una unidad de datos firmada.

El primer proceso utiliza información que es privada (es decir, única y confidencial) del firmante. El segundo proceso utiliza procedimientos de información que están disponibles públicamente, pero a partir de los cuales no puede deducirse cuál es la información privada del firmante.

5.3.2.1 El proceso de firma conlleva un cifrado de la unidad de datos o la producción de un valor de control criptográfico de la unidad de datos, utilizando la información privada del firmante como una clave privada.

5.3.2.2 El proceso de verificación conlleva la utilización de los procedimientos e información públicos para determinar si la firma se produjo con la información privada del firmante.

5.3.2.3 La característica esencial del mecanismo de firma es que la firma sólo puede producirse utilizando la información privada del firmante. De este modo, cuando se verifica la firma, puede probarse subsiguientemente a una tercera parte (por ejemplo, a un juez o árbitro), en cualquier momento, que sólo el poseedor único de la información privada pudo haber producido la firma.

5.3.3 *Mecanismos de control de acceso*

5.3.3.1 Estos mecanismos pueden utilizar la identidad autenticada de una entidad o información sobre la entidad (tal como la lista de miembros de un conjunto conocido de entidades) o capacidades de la entidad, para determinar y aplicar los derechos de acceso de la entidad. Si la entidad intenta utilizar un recurso no autorizado, o un recurso autorizado con un tipo impropio de acceso, la función de control de acceso rechazará la tentativa y puede informar además el incidente a los efectos de generar una alarma y/o anotarlo en el registro de auditoría de seguridad. La notificación al expedidor del rechazo de acceso para una transmisión de datos en modo sin conexión puede proporcionarse solamente como resultado de controles de accesos impuestos en el origen.

5.3.3.2 Los mecanismos de control de acceso pueden basarse, por ejemplo, en la utilización de uno o más de los elementos siguientes:

a) Bases de información de control de acceso, donde se mantienen los derechos de acceso de entidades pares. Esta información debe ser mantenida por centros de autorización o por la entidad a la que se accede, y puede tener la forma de una lista de control de acceso o de una matriz de estructura jerárquica o distribuida. Esto presupone que se ha asegurado la autenticación de la entidad par.

b) Información de autenticación como contraseñas, cuya posesión y presentación ulterior son la prueba de la autorización de la entidad que efectúa el acceso.

c) Capacidades, cuya posesión y presentación ulterior son la prueba del derecho a acceder a la entidad o recurso definido por la capacidad.

   Nota – Una capacidad debe ser inusurpable y debe transmitirse de una manera fiable.

d) Etiquetas de seguridad, que cuando están asociadas con una entidad, pueden utilizarse para conceder o negar el acceso, en general de acuerdo con una política de seguridad.

e) Hora del intento de acceso.

f) Ruta del intento de acceso, y

g) Duración del acceso.

5.3.3.3 Pueden aplicarse mecanismos de control de acceso en cualquiera de los dos extremos de una asociación de comunicaciones y/o cualquier punto intermedio.

Los controles de acceso aplicados en el origen con cualquier punto intermedio se utilizan para determinar si el expedidor está autorizado a comunicar con el destinatario y/o a utilizar los recursos de comunicaciones requeridos.

En una transmisión de datos en modo sin conexión, los requisitos de los mecanismos de control de acceso de la entidad par en el destino, deben conocerse con prioridad en el origen, y deben registrarse en la base de informaciones de gestión de seguridad (véanse los § 6.2 y 8.1).

5.3.4 *Mecanismos de integridad de los datos*

5.3.4.1 La integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un solo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. En general, se utilizan diferentes mecanismos para proporcionar estos dos tipos de servicios de integridad, aunque no es práctica la provisión del segundo sin el primero.

5.3.4.2 La determinación de la integridad de una sola unidad de datos entraña dos procesos, uno en la entidad expedidora y otro en la entidad receptora. La entidad expedidora añade a una unidad de datos una cantidad que es una función de los propios datos. Esta cantidad puede ser una información suplementaria, tal como un código de control de bloque o un valor de control criptográfico, y puede estar cifrada. La entidad receptora genera una cantidad correspondiente y la compara con la cantidad recibida para determinar si los datos han sido modificados en tránsito. Este mecanismo por sí solo no ofrecerá protección contra la reproducción de una sola unidad de datos. En las capas apropiadas de la arquitectura, la detección de una manipulación puede conducir a una acción de recuperación (por ejemplo, una retransmisión o una corrección de error) en esa capa o en otra superior.

5.3.4.3 Para la transferencia de datos en modo con conexión, la protección de la integridad de una secuencia de unidades de datos (es decir, la protección contra errores de secuenciación, pérdida, reproducción, inserción o modificación de datos) requiere además alguna forma de ordenación explícita, como la numeración de secuencias, el estampado de la hora o el encadenamiento criptográfico.

5.3.4.4 Para la transmisión de datos en modo sin conexión, el estampado de la hora puede utilizarse para proporcionar una forma limitada de protección contra la reproducción de unidades de datos individuales.

5.3.5 *Mecanismo de intercambio de autentificación*

5.3.5.1 Algunas de las técnicas que pueden aplicarse a los intercambios de autenticación son:

a) utilización de información de autenticación, como contraseñas, suministradas por una entidad expedidora y verificadas, por la entidad receptora;

b) técnicas criptográficas; y

c) uso de características y/o propiedades de la entidad.

5.3.5.2 Los mecanismos pueden incorporarse en la capa (N) para proporcionar autenticación de la entidad par. Si el mecanismo no logra autenticar la entidad, el resultado será el rechazo o la terminación de la conexión y puede causar también una anotación en el registro de auditoría de seguridad y/o un informe a un centro de gestión de seguridad.

5.3.5.3 Cuando se utilizan técnicas criptográficas, éstas pueden combinarse con protocolos de «toma de contacto» como protección contra la repetición (es decir, asegurar el funcionamiento en tiempo real).

5.3.5.4 Las elecciones de técnicas de intercambio de autenticación dependerán de las circunstancias en las cuales habrá que utilizarlas con:

a) estampado de la hora y relojes sincronizados;

b) dos o tres tomas de contacto (para autenticación unilateral y mutua respectivamente); y

c) servicios de no repudio, mediante firma digital y mecanismos de notarización.

5.3.6 *Mecanismo de relleno de tráfico*

Pueden utilizarse mecanismos de relleno de tráfico para proporcionar diversos niveles de protección contra análisis del tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad.

5.3.7 *Mecanismo de control de encaminamiento*

5.3.7.1 Las rutas pueden elegirse dinámicamente o por acuerdo previo con el fin de utilizar sólo subredes, relevadores o enlaces físicamente seguros.

5.3.7.2 Al detectar ataques de manipulación persistentes, los sistemas extremos pueden dar instrucciones al proveedor del servicio de red que establezca una conexión por una ruta diferente.

5.3.7.3 La política de seguridad puede prohibir que los datos que transportan ciertas etiquetas de seguridad pasen a través de ciertas subredes, relevadores o enlaces. Asimismo, el iniciador de una conexión (o el expedidor de una unidad de datos en modo sin conexión) puede especificar prohibiciones de encaminamiento en las que se indica que se eviten determinadas subredes, enlaces o relevadores.

5.3.8 *Mecanismo de notarización*

5.3.8.1 Pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino, mediante la provisión de un mecanismo de notarización. La seguridad es proporcionada por una tercera parte que actúa como notario, en el que las entidades comunicantes tienen confianza y que mantiene la información necesaria para proporcionar la garantía requerida de una manera verificable. Cada instancia de comunicación puede utilizar la firma digital, el cifrado y los mecanismos de integridad, según sea apropiado, para el servicio que es proporcionado por el notario. Cuando se invoca este mecanismo de notarización, los datos se comunican entre las entidades comunicantes por las instancias de comunicación protegidas y el notario.

5.4 *Mecanismos de seguridad pervasivos*

En este punto se describen varios mecanismos que no son específicos a un servicio particular. Por tanto, en el § 7, no se describen explícitamente como que forman parte de una capa determinada. Algunos mecanismos de seguridad pervasivos pueden considerarse como aspectos de gestión de seguridad (véase también el § 8). En general, la importancia de estos mecanismos está directamente relacionada con el nivel de seguridad requerido.

5.4.1 *Funcionalidad de confianza*

5.4.1.1 La funcionalidad de confianza puede utilizarse para ampliar el campo de aplicación o para establecer la eficacia de otros mecanismos de seguridad. Toda funcionalidad que proporciona directamente mecanismos de seguridad o que permite el acceso a estos mecanismos deberá ser digna de confianza.

5.4.1.2 Los procedimientos utilizados para asegurar que puede confiarse en determinados soportes físicos y soportes lógicos están fuera del alcance de esta Recomendación y, en todo caso, varían según el nivel de amenaza percibida y el valor de la información que ha de protegerse.

5.4.1.3 En general, estos procedimientos son costosos y difíciles de aplicar. Los problemas pueden minimizarse eligiendo una arquitectura que permita realizar funciones de seguridad en módulos que puedan estar separados de las funciones no relacionadas con la seguridad o proporcionadas por éstas.

5.4.1.4 Toda protección de asociaciones por encima de la capa en la cual se aplica la protección debe ser proporcionada por otros medios, por ejemplo, por una funcionalidad de confianza apropiada.

5.4.2 *Etiquetas de seguridad*

5.4.2.1 Los recursos que comprenden elementos de datos pueden tener asociadas etiquetas de seguridad, por ejemplo, para indicar un nivel de sensibilidad. A menudo es necesario transportar la etiqueta de seguridad apropiada con datos en tránsito. Una etiqueta de seguridad puede ser un dato suplementario asociado a los datos transferidos o puede estar implícita; por ejemplo, puede ser la consecuencia de la utilización de una clave específica para cifrar los datos o puede resultar del contexto de los datos, como la fuente o la ruta. Las etiquetas de seguridad explícitas deben ser claramente identificables, para poder verificarlas de manera apropiada. Además, deben estar vinculadas de una manera segura a los datos con los cuales están asociadas.

5.4.3 *Detección de eventos*

5.4.3.1 La detección de eventos relativos a la seguridad comprende la detección de violaciones aparentes de seguridad y puede incluir también la detección de eventos «normales» tales como el acceso logrado (o «log on»). Los eventos relativos a la seguridad pueden ser detectados por entidades, dentro de la ISA, que comprenden mecanismos de seguridad. La especificación de lo que constituye un evento es actualizada por la gestión del tratamiento de eventos (véase el § 8.3.1). La detección de los diversos eventos vinculados a la seguridad puede provocar, por ejemplo, una o varias de las acciones siguientes:

a) informe local del evento;

b) informe a distancia del evento;

c) registro (cronológico, «logging») del evento (véase el § 5.4.3); y

d) acción de recuperación (véase el § 5.4.4).

Ejemplos de eventos relativos a la seguridad son:

a) una violación específica de la seguridad;

b) un evento específico seleccionado; y

c) un rebasamiento en la cuenta de un cierto número de ocurrencias.

5.4.3.2 La normalización en este campo tomará en consideración la transmisión de informaciones pertinentes para el informe y el registro de eventos y la definición sintáctica y semántica que ha de utilizarse para la transmisión de informes y registros de eventos.

5.4.4 *Registro de auditoría de seguridad*

5.4.4.1 Los registros de auditoría de seguridad proporcionan un mecanismo de seguridad valioso dado que hacen posible detectar e investigar potencialmente las violaciones de seguridad permitiendo una auditoría de seguridad posterior. Una auditoría de seguridad es un estudio independiente y un examen de las anotaciones y de las actividades del sistema para probar la idoneidad de los controles, asegurar la coherencia con la política establecida y con los procedimientos de explotación, ayudar a evaluar los daños y recomendar modificaciones de los controles, de la política y de los procedimientos. Una auditoría de seguridad necesita la anotación de informaciones relativas a la seguridad en un registro de auditoría de seguridad, así como el análisis y la producción de informes a partir de las anotaciones que figuran en un registro de auditoría de seguridad. El registro o anotación se considera como un mecanismo de seguridad y se describe en este punto. El análisis y la producción de informes se consideran como una función de gestión de seguridad (véase el § 8.3.2).

5.4.4.2 La recopilación de información para el registro de auditoría de seguridad puede adaptarse a diversas necesidades especificando el tipo o tipos de eventos relativos a la seguridad que han de registrarse (por ejemplo, violaciones aparentes de la seguridad o ejecución de operaciones correctas).

La existencia conocida de un registro de auditoría de seguridad puede servir de elemento disuasivo para ciertas fuentes potenciales de ataques a la seguridad.

5.4.4.3 En un análisis del registro de auditoría de seguridad de ISA se tendrá en cuenta el tipo de información que podrá registrarse, facultativamente, las condiciones en las cuales esta información deberá registrarse y la definición sintáctica y semántica que ha de utilizarse para intercambiar información de registro de auditoría de seguridad.

5.4.5 *Recuperación de seguridad*

5.4.5.1 La recuperación de seguridad trata las peticiones provenientes de mecanismos tales como las funciones de tratamiento y de gestión de los eventos y realiza acciones de recuperación como resultado de la aplicación de un conjunto de reglas. Estas acciones de recuperación pueden ser de tres tipos:

a) inmediatas;

b) temporales; y

c) a largo plazo.

Por ejemplo:

Las acciones inmediatas pueden provocar un aborto inmediato de las operaciones, como una desconexión.

Las acciones temporales pueden producir la invalidación temporal de una entidad.

Las acciones a largo plazo pueden ser la inclusión de una entidad en una «lista negra» o el cambio de una clave.

5.4.5.2 Los elementos que han de normalizarse comprenden los protocolos para las acciones de recuperación y la gestión de recuperación de seguridad (véase el § 8.3.3).

5.5 *Ilustración de la relación entre servicios y mecanismos de seguridad*

El cuadro 1/X.800 muestra los mecanismos, solos o combinados con otros, que a veces se consideran apropiados para suministrar cada servicio. Este cuadro presenta una visión de conjunto de estas relaciones y no es definitivo. Los servicios y mecanismos indicados en este cuadro se describen en los § 5.2 y 5.3. Las relaciones se describen más detalladamente en el § 6.

CUADRO 1/X.800

Ilustración de la relación entre servicios de seguridad y mecanismos de seguridad

Mecanismo / Servicio	Cifrado	Firma digital	Control de acceso	Integridad de datos	Intercambio de automatización	Relleno de tráfico	Control de encaminamiento	Notarización
Autenticación de la entidad par	S	S	·	·	S	·	·	·
Autenticación del origen de los datos	S	S	·	·	·	·	·	·
Servicio de control de acceso	·	·	S	·	·	·	·	·
Confidencialidad en modo con conexión	S	·	·	·	·	·	S	·
Confidencialidad en modo sin conexión	S	·	·	·	·	·	S	·
Confidencialidad de campos seleccionados	S	·	·	·	·	·	·	·
Confidencialidad del flujo de tráfico	S	·	·	·	·	S	S	·
Integridad en modo con conexión con recuperación	S	·	·	S	·	·	·	·
Integridad en modo con conexión sin recuperación	S	·	·	S	·	·	·	·
Integridad de campos seleccionados en modo con conexión	S	·	·	S	·	·	·	·
Integridad en modo sin conexión	S	S	·	S	·	·	·	·
Integridad de campos seleccionados en modo sin conexión por campos selectivos	S	S	·	S	·	·	·	·
No repudio. Origen	·	S	·	S	·	·	·	S
No repudio. Entrega	·	S	·	S	·	·	·	S

· Se considera que el mecanismo no es apropiado.

S Sí: El mecanismo es apropiado, por sí mismo o en combinación con otros mecanismos.

Nota – En algunos casos, el mecanismo proporciona más de lo que es necesario para el servicio en cuestión, no obstante lo cual podrá utilizarse.

6 Relaciones entre servicios, mecanismos y capas

6.1 *Principios de estratificación de los servicios y mecanismo de seguridad*

6.1.1 Se han utilizado los siguientes principios para determinar la asignación de servicios de seguridad a las capas y a la consiguiente ubicación de mecanismos de seguridad en las capas:

a) el número de maneras alternativas de proporcionar un servicio debe reducirse al mínimo;

b) es aceptable construir sistemas seguros proporcionando servicios de seguridad en más de una capa;

c) la funcionalidad adicional requerida para seguridad no debe duplicar innecesariamente las funciones de ISA existentes;

d) debe evitarse la violación de la independencia de las capas;

e) debe minimizarse la cantidad de funcionalidad de confianza;

f) cuando una entidad dependa de un mecanismo de seguridad proporcionado por una entidad en una capa inferior, las capas intermedias deben construirse de manera que no pueda violarse la seguridad;

g) siempre que sea posible, las funciones de seguridad suplementarias de una capa deben definirse de modo que no se impida la realización en forma de uno o varios módulos autónomos;

h) debe poder aplicarse la presente Recomendación a los sistemas abiertos constituidos por sistemas extremos que contienen las siete capas y a los sistemas relevadores.

6.1.2 Puede ser necesario modificar las definiciones de servicio en cada capa para satisfacer peticiones de servicio de seguridad si los servicios solicitados se proporcionan en esa capa o en una inferior.

6.2 *Modelo de invocación, de gestión y de utilización de servicios (N) protegidos*

Este punto debe leerse junto con el § 8 que contiene una presentación general de los aspectos de gestión de seguridad. Se tiene el propósito de que los servicios y mecanismos de seguridad puedan ser activados por la entidad de gestión a través del interfaz de gestión y/o por la invocación del servicio.

6.2.1 *Determinación de prestaciones de protección para una instancia de comunicación*

6.2.1.1 *Generalidades*

En este punto se describe la invocación de la protección de instancias de comunicación en modo con conexión y en modo sin conexión. En el caso de una comunicación en modo con conexión, los servicios de protección se solicitan/conceden generalmente en la fase de establecimiento de la conexión. En el caso de una invocación de servicio en el modo sin conexión, la protección se solicita/concede para cada caso de petición de un servicio en el modo sin conexión.

Para simplificar la descripción siguiente, el término «petición de servicio» se utilizará en el sentido del establecimiento de una conexión o de una petición de servicio en el modo sin conexión. La invocación de protección de los datos elegidos puede realizarse pidiendo una protección de campos seleccionados. Por ejemplo, esto puede realizarse estableciendo varias conexiones, cada una con un tipo o un nivel de protección diferente.

Esta arquitectura de seguridad admite toda una gama de políticas de seguridad, incluidas las basadas en reglas, las basadas en identidades y las que son una combinación de ambas. La arquitectura de seguridad admite también la protección impuesta administrativamente, la protección seleccionada dinámicamente y una combinación de ambas.

6.2.1.2 *Petición de servicio*

Para cada petición de servicio (N), la entidad (N + 1) puede pedir la protección de seguridad deseada, fijada como objetivo (la protección de seguridad nominal). La petición de servicio (N) especificará los servicios de seguridad junto con los parámetros y toda la información pertinente suplementaria (como la información de sensibilidad y/o las etiquetas de seguridad) para lograr la protección de seguridad nominal.

Antes de cada instancia de comunicación, la capa (N) debe ganar acceso a la Base de Información de Gestión de Seguridad (BIGS) (véase el § 8.1). La BIGS contiene información sobre las peticiones de protección impuestas administrativamente asociadas con la entidad (N + 1). Se requiere funcionalidad de confianza para aplicar estos requisitos de seguridad impuestos administrativamente.

La realización de prestaciones de seguridad en el curso de una instancia de comunicación en modo con conexión puede requerir la negociación de los servicios de seguridad que se necesitan. Los procedimientos requeridos para negociar mecanismos y parámetros pueden ejecutarse como un procedimiento aparte, o como una parte integrante del procedimiento normal de establecimiento de la conexión.

Cuando la negociación se efectúa como un procedimiento aparte, los resultados del acuerdo (es decir, sobre el tipo de mecanismos de seguridad y los parámetros de seguridad que son necesarios para proporcionar estos servicios de seguridad) se introducen en la base de información de gestión de seguridad (véase el § 8.1).

Cuando la negociación se efectúa como una parte integrante del procedimiento normal de establecimiento de la conexión, los resultados de la negociación entre las entidades (N) se almacenarán temporalmente en la BIGS. Antes de la negociación, cada entidad (N) ganará acceso a la BIGS con el fin de obtener la información requerida para la negociación.

La capa (N) rechazará la petición de servicio si ésta viola los requisitos impuestos administrativamente que están registrados en la BIGS para la entidad (N + 1).

La capa (N) añadirá también a los servicios de protección solicitados cualesquiera servicios de seguridad que están definidos en la BIGS como obligatorios para obtener la protección de seguridad nominal.

Si la entidad (N + 1) no especifica una protección de seguridad nominal, la capa (N) seguirá una política de seguridad de acuerdo con las informaciones de la BIGS. Esta podrá ser la de proseguir la comunicación con una protección de seguridad por defecto dentro de la gama definida para la entidad (N + 1) en la BIGS.

6.2.2 *Prestación de servicios de protección*

Después de haber determinado la combinación de los requisitos de seguridad impuestos administrativamente y de los seleccionados dinámicamente, según se describe en el § 6.2.1, la capa (N) intentará lograr, como mínimo, la protección nominal. Esta se logrará aplicando uno de estos dos métodos, o ambos:

a) invocación directa de mecanismos de seguridad dentro de la capa (N), y/o

b) petición de servicios de protección de la capa (N – 1). En este caso, el alcance de la protección debe extenderse hasta el servicio (N) mediante una combinación de funcionalidad de confianza y/o mecanismos de seguridad específicos en la capa (N).

Nota – Esto no implica necesariamente que todas las funcionalidades de la capa (N) deben ser de confianza.

Por tanto, la capa (N) determina si es capaz de lograr la protección nominal solicitada. Si no es capaz de lograrla, no se produce ninguna instancia de comunicación.

6.2.2.1 *Establecimiento de una conexión (N) protegida*

A continuación se trata la prestación de servicios dentro de la capa (N) (en lugar de contar con los servicios (N – 1)).

En algunos protocolos, para lograr una protección nominal satisfactoria la secuencia de operaciones es un factor de importancia capital.

a) *Control de acceso de salida*

   La capa (N) puede imponer controles de acceso de salida, es decir, puede determinar localmente (a partir de la BIGS) si puede intentarse el establecimiento de la conexión (N) protegida o si ésta está prohibida.

b) *Autenticación de entidad par*

   Si la protección nominal incluye autenticación de la entidad par, o si se sabe (por medio de la BIGS) que la entidad (N) de destino exigirá la autenticación de la entidad par, debe efectuarse un intercambio de autenticación. Esto puede requerir procedimientos bidireccionales o tridireccionales de toma de contacto para proporcionar autenticación unilateral o mutua, según se necesite.

   Algunas veces, el intercambio de autenticación puede integrarse en los procedimientos usuales de establecimiento de la conexión (N). En ciertas circunstancias, el intercambio de autenticación puede realizarse separadamente del establecimiento de la conexión (N).

c) *Servicio de control de acceso*

La entidad (N) de destino o las entidades intermedias pueden imponer restricciones de control de acceso. Si un mecanismo de control de acceso distante requiere información específica, la entidad (N) iniciadora suministra esta información dentro del protocolo de capa (N) o por canales de gestión.

d) *Confidencialidad*

Si se ha elegido un servicio de confidencialidad total o selectiva, debe establecerse una conexión (N) protegida. Esto debe incluir el establecimiento de la clave o claves de trabajo apropiadas y la negociación de los parámetros criptográficos para la conexión, lo que puede haberse hecho por acuerdo previo en el intercambio de autenticación, o mediante un protocolo aparte.

e) *Integridad de los datos*

Si se ha seleccionado la integridad de todos los datos de usuario (N), con o sin recuperación, o la integridad de campos seleccionados, debe establecerse una conexión (N) protegida. Esta puede ser la misma conexión establecida para proporcionar el servicio de confidencialidad y puede proporcionar autenticación. Las consideraciones relativas a una conexión protegida aplicables al servicio de confidencialidad son válidas para el servicio de integridad de los datos.

f) *Servicios de no repudio*

Si se ha elegido el servicio de no repudio con prueba del origen, deben establecerse los parámetros criptográficos apropiados, o una conexión protegida con una entidad de notarización.

Si se ha elegido el servicio de no repudio con prueba de la entrega, deben establecerse los parámetros apropiados (que son diferentes de los requeridos para el servicio de no repudio con prueba del origen), o una conexión protegida con una entidad de notarización.

Nota – El establecimiento de la conexión (N) protegida puede fracasar por falta de acuerdo sobre los parámetros criptográficos (incluida posiblemente la no posesión de las claves apropiadas) o debido al rechazo de un mecanismo de control de acceso.

6.2.3 *Operación de una conexión (N) protegida*

6.2.3.1 Durante la fase de transferencia de datos de una conexión (N) protegida, deben prestarse los servicios de protección negociados.

Los elementos siguientes serán visibles en la frontera del servicio (N):

a) autenticación de la entidad par (a intervalos);

b) protección de campos seleccionados, y

c) informe de ataque activo (por ejemplo, cuando se ha producido una manipulación de datos y el servicio que se presta es «integridad en modo con conexion sin recuperación», véase el § 5.2.4.2).

Además, puede necesitarse:

a) anotación en el registro de auditoría de seguridad, y

b) detección y tratamiento de eventos.

6.2.3.2 *Los servicios que son sensibles a la aplicación selectiva son:*

a) confidencialidad;

b) integridad de los datos (posiblemente con autenticación); y

c) no repudio (por el receptor o por el expedidor).

Nota 1 – Se sugieren dos técnicas para marcar los elementos de datos seleccionados para la aplicación de un servicio. La primera conlleva la utilización de una tipificación fuerte. Se prevé que la capa de presentación reconocerá ciertos tipos que requieren la aplicación de ciertos servicios de protección. La segunda supone alguna forma de indicación (por ejemplo, mediante banderas) de los elementos de datos individuales a los cuales deben aplicarse servicios de protección especificados.

Nota 2 – Se supone que una razón para proporcionar la aplicación selectiva de servicios de no repudio debe provenir del siguiente escenario. Se produce alguna forma de diálogo de negociación sobre una asociación antes de que ambas entidades (N) acuerden que una versión final de un ítem de datos es mutuamente aceptable. En ese punto, el recibiente deseado puede pedir al expedidor que aplique servicios de no repudio (con prueba del origen y de la entrega) a la versión final acordada del ítem de datos. El expedidor pide y obtiene estos servicios, transmite el ítem de datos y recibe subsiguientemente notificación de que el ítem de datos ha sido recibido con acuse por el destinatario.Los servicios de no repudio garantizan al originador y al recibiente del ítem de datos que éste ha sido transmitido correctamente.

Nota 3 – Ambos servicios de no repudio (es decir, con prueba del origen y de la entrega) son invocados por el originador.

6.2.4 *Provisión de transmisión de datos protegida en modo sin conexión*

No todos los servicios de seguridad disponibles en los protocolos para las transmisiones en modo con conexión están disponibles en los protocolos para las transmisiones en modo sin conexión. Concretamente, debe proporcionarse protección contra la supresión, inserción y reproducción, si es necesario, en las capas superiores en modo con conexión. Puede suministrarse una protección limitada contra la reproducción por un mecanismo de estampado de hora. Además, algunos otros servicios de seguridad no son capaces de proporcionar el mismo grado de seguridad que puede obtenerse por los protocolos para las transmisiones en modo con conexión.

Los servicios de protección apropiados para la transmisión de datos en modo sin conexión son los siguientes:

a) autenticación de la entidad par (véase el § 5.2.1.1);

b) autenticación del origen de los datos (véase el § 5.2.1.2);

c) servicio de control de acceso (véase el § 5.2.2);

d) confidencialidad en el modo sin conexión (véase el § 5.2.3.2);

e) confidencialidad para campos seleccionados (véase el § 5.2.3.3);

f) integridad en el modo sin conexión (véase el § 5.2.4.4);

g) integridad de campos seleccionados en modo sin conexión (véase el § 5.2.4.5); y

h) no repudio, origen (véase el § 5.2.5.1).

Los servicios se proporcionan mediante cifrado, mecanismos de firma, mecanismos de control de acceso, mecanismos de encaminamiento, mecanismos de integridad de los datos y/o mecanismos de notarización (véase el § 5.3).

El originador de una transmisión de datos en modo sin conexión tendrá que asegurar que su UDS única contiene toda la información requerida para que sea aceptable en el destino.

7 Ubicación de los servicios y mecanismos de seguridad

En este punto se definen los servicios de seguridad que han de proporcionarse en el marco del modelo de referencia básico de ISA y se esboza la manera en la cual han de realizarse. La prestación de cualquier servicio de seguridad es facultativa, según las necesidades.

Cuando en este punto se indica que un servicio de seguridad específico es proporcionado facultativamente por una capa determinada, ese servicio de seguridad se proporciona mediante mecanismos de seguridad que funcionan dentro de esa capa, a menos que se indique otra cosa. Como se expresa en el § 6, muchas capas ofrecerán prestar servicios de seguridad particulares. Es posible que estas capas no proporcionen siempre los servicios de seguridad por ellas mismas, sino que pueden utilizar los servicios de seguridad apropiados suministrados en capas inferiores. Aun cuando no se proporcionen servicios de seguridad dentro de una capa, puede ser necesario modificar las definiciones de servicio de esa capa para poder pasar peticiones de servicios de seguridad a una capa inferior.

Nota 1 – Los mecanismos de seguridad pervasivos no se tratan en este punto (véase el § 5.4).

Nota 2 – La elección de la posición de los mecanismos de cifrado para las aplicaciones se trata en el anexo C.

7.1 *Capa física*

7.1.1 *Servicios*

Los únicos servicios de seguridad proporcionados en la capa física, individualmente o combinados, son los siguientes:

a) confidencialidad en modo con conexión, y

b) confidencialidad del flujo de tráfico.

El servicio de confidencialidad del flujo de tráfico adopta dos formas:

1) confidencialidad total del flujo de tráfico, que puede proporcionarse solamente en ciertas circunstancias, por ejemplo, transmisión bidireccional simultánea, síncrona, punto a punto, y

2) confidencialidad limitada del flujo de tráfico, que se puede proporcionar para otros tipos de transmisión, por ejemplo, transmisión asíncrona.

Estos servicios de seguridad están limitados a amenazas pasivas y pueden aplicarse a comunicaciones punto a punto o a comunicaciones multipares.

7.1.2 *Mecanismos*

El cifrado total de un tren de datos es el principal mecanismo de seguridad en la capa física.

Una de las formas de cifrado, aplicable únicamente en la capa física, es la seguridad de transmisión (es decir, una seguridad de espectro ensanchado).

La protección de la capa física es suministrada por medio de un dispositivo de cifrado que funciona de manera transparente. El objetivo de la protección de la capa física es proteger todo el tren binario de datos del servicio físico y suministrar la confidencialidad del flujo de tráfico.

7.2 *Capa de enlace de datos*

7.2.1 *Servicios*

Los únicos servicios de seguridad proporcionados en la capa de enlace de datos son:

a) confidencialidad en modo con conexión, y

b) confidencialidad en modo sin conexión.

7.2.2 *Mecanismos*

El mecanismo de cifrado se utiliza para proporcionar los servicios de seguridad en la capa de enlace de datos (véase el anexo C).

La funcionalidad adicional de protección de seguridad de la capa de enlace de datos se realiza antes de las funciones normales de capa para la transmisión y después de estas funciones para la recepción, es decir, los mecanismos de seguridad se basan en, y utilizan, todas las funciones normales de la capa.

Los mecanismos de cifrado de la capa de enlace de datos son sensibles al protocolo de la capa de enlace de datos.

7.3 *Capa de red*

La capa de red está organizada internamente para proporcionar protocolos que realizan las siguientes operaciones:

a) acceso a subred;

b) convergencia dependiente de la subred;

c) convergencia independiente de la subred; y

d) relevo y encaminamiento.

7.3.1 *Servicios*

Los servicios de seguridad que puede proporcionar el protocolo que realiza las funciones de acceso a subred asociado con la prestación del servicio de red de ISA son los siguientes:

a) autenticación de entidad par;

b) autenticación del origen de los datos;

c) servicio de control de acceso;

d) confidencialidad en modo con conexión;

e) confidencialidad en modo sin conexión;

f) confidencialidad del flujo de tráfico;

g) integridad en modo con conexión sin recuperación; y

h) integridad en modo sin conexión.

Estos servicios de seguridad pueden prestarse individualmente o combinados. Los servicios de seguridad que pueden ser proporcionados por el protocolo que realiza las operaciones de relevo y encaminamiento asociadas con la prestación de servicio de red ISA, de sistema extremo a sistema extremo, son iguales a los proporcionados por el protocolo que realiza las operaciones de acceso a subredes.

7.3.2 *Mecanismos*

7.3.2.1 Los protocolos que realizan el acceso a subred y las operaciones de relevo y encaminamiento asociadas con la presentación del servicio de red de ISA de sistema extremo a sistema extremo utilizan mecanismos de seguridad idénticos. El encaminamiento se efectúa en esta capa y, por tanto, el control de encaminamiento está situado en esta capa. Los servicios de seguridad identificados se proporcionan como sigue:

a) el servicio de autenticación de entidad par se proporciona por una combinación adecuada de intercambios de autenticación derivados criptográficamente o protegidos, mecanismos de intercambio de contraseñas protegidos y mecanismos de firma;

b) el servicio de autenticación del origen de los datos puede proporcionarse mediante mecanismos de cifrado o de firma;

c) el servicio de control de acceso se proporciona mediante el uso apropiado de mecanismos específicos de control de acceso;

d) el servicio de confidencialidad en modo con conexión se proporciona mediante un mecanismo de cifrado y/o control de encaminamiento;

e) el servicio de confidencialidad en modo sin conexión se proporciona mediante un mecanismo de cifrado y/o control de encaminamiento;

f) el servicio de confidencialidad del flujo de tráfico se presta mediante un mecanismo de relleno de tráfico, combinado con un servicio de confidencialidad en la capa de red o debajo de ésta y/o control de encaminamiento;

g) el servicio de integridad en modo con conexión sin recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado, y

h) el servicio de integridad en modo sin conexión se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado.

7.3.2.2 Los mecanismos del protocolo que efectúan las operaciones de acceso a subred asociadas con la prestación del servicio de red de ISA de sistema extremo a sistema extremo ofrecen servicios a través de una sola subred.

La protección de una subred impuesta por la administración de la subred se aplicará según lo prescrito por los protocolos de acceso a la subred, pero se aplicará normalmente antes de las funciones normales de subred en la transmisión y después de las funciones normales de subred en la recepción.

7.3.2.3 Los mecanismos proporcionados por el protocolo que efectúa las operaciones de relevo y encaminamiento asociadas con la prestación del servicio de red de ISA, de sistema extremo a sistema extremo, ofrecen servicios por una o más redes interconectadas.

Estos mecanismos se invocarán antes de las funciones de retransmisión y reencaminamiento en la transmisión y después de dichas funciones en la recepción. En el caso del mecanismo del control de encaminamiento, las restricciones de encaminamiento apropiadas se obtienen de la BIGS antes de que los datos, junto con las necesarias restricciones de encaminamiento, se pasen a las funciones de relevo y encaminamiento.

7.3.2.4 El control de acceso en la capa de red puede tener muchos fines; por ejemplo, permite que un sistema extremo controle el establecimiento de conexiones de red y rechace las llamadas no deseadas. Permite también que una o varias subredes controlen la utilización de los recursos de la capa de red. En algunos casos, esta última finalidad se relaciona con la tarificación por la utilización de la red.

Nota – A menudo el establecimiento de una conexión de red puede producir una tarificación por la administración de la subred. El costo puede minimizarse controlando el acceso y seleccionando el cobro revertido u otros parámetros específicos de la red.

7.3.2.5 Las exigencias de una subred particular pueden imponer mecanismos de control de acceso al protocolo que efectúa las operaciones de acceso a la subred asociadas con la prestación del servicio de red de ISA de sistema extremo a sistema extremo. Cuando los mecanismos de control de acceso son proporcionados por el protocolo que efectúa las operaciones de relevo y de encaminamiento asociadas a la prestación del servicio de red ISA, de sistema extremo a sistema extremo, éstos pueden utilizarse a la vez para controlar el acceso a subredes por las entidades relevadoras y controlar el acceso a los sistemas extremos. Evidentemente, el grado de aislamiento del control de acceso está delimitado de una manera bastante general, y sólo distingue entre entidades de la capa de red.

7.3.2.6 Si se utiliza relleno de tráfico junto con un mecanismo de cifrado en la capa de red (o un servicio de confidencialidad proporcionado por la capa física), puede lograrse un nivel razonable de confidencialidad del flujo de tráfico.

7.4 *Capa de transporte*

7.4.1 *Servicios*

Los servicios de seguridad que pueden prestarse, individualmente o combinados, en la capa de transporte son:

a) autenticación de entidad par;

b) autenticación del origen de los datos;

c) servicio de control de acceso;

d) confidencialidad en modo con conexión;

e) confidencialidad en modo sin conexión;

f) integridad en modo con conexión con recuperación;

g) integridad en modo con conexión sin recuperación;

h) integridad en modo sin conexión.

7.4.2 *Mecanismos*

Los servicios de seguridad identificados se proporcionan como sigue:

a) el servicio de autenticación de entidad par es proporcionado por una combinación apropiada de intercambios de autenticación o protegidos, mecanismos de intercambio derivados criptográficamente o protegidos, o por mecanismos protegidos de intercambio de contraseñas y firmas;

b) el servicio de autenticación de origen de los datos puede proporcionarse por mecanismos de cifrado o de firma;

c) el servicio de control de acceso se proporciona mediante el uso apropiado de mecanismos específicos de control de acceso;

d) el servicio de confidencialidad en modo con conexión se proporciona mediante un mecanismo de cifrado;

e) el servicio de confidencialidad en modo sin conexión se proporciona mediante un mecanismo de cifrado;

f) el servicio de integridad en modo con conexión con recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;

g) el servicio de integridad en modo con conexión y recuperación se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado; y

h) el servicio de integridad en modo sin conexión se proporciona utilizando un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado.

Los mecanismos de protección operarán de manera que los servicios de seguridad puedan invocarse para conexiones individuales de transporte. La protección será tal que cada conexión de transporte pueda aislarse de todas las otras conexiones de transporte.

7.5 *Capa de sesión*

7.5.1 *Servicios*

En la capa de sesión no se proporcionan servicios de seguridad.

7.6 *Capa de presentación*

7.6.1 *Servicios*

La capa de presentación proporcionará facilidades para el soporte de la prestación de los siguientes servicios de seguridad por la capa de aplicación al proceso de aplicación:

a) confidencialidad en modo con conexión;

b) confidencialidad en modo sin conexión; y

c) confidencialidad de campos seleccionados.

Las facilidades de la capa de presentación pueden también soportar la prestación de los siguientes servicios de seguridad por la capa de aplicación al proceso de aplicación:

d) confidencialidad del flujo de tráfico;

e) autenticación de entidad par;

f) autenticación de origen de los datos;

g) integridad en modo con conexión con recuperación;

h) integridad en modo con conexión sin recuperación;

j) integridad en modo con conexión de campos seleccionados;

k) integridad en modo sin conexión;

m) integridad en modo sin conexión de campos seleccionados;

n) no repudio con prueba del origen; y

p) no repudio con prueba de la entrega.

Nota – Las facilidades proporcionadas por la capa de presentación serán las que dependen de mecanismos que sólo pueden operar sobre una codificación de sintaxis de transferencia de datos y comprenden, por ejemplo, las funcionalidades basadas en técnicas criptográficas.

7.6.2 *Mecanismos*

Para los siguientes servicios de seguridad, los mecanismos de soporte pueden situarse dentro de la capa de presentación y, en tal caso, pueden utilizarse junto con mecanismos de seguridad de la capa de aplicación para proporcionar servicios de seguridad de la capa de aplicación:

a) el servicio de autenticación de entidad par puede ser soportado por mecanismos de transformación sintáctica (por ejemplo, el cifrado)

b) el servicio de autenticación del origen de los datos puede ser soportado por mecanismos de cifrado o de firma;

c) el servicio de confidencialidad en modo con conexión puede ser soportado por un mecanismo de cifrado;

d) el servicio de confidencialidad en modo sin conexión puede ser soportado por un mecanismo de cifrado;

e) el servicio de confidencialidad de campos seleccionados puede ser soportado por un mecanismo de cifrado;

f) el servicio de confidencialidad de flujo de tráfico puede ser soportado por un mecanismo de cifrado.

g) el servicio de integridad en modo con conexión con recuperación puede ser soportado por un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;

h) el servicio de integridad en modo con conexión sin recuperación puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado;

j) el servicio de integridad en modo con conexión de campos seleccionados puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado.

k) el servicio de integridad en modo sin conexión puede ser soportado por un mecanismo de integridad de datos, algunas veces combinado con un mecanismo de cifrado.

m) el servicio de integridad en modo sin conexión de campos seleccionados puede ser soportado por un mecanismo de integridad de los datos, algunas veces combinado con un mecanismo de cifrado;

n) el servicio de no repudio con prueba del origen puede ser soportado por una combinación apropiada de mecanismos de integridad de datos, de firma y de notarización, y;

p) el servicio de no repudio con prueba de la entrega puede ser soportado por una combinación apropiada de mecanismos de integridad de datos, de firma y de notarización.

Los mecanismos de cifrado aplicados a la transferencia de datos, cuando están situados en las capas superiores, estarán contenidos en la capa de presentación.

Algunos de los servicios de seguridad indicados en la lista anterior pueden ser proporcionados alternativamente por mecanismos de seguridad contenidos completamente dentro de la capa de aplicación.

Sólo los servicios de seguridad de confidencialidad pueden ser proporcionados enteramente por mecanismos de seguridad contenidos dentro de la capa de presentación.

Los mecanismos de seguridad en la capa de presentación operan como la etapa final de transformación en la sintaxis de transferencia en la transmisión, y como la etapa inicial del proceso de transformación en la recepción.

7.7 *Capa de aplicación*

7.7.1 *Servicios*

La capa de aplicación puede proporcionar uno o más de los siguientes servicios de seguridad básicos individualmente o combinados:

a) autenticación de entidad par;

b) autenticación del origen de los datos;

c) servicio de control de acceso;

d) confidencialidad en modo con conexión;

e) confidencialidad en modo sin conexión;

f) confidencialidad de campos seleccionados;

g) confidencialidad del flujo de tráfico

h) integridad en modo con conexión con recuperación;

j) integridad en modo con conexión sin recuperación;

k) integridad en modo con conexión de campos seleccionados;

m) integridad en modo sin conexión;

n) integridad en modo sin conexión de campos seleccionados;

p) no repudio con prueba del origen y;

q) no repudio con prueba de la entrega.

La autenticación de los partícipes previstos en la comunicación facilita los controles de acceso a recursos ISA y distintos de ISA (por ejemplo, ficheros, logical (software), terminales, impresoras) en sistemas abiertos reales.

La determinación de requisitos específicos de seguridad en una instancia de comunicación, incluidas la confidencialidad, la integridad y la autenticación de los datos, puede ser efectuada por la gestión de seguridad de ISA o por la gestión de la capa de aplicación sobre la base de la información que figura en la BIGS, además de las peticiones hechas por el proceso de aplicación.

7.7.2 *Mecanismos*

Los servicios de seguridad de la capa de aplicación se proporcionan mediante los siguientes mecanismos:

a) el servicio de autenticación de entidad par puede proporcionarse utilizando la información de autenticación transferida entre entidades de aplicación, protegida por mecanismos de cifrado de la capa de presentación o de capas más bajas;

b) el servicio de autenticación del origen de los datos puede proporcionarse utilizando mecanismos de firma o mecanismos de cifrado de capas más bajas;

c) el servicio de control de acceso para estos aspectos de un sistema abierto real que son pertinentes a ISA, tales como la capacidad de comunicar con sistemas específicos o entidades de aplicación distantes, puede ser proporcionado por una combinación de mecanismos de control de acceso en la capa de aplicación y en capas inferiores;

d) el servicio de confidencialidad en modo con conexión puede proporcionarse utilizando un mecanismo de cifrado de capas inferiores;

e) el servicio de confidencialidad en modo sin conexión puede ser proporcionarse utilizando un mecanismo de cifrado de capas inferiores;

f) el servicio de confidencialidad de campos seleccionados puede proporcionarse utilizando un mecanismo de cifrado en la capa de presentación;

g) un servicio limitado de confidencialidades del flujo de tráfico puede proporcionarse utilizando un mecanismo de relleno de tráfico en la capa de aplicación, combinado con un servicio de confidencialidad en una capa inferior;

h) el servicio de integridad en modo con conexión con recuperación puede proporcionarse utilizando un mecanismo de integridad de los datos de una capa inferior (algunas veces combinado con un mecanismo de cifrado);

j) el servicio de integridad en modo con conexión sin recuperación puede proporcionarse utilizando un mecanismo de integridad de los datos de una capa inferior (algunas veces combinado con un mecanismo de cifrado);

k) el servicio de integridad en modo con conexión de campos seleccionados puede proporcionarse utilizando un mecanismo de integridad de los datos (algunas veces combinado con un mecanismo de cifrado) en la capa de presentación;

m) el servicio de integridad en modo sin conexión puede proporcionarse utilizando un mecanismo de integridad de los datos de una capa inferior (algunas veces combinado con un mecanismo de cifrado);

n) el servicio de integridad en modo sin conexión de campos seleccionados puede proporcionarse utilizando un mecanismo de integridad de datos (algunas veces combinado con un mecanismo de cifrado) en la capa de presentación;

p) el servicio de no repudio con prueba del origen puede proporcionarse mediante una combinación apropiada de mecanismos de firma y de integridad de datos de una capa inferior, posiblemente junto con el uso de notarios;

q) el servicio de no repudio con prueba de la entrega puede proporcionarse mediante una combinación apropiada de mecanismos de firma y de integridad de los datos de una capa inferior, posiblemente junto con la utilización de notarios.

Si se utiliza un mecanismo de notarización para proporcionar un servicio de no repudio, éste actuará como un tercero de confianza. Puede tener un registro de las unidades de datos relevadas en su forma transferida (es decir, en la sintaxis de transferencia) con el fin de resolver los conflictos. Puede utilizar servicios de protección de las capas inferiores.

7.7.3 *Servicios de seguridad distintos de ISA*

Los propios procesos de aplicación pueden proporcionar esencialmente todos los servicios, y utilizar las mismas clases de mecanismos que se describen en esta Recomendación, como debidamente situadas en las diversas capas de la arquitectura. Esta utilización no está contenida en el ámbito de las definiciones de los protocolos y servicios de ISA y de la arquitectura de ISA, pero no es incompatible con ellas.

7.8 *Ilustración de la relación entre los servicios de seguridad y las capas*

En el cuadro 2/X.800 se ilustran las capas del modelo de referencia en las cuales pueden proporcionarse servicios de seguridad particulares. Las descripciones de los servicios de seguridad figuran en el § 5.2. La justificación para la ubicación de un servicio en una capa determinada se indica en el anexo B.

CUADRO 2/X.800

Ilustración de la relación entre los servicios de seguridad y las capas

Servicio	Capas						
	1	2	3	4	5	6	7*
Autenticación de la entidad par	·	·	S	S	·	·	S
Autenticación del origen de los datos	·	·	S	S	·	·	S
Servicio de control de acceso	·	·	S	S	·	·	S
Confidencialidad en modo con conexión	S	S	S	S	·	S	S
Confidencialidad en modo sin conexión	·	S	S	S	·	S	S
Confidencialidad de campos seleccionados	·	·	·	·	·	S	S
Confidencialidad del tren de datos	S	·	S	·	·	·	S
Integridad en modo con conexión con recuperación	·	·	·	S	·	·	S
Integridad en modo con conexión sin recuperación	·	·	S	S	·	·	S
Integridad en modo con conexión de campos seleccionados	·	·	·	·	·	·	S
Integridad en modo sin conexión	·	·	S	S	·	·	S
Integridad en modo sin conexión de campos seleccionados	·	·	·	·	·	·	S
No repudio. Origen	·	·	·	·	·	·	S
No repudio. Entrega	·	·	·	·	·	·	S

S Sí, el servicio debe incorporarse en las normas de la capa como opción del proveedor.

· No se suministra el servicio.

* Debe señalarse que, para la capa 7, el propio proceso de aplicación puede suministrar servicios de seguridad.

Nota 1 – En el cuadro 2/X.800 no se trata de indicar que las entradas son de igual importancia; sin embargo, hay una variación considerable de la importancia de las entradas del cuadro.

Nota 2 – La ubicación de los servicios de seguridad en la capa de red se describe en el § 7.3.2. La ubicación de los servicios de seguridad en la capa de red no afecta significativamente la naturaleza y el alcance de los servicios que se proporcionan.

Nota 3 – La capa de presentación contiene varias facilidades de seguridad que soportan la prestación de servicios de seguridad por la capa de aplicación.

8 Gestión de seguridad

8.1 *Generalidades*

8.1.1 La gestión de seguridad de ISA trata los aspectos de gestión de seguridad relativos a ISA y a la seguridad de gestión de ISA. Los aspectos de gestión de seguridad de ISA se relacionan con las operaciones que están fuera de las instancias normales de comunicación pero que se necesitan para exportar y controlar los aspectos de seguridad de estas comunicaciones.

Nota – La disponibilidad de un servicio de comunicación es determinada por la configuración de la red y/o por los protocolos de gestión de red. Es necesario tomar decisiones apropiadas para protegerse contra la negación de servicio.

8.1.2 La administración o administraciones de los sistemas abiertos distribuidos pueden imponer un gran número de políticas de seguridad y las normas de gestión de seguridad de ISA deberán apoyar estas políticas. Las entidades sujetas a una sola política de seguridad, administrada por una sola autoridad se reúnen algunas veces en lo que se ha denominado un «dominio de seguridad». Los dominios de seguridad y sus interacciones son elementos importantes para las futuras ampliaciones de la presente Recomendación.

8.1.3 La gestión de seguridad de ISA trata la gestión de los servicios y mecanismos de seguridad de ISA. Este tipo de gestión requiere la distribución de información de gestión en estos servicios y mecanismos así como la recopilación de informaciones relativas a la operación de estos servicios y mecanismos. Estas informaciones pueden ser, por ejemplo, la distribución de las claves criptográficas, la determinación de parámetros de selección de seguridad impuestos administrativamente, el informe de eventos de seguridad normales y anómalos (registros de auditoría) y la activación y desactivación de los servicios. La gestión de seguridad no se ocupa de hacer pasar informaciones relativas a la seguridad en los protocolos que requieren servicios de seguridad específicos (por ejemplo, en los parámetros de peticiones de conexión).

8.1.4 La Base de Información de Gestión de Seguridad (BIGS) es el conjunto conceptual de información de seguridad que necesitan los sistemas abiertos. Este concepto no supone nada en cuanto a la forma y a la realización del almacenamiento de la información. Sin embargo, cada sistema extremo debe contener las informaciones locales necesarias que le permitan aplicar una política de seguridad apropiada. La BIGS es una base de información distribuida en la medida en que es necesario aplicar una política de seguridad coherente en una agrupación (lógica o física) de sistemas extremos. En la práctica, partes de la BIGS pueden estar o no integradas a la BIG.

Nota – Puede haber muchas realizaciones de la BIGS, por ejemplo:

a) una tabla de datos;

b) un fichero;

c) datos o reglas integradas en el logical (software) o en el material (hardware) del sistema abierto real.

8.1.5 Los protocolos de gestión, sobre todo los protocolos de gestión de seguridad y los canales de comunicación que transmiten informaciones de gestión, son potencialmente vulnerables. Por tanto, hay que cuidar especialmente de garantizar que los protocolos de gestión y la información están protegidos de modo que no se debilite la protección de seguridad prevista para las instancias de comunicación habituales.

8.1.6 La gestión de seguridad puede requerir el intercambio de información de seguridad entre diversas administraciones de sistemas para que la BIGS pueda establecerse o ampliarse. En algunos casos, las informaciones relativas a la seguridad se transmitirán por trayectos de comunicación distintos de la ISA, y los administradores de sistemas locales actualizarán la BIGS según métodos no normalizados por la ISA. En otros casos, puede ser conveniente intercambiar estas informaciones por un trayecto de comunicación de la ISA; las informaciones se transmitirán entonces entre dos aplicaciones de gestión de seguridad que funcionan en los sistemas abiertos reales. Para aplicar la gestión de seguridad se utilizarán las informaciones comunicadas para actualizar la BIGS. Esta actualización de la BIGS puede requerir la autorización previa del administrador de seguridad apropiado.

8.1.7 Se definirán protocolos de aplicación para el intercambio de informaciones relativas a la seguridad por canales de comunicaciones de ISA.

8.2 *Categorías de gestión de seguridad de ISA*

Hay tres categorías de actividad de gestión de seguridad de ISA:

a) gestión de seguridad de sistema;

b) gestión de servicios de seguridad;

c) gestión de mecanismos de seguridad.

Además, hay que tomar en consideración la seguridad de la gestión propiamente dicha de ISA (véase el § 8.2.4). A continuación se resumen las funciones esenciales realizadas por estas categorías de gestión de seguridad.

8.2.1 *Gestión de seguridad de sistema*

La gestión de seguridad de sistema se relaciona con la gestión de aspectos de seguridad de todo el entorno de ISA. La siguiente lista contiene las actividades típicas comprendidas en esta categoría de gestión de seguridad:

a) gestión global de la política de seguridad, que abarca las actualizaciones y el mantenimiento de la coherencia;

b) interacción con otras funciones de gestión de ISA;

c) interacción con la gestión de servicios de seguridad y la gestión de mecanismos de seguridad;

d) gestión de tratamiento de eventos (véase el § 8.3.1);

e) gestión de auditoría de seguridad (véase el § 8.3.2); y

f) gestión de recuperación de seguridad (véase el § 8.3.3).

8.2.2 *Gestión de servicios de seguridad*

La gestión de servicios de seguridad trata la gestión de servicios de seguridad particulares. La siguiente lista es un ejemplo de las actividades que pueden efectuarse en la gestión de un servicio de seguridad particular:

a) determinación y asignación de la protección de seguridad nominal (es decir, fijada como objetivo) para el servicio;

b) asignación y mantenimiento de reglas de selección (cuando existen otras posibilidades) del mecanismo de seguridad específico que ha de utilizarse para prestar el servicio de seguridad solicitado;

c) negociación (local y a distancia) de los mecanismos de seguridad disponibles que requieren un acuerdo de gestión previo;

d) aplicación de mecanismos de seguridad específicos por la función apropiada de gestión de mecanismos de seguridad, por ejemplo, para la prestación de servicios de seguridad impuestos administrativamente;

e) interacción con otras funciones de gestión de servicios de seguridad y de mecanismos de seguridad.

8.2.3 *Gestión de mecanismos de seguridad*

La gestión de mecanismos de seguridad trata la gestión de mecanismos de seguridad particulares. A modo de ejemplo, a continuación figura una lista, que no es exhaustiva, de funciones de gestión de mecanismos de seguridad:

a) gestión de claves;

b) gestión de cifrado;

c) gestión de firma digital;

d) gestión de control de acceso;

e) gestión de integridad de los datos;

f) gestión de autenticación;

g) gestión de relleno;

h) gestión de control de encaminamiento; y

j) gestión de notarización.

En el § 8.4 se presentan más detalladamente estas funciones de gestión de mecanismo de seguridad.

8.2.4 *Seguridad de la gestión de ISA*

La seguridad de todas las funciones de gestión de ISA y de la comunicación de información de gestión de ISA son partes importantes de la seguridad de una ISA. Esta categoría de gestión de seguridad reposa sobre elecciones apropiadas de servicios y de mecanismos de seguridad de ISA clasificados para garantizar que los protocolos y las informaciones de gestión de ISA están protegidos de manera adecuada (véase el § 8.1.5). Por ejemplo, las comunicaciones entre las entidades de gestión que implican la base de información de gestión requieren por lo general cierta forma de protección.

8.3 *Actividades específicas de gestión de seguridad de sistema*

8.3.1 *Gestión de tratamiento de eventos*

Los aspectos de gestión de tratamiento de eventos visibles en la ISA son el informe a distancia de intentos evidentes de violar la seguridad del sistema y la modificación de los umbrales utilizados para poner en marcha la generación de informes de eventos.

8.3.2 *Gestión de auditoría de seguridad*

La gestión de auditoría de seguridad puede comprender:

a) la selección de los eventos que han de anotarse y/o recopilarse a distancia;

b) la habilitación y la inhabilitación de la anotación en el registro de auditoría de eventos seleccionados;

c) la recopilación a distancia de anotaciones de auditoría seleccionadas;

d) la preparación de informes de auditoría de seguridad.

8.3.3 *Gestión de recuperación de seguridad*

La gestión de recuperación de seguridad puede comprender:

a) el mantenimiento de las reglas utilizadas para reaccionar contra violaciones de seguridad reales o sospechadas;

b) el informe a distancia de violaciones evidentes de la seguridad del sistema;

c) las interacciones del administrador de seguridad.

8.4 *Funciones de gestión de mecanismos de seguridad*

8.4.1 *Gestión de claves*

La gestión de claves puede comprender:

a) la generación de claves apropiadas a intervalos que dependen del nivel de seguridad requerido;

b) la determinación, conforme a las necesidades de control de acceso, de las entidades que deberán recibir una copia de cada clave;

c) la puesta a disposición o la distribución de las claves de manera segura a las instancias de identidad en los sistemas abiertos reales.

Queda entendido que algunas funciones de gestión de clave se efectuarán fuera del entorno de ISA. Estas funciones comprenden la distribución física de las claves por medios de confianza.

El intercambio de las claves de trabajo que han de utilizarse en el curso de una asociación es una función normal de protocolo de capa. La selección de claves de trabajo puede hacerse también mediante el acceso a un centro de distribución de claves o mediante la distribución previa por los protocolos de gestión.

8.4.2 *Gestión de cifrado*

La gestión de cifrado puede comprender:

a) la interacción con la gestión de claves;

b) el establecimiento de parámetros criptográficos;

c) la sincronización criptográfica.

La existencia de un mecanismo de cifrado implica la utilización de la gestión de claves y de métodos comunes para hacer referencia a los algoritmos criptográficos.

El grado de discriminación de la protección aportada por el cifrado es determinada por las entidades que, en el entorno de ISA, son cifradas independientemente. Esto es determinado a su vez, en general, por la arquitectura de seguridad y, más específicamente, por el mecanismo de gestión de claves.

Puede obtenerse una referencia común para los algoritmos criptográficos utilizando un registro para estos algoritmos o por acuerdo previo entre entidades.

8.4.3 *Gestión de firma digital*

La gestión de firma digital puede comprender:

a) la interacción con la gestión de claves;

b) el establecimiento de parámetros y de algoritmos criptográficos;

c) la utilización de un protocolo entre las entidades comunicantes y, eventualmente, un tercero.

Nota – En general, la gestión de firma digital y la gestión de cifrado son muy similares.

8.4.4 *Gestión de control de acceso*

La gestión de control de acceso puede comprender la distribución de los atributos de seguridad (incluidas las contraseñas) o las actualizaciones de listas de control de acceso o de listas de capacidades. Puede comprender también la utilización de un protocolo entre las entidades comunicantes y otras entidades que prestan servicios de control de acceso.

8.4.5 *Gestión de integridad de los datos*

La gestión de integridad de los datos puede comprender:

a) la interacción con la gestión de claves;

b) el establecimiento de parámetros y de algoritmos criptográficos;

c) la utilización de un protocolo entre las entidades comunicantes.

Nota – Cuando se utilizan técnicas criptográficas para la integridad de los datos, la gestión de integridad de los datos y la gestión de cifrado son muy similares.

8.4.6 *Gestión de autenticación*

La gestión de autenticación puede comprender la distribución de información descriptiva, de contraseñas o de claves (con ayuda de la gestión de claves) entre las entidades que deben efectuar una autenticación. Puede comprender también la utilización de un protocolo entre las entidades comunicantes y otras entidades que prestan servicios de autenticación.

8.4.7 *Gestión de relleno de tráfico*

La gestión de relleno puede comprender el mantenimiento de las reglas que han de utilizarse para el relleno. Por ejemplo, puede comprender:

a) velocidades de datos especificadas previamente;

b) especificación de velocidades binarias aleatorias;

c) especificación de características de mensajes, como la longitud, y

d) variación deliberada de la especificación, eventualmente en función de la hora y/o del calendario.

8.4.8 *Gestión de control de encaminamiento*

La gestión de control encaminamiento puede comprender la definición de los enlaces o las subredes que se consideran seguros, o de confianza, con respecto a determinados criterios.

8.4.9 *Gestión de notarización*

La gestión de notarización puede comprender:

a) la distribución de información relativa a los notarios;

b) la utilización de un protocolo entre un notario y las entidades comunicantes; y

c) la interacción con notarios.

ANEXO A

Información básica sobre seguridad en la interconexión de sistemas abiertos (ISA)

(Este anexo no forma parte de la presente Recomendación)

A.1 *Información básica*

Este anexo contiene:

a) información sobre la seguridad de ISA con el fin de dar cierta perspectiva a la presente ampliación a esta Recomendación;

b) información complementaria sobre las repercusiones arquitecturales de diversas prestaciones y exigencias de seguridad.

La seguridad en un entorno de ISA es sólo un aspecto de la seguridad del procesamiento de los datos y de las comunicaciones de datos. Para ser eficaces, las medidas de protección utilizadas en un entorno de ISA requieren la utilización de medios que están fuera de la ISA. Por ejemplo, las informaciones que fluyen entre sistemas pueden estar cifradas, pero si no se imponen restricciones físicas de seguridad al acceso a los propios sistemas, el cifrado puede resultar vano. La interconexión de sistemas abiertos sólo trata la interconexión de sistemas. Para que las medidas de seguridad de ISA sean eficaces deberán utilizarse con medidas que están fuera del ámbito de la ISA.

A.2 *Exigencias de seguridad*

A.2.1 *¿Qué se entiende por seguridad?*

El término «seguridad» se utiliza en el sentido de minimizar las vulnerabilidades de los bienes y recursos. Un «bien» es todo elemento de valor. Vulnerabilidad es toda debilidad que pudiera explotarse para violar un sistema o las informaciones que éste contiene. Una amenaza es una violación potencial de la seguridad.

A.2.2 *Motivación para la seguridad en los sistemas abiertos*

El CCITT ha reconocido la necesidad de una serie de Recomendaciones para mejorar la seguridad en la arquitectura de interconexión de sistemas abiertos. Esta necesidad proviene de:

a) la creciente dependencia de la sociedad con respecto a los computadores a los que se gana acceso, o están enlazados, por comunicaciones de datos y que requieren protección contra diversas amenazas;

b) la aparición, en algunos países, de una legislación sobre la «protección de los datos», que obliga a los proveedores a demostrar la integridad de su sistema y el respeto de la privacidad;

c) el deseo de diversas organizaciones de utilizar recomendaciones sobre la ISA, mejoradas según las necesidades, para sistemas seguros existentes y futuros.

A.2.3 *¿Qué debe protegerse?*

En general, los elementos siguientes pueden necesitar protección:

a) informaciones y datos (incluidos el logicial y los datos pasivos relativos a las medidas de seguridad, tales como las contraseñas);

b) los servicios de comunicación y de procesamiento de datos;

c) los equipos y facilidades.

A.2.4 *Amenazas*

Las amenazas contra un sistema de comunicación de datos son las siguientes:

a) destrucción de información y/o de otros recursos;

b) corrupción o modificación de información;

c) robo, supresión o pérdida de información y/o de otros recursos;

d) revelación de información;

e) interrupción de servicios.

Las amenazas pueden clasificarse en amenazas accidentales o amenazas intencionales y pueden ser activas o pasivas.

A.2.4.1 *Amenazas accidentales*

Las amenazas accidentales son las que existen sin que haya premeditación. Ejemplos de amenazas accidentales que se concretizan son: fallos del sistema, equivocaciones en la operación y errores en los programas.

A.2.4.2 *Amenazas intencionales*

Las amenazas intencionales pueden ir desde el examen ocasional, mediante el empleo de instrumentos de monitorización de fácil adquisición, hasta ataques sofisticados, gracias a un conocimiento especial del sistema. Una amenaza intencional que se concretiza puede considerarse como un «ataque».

A.2.4.3 *Amenazas pasivas*

Las amenazas pasivas son las que, si se concretizan, no producirían ninguna modificación de las informaciones contenidas en el(los) sistema(s) y que no modifican el funcionamiento ni el estado del sistema. La interceptación pasiva para observar informaciones transmitidas por una línea de comunicaciones es una forma de concretar una amenaza pasiva.

A.2.4.4 *Amenazas activas*

Las amenazas activas contra un sistema conllevan la alteración de información contenida en el sistema, o las modificaciones del estado o de la operación del sistema. La modificación maliciosa de las tablas de encaminamiento de un sistema por un usuario no autorizado es un ejemplo de amenaza activa.

A.2.5 *Algunos tipos específicos de ataque*

A continuación se examinan brevemente algunos ataques particularmente importantes en un entorno de procesamiento de datos/comunicaciones de datos. En los puntos que siguen aparecen los términos «autorizado» y «no autorizado». «Autorización» significa «concesión de derechos». Esta definición entraña que: los derechos son derechos de efectuar ciertas actividades (como el acceso a los datos); y que estos derechos se han concedido a una entidad, operador humano o proceso. Por tanto, el comportamiento autorizado es la ejecución de las actividades para los cuales se han concedido (y no se han revocado) los derechos. En el § A.3.3.1 se describe más detalladamente el concepto de autorización.

A.2.5.1 *Usurpación de identidad (o impostura)*

La usurpación de identidad (o impostura) tiene lugar cuando una entidad se hace pasar por otra. Se utiliza generalmente con otras formas de ataque activo, especialmente la reproducción y la modificación de los mensajes. Por ejemplo, las secuencias de autenticación pueden ser capturadas y reproducidas después que se ha efectuado una secuencia de autenticación válida. Una entidad autorizada que tiene pocos privilegios puede usurpar la identidad de otra para obtener privilegios suplementarios de otra entidad que tiene estos privilegios.

A.2.5.2 *Reproducción*

La reproducción ocurre cuando un mensaje o una parte de un mensaje se repite para producir un efecto no autorizado. Por ejemplo, un mensaje válido que contiene informaciones de autenticación puede ser reproducido por otra entidad para autenticarse a sí misma (como algo que no es).

A.2.5.3 *Modificación de los mensajes*

La modificación de un mensaje se produce cuando el contenido de una transmisión de datos se modifica sin que esto sea detectado y produce un efecto no autorizado, por ejemplo, cuando un mensaje que dice «se autoriza a 'Juan López' a leer el fichero confidencial 'Cuentas'» se modifica como sigue «Se autoriza a 'Pedro Pérez' a leer el fichero confidencial 'Cuentas'».

A.2.5.4 *Negación de servicio*

La negación de servicio se produce cuando una entidad no cumple su función propia o actúa de manera que impide a otras entidades cumplir sus funciones propias. El ataque puede ser general, cuando una entidad suprime todos los mensajes, o bien el ataque puede tener un objetivo específico, cuando una entidad suprime todos los mensajes enviados a un destino particular, como el servicio de auditoría de seguridad. El ataque puede comprender la supresión del tráfico tal como se describe en este ejemplo, o bien puede generar un tráfico suplementario. También es posible generar mensajes con el fin de desorganizar el funcionamiento de la red, sobre todo si esta red tiene entidades relevadoras que toman decisiones de encaminamiento basadas en los informes de status recibidos de otras entidades relevadoras.

A.2.5.5 *Ataques del interior*

Los ataques del interior se producen cuando los usuarios legítimos de un sistema se comportan de manera imprevista o no autorizada. La mayor parte de los delitos conocidos en que han intervenido computadores son cometidos por ataques del interior que han comprometido la seguridad del sistema. Los métodos de protección que pueden utilizarse contra los ataques del interior son:

a) una supervisión cuidadosa del personal;

b) un examen minucioso del material, del logicial, de la política de seguridad y de las configuraciones de sistema, con el fin de que haya un cierto grado de garantía de buen funcionamiento (esto se ha denominado funcionalidad de confianza);

c) registros de auditoría para aumentar la probabilidad de detectar estos ataques.

A.2.5.6 *Ataques del exterior*

Los ataques del exterior pueden utilizar las técnicas siguientes:

a) interceptación (activa y pasiva);

b) interceptación de emisiones;

c) usurpación de la identidad de usuarios autorizados del sistema o de componentes del sistema;

d) contorneo de los mecanismos de autenticación o de control de acceso.

A.2.5.7 *Trampa*

Cuando una entidad de un sistema se modifica para permitir que un atacante produzca un efecto no autorizado a petición o en el curso de un evento o secuencia de eventos predeterminados, el resultado se denomina trampa. Por ejemplo, la validación de una contraseña podría modificarse de modo que, además de su efecto normal, validase también la contraseña de un atacante.

A.2.5.8 *Caballo de Troya*

Un «Caballo de Troya» es un programa introducido en el sistema con una función no autorizada además de su función autorizada. Un relevador que copia también mensajes destinados a un canal no autorizado es un «Caballo de Troya».

A.2.6 *Evaluación de las amenazas, riesgos y contramedidas*

Las características de seguridad aumentan generalmente el costo de un sistema y pueden hacer más difícil su utilización. Antes de diseñar un sistema seguro, conviene por tanto identificar las amenazas específicas contra las cuales se necesita una protección. Esto es lo que se llama «evaluación de amenazas». Un sistema es vulnerable en muchos aspectos pero sólo algunos de éstos son explotables porque el atacante no tiene ocasión de intervenir, o porque el resultado no justifica ni el esfuerzo ni el riesgo de detección. El detalle de la evaluación de las amenazas está fuera del alcance del presente anexo; no obstante, en general, esta evaluación abarca:

a) la identificación de las vulnerabilidades del sistema;

b) el análisis de la probabilidad de las amenazas destinadas a explotar estas vulnerabilidades;

c) la evaluación de las consecuencias que tendría la ejecución de cada amenaza;

d) la estimación del costo de cada ataque;

e) la determinación del costo de posibles contramedidas;

f) la elección de mecanismos de seguridad justificados (eventualmente mediante un análisis de la relación costo/beneficio).

Algunas medidas no técnicas, como una cobertura de seguro mercantil, pueden ser soluciones sustitutivas rentables de las medidas de seguridad técnica. Una seguridad técnica perfecta, como una seguridad física perfecta, es imposible. Por consiguiente, el objetivo debería ser hacer que el costo de un ataque sea suficientemente elevado para reducir el riesgo a niveles aceptables.

A.3 *Política de seguridad*

En este punto se examina la política de seguridad: la necesidad de una política de seguridad correctamente definida, su función; los métodos políticos utilizados y las mejoras que han de efectuarse en situaciones específicas. Estos conceptos se aplican después a los sistemas de comunicación.

A.3.1 *Necesidad y objetivo de una política de seguridad*

El dominio total de la seguridad es a la vez complejo y de un alcance considerable. Todo análisis suficientemente completo dará una plétora de detalles. Una política de seguridad apropiada debería concentrarse en los aspectos de una situación que el nivel más alto de autoridad juzgue digna de atención. En cuanto a lo esencial, una política de seguridad establece, en términos generales, lo que se permite y lo que no se permite, en el campo de la seguridad durante el funcionamiento en general del sistema en cuestión. Una política de seguridad no suele ser específica; indica lo que tiene una importancia capital sin decir precisamente cómo deben obtenerse los resultados deseados. Una política de seguridad fija el nivel máximo de una especificación de seguridad.

A.3.2 *Repercusiones de la definición de políticas: Proceso de refinamiento*

Como una política de seguridad es tan general, no está muy claro al principio cómo la política puede asociarse con una aplicación dada. A menudo, la mejor manera de conseguir esto consiste en someter la política de seguridad a un refinamiento progresivo añadiendo más y más detalles a partir de la aplicación en cada nivel. Para saber cuáles deben ser estos detalles se necesita un estudio minucioso del dominio de la aplicación a la luz de la política general de seguridad. Este examen debería definir los problemas que se plantean cuando se tratan de imponer las condiciones de la política de seguridad a la aplicación. El proceso de refinamiento permitirá redefinir la política de seguridad general en términos muy precisos directamente deducidos de la aplicación. Esta política redefinida facilitará la determinación de los detalles de realización.

A.3.3 *Componentes de la política de seguridad*

Las políticas de seguridad existentes comprenden dos aspectos, que dependen del concepto de comportamiento autorizado.

A.3.3.1 *Autorización*

Todas las amenazas mencionadas entrañan la noción de comportamiento autorizado o no autorizado. La declaración que define lo que constituye una autorización se concreta en la política de seguridad. Una política de seguridad genérica podrá decir: «la información no puede darse a personas que no tengan la autorización apropiada; estas personas no pueden tener acceso, ni pueden intervenir en esta información, ni utilizar un recurso». La naturaleza de la autorización es lo que distingue las diferentes políticas de seguridad. Estas pueden dividirse en dos componentes, según la naturaleza de la autorización que contienen: políticas basadas en reglas o políticas basadas en la identidad. Las primeras utilizan reglas basadas en un pequeño número de atributos generales o de clases de sensibilidad aplicadas universalmente. Las segundas comprenden criterios de utilización basados en atributos específicos individualizados. Se supone que ciertos atributos están asociados permanentemente a la entidad a la cual se aplican; otros pueden ser propiedades (como las capacidades) que pueden transmitirse a otras entidades. Puede distinguirse también entre el servicio de autorización impuesto administrativamente y el servicio de autorización elegido de manera dinámica. La política de seguridad determinará los elementos de la seguridad de sistema que se aplican siempre y están en vigor (por ejemplo, los eventuales componentes de la política de seguridad basada en reglas y los de la política de seguridad basada en la identidad) y los que el usuario puede elegir y utilizar a su conveniencia.

A.3.3.2 *Política de seguridad basada en la identidad*

En las políticas de seguridad, el aspecto «basada en la identidad» corresponde en parte al concepto de seguridad conocido como «necesidad de conocer». El objetivo es filtrar el acceso a los datos o a los recursos. Hay dos maneras principales de aplicar las políticas basadas en la identidad: que las informaciones o los derechos a acceso sean mantenidos por los que tienen acceso o que estas informaciones formen parte de datos a los cuales se tiene acceso. Por ejemplo, en el primer caso, los privilegios o capacidades son concedidos a los usuarios y utilizados por procesos que actúan en su nombre. En el segundo caso, pueden utilizarse Listas de Control de Acceso (LCA). En los dos casos, el tamaño del ítem de datos (que varía desde un fichero completo hasta un elemento de datos) que puede denominarse en una capacidad o que transporta su propia LCA puede ser extremadamente variable.

A.3.3.3 *Política de seguridad basada en reglas*

En una política de seguridad basada en reglas, la política de seguridad suele reposar en la sensibilidad. En un sistema seguro, los datos y/o recursos deben marcarse con etiquetas de seguridad. Los procesos que actúan en nombre de usuarios humanos pueden adquirir la etiqueta de seguridad apropiada a sus originadores.

A.3.4 *Política de seguridad, comunicaciones y etiquetas*

El concepto de etiquetado es importante en un entorno de comunicaciones de datos. Las etiquetas que transportan atributos desempeñan una diversidad de funciones. Hay ítems de datos que son transferidos durante la comunicación; hay procesos y entidades que inician la comunicación, y procesos y entidades que responden, y hay canales y otros recursos del propio sistema que son utilizados durante la comunicación. Todo puede etiquetarse, de una

manera o de otra, con sus atributos. Las políticas de seguridad deben indicar cómo pueden utilizarse los atributos de cada uno para proporcionar la seguridad requerida. Puede ser necesario efectuar la negociación para establecer el significado de seguridad apropiado de determinados atributos etiquetados. Cuando se añaden etiquetas de seguridad a los procesos de acceso y a los datos a los que se tiene acceso, la información adicional necesaria para aplicar el control de acceso basado en la identidad deben ser las etiquetas pertinentes. Cuando la política de seguridad se basa en la identidad del usuario que tiene acceso a los datos, sea directamente o a través de un proceso, las etiquetas de seguridad deben incluir información sobre la identidad del usuario. En una política de seguridad, las reglas relativas a etiquetas particulares deben indicarse e incluirse en la Base de Información de Gestión de Seguridad (BIGS) y/o negociarse con los sistemas extremos, según proceda. La etiqueta puede estar acompañada de atributos que califican su sensibilidad, especifican las protecciones relativas al tratamiento y a la distribución, introducen restricciones de tiempo y de puesta a disposición y anuncian exigencias específicas al sistema extremo.

A.3.4.1 *Etiquetas de proceso*

En la autenticación, es decir la identificación completa, los procesos o entidades que actúan como iniciadores o respondedores en una instancia de comunicación, así como los atributos apropiados son de una importancia fundamental. Por tanto, las BIGS contendrán información suficiente sobre los atributos que son importantes para toda política impuesta por una Administración.

A.3.4.2 *Etiquetas de ítems de datos*

Los ítems de datos transferidos en una instancia de comunicación están estrechamente vinculados a su etiqueta (esta vinculación es significativa y para ciertas instancias de política de seguridad basadas en reglas, se prescribe que la etiqueta sea una parte especial del ítem de datos antes que sea presentado a la aplicación). Las técnicas que permiten preservar la integridad del ítem de datos mantendrán también la exactitud y el acoplamiento de la etiqueta. Estos atributos pueden ser utilizados por funciones de control de encaminamiento en la capa de enlace de datos del modelo de referencia básico de ISA.

A.4 *Mecanismos de seguridad*

Una política de seguridad puede aplicarse utilizando diversos mecanismos; según los objetivos de la política de seguridad y los mecanismos utilizados, cada mecanismo puede emplearse solo o combinado con otros mecanismos. En general, un mecanismo pertenecerá a una de las tres clases siguientes (que se superponen):

a) prevención;

b) detección; y

c) recuperación.

A continuación se presentan los mecanismos de seguridad apropiados para el entorno de comunicación de datos.

A.4.1 *Técnicas criptográficas y cifrado*

La criptografía es el fundamento de numerosos servicios y mecanismos de seguridad. Pueden utilizarse funciones criptográficas en el cifrado, el descifrado, la integridad de los datos, los intercambios de autenticación, el almacenamiento y la verificación de las contraseñas, etc., para ayudar a obtener la confidencialidad, la integridad y/o la autenticación. El cifrado utilizado en la confidencialidad, transforma los datos sensibles (es decir, los datos que deben protegerse) en datos menos sensibles. En la integridad o la autenticación, se utilizan técnicas criptográficas para computar funciones «inforzables».

El cifrado se efectúa inicialmente en un texto claro para producir un texto cifrado o criptograma. El resultado del descifrado es un texto claro, o un texto cifrado en cualquier forma. Es computacionalmente factible utilizar texto claro para un procesamiento de propósito general; el contenido semántico del texto es accesible; no es posible tratar un texto cifrado, cuando su contenido semántico está escondido, salvo de manera muy específica (por ejemplo, descifrado o correspondencia exacta). A veces el cifrado es intencionalmente irreversible (por ejemplo, por truncamiento o pérdida de datos) cuando se desea que no se recupere nunca el texto claro original, como las contraseñas.

Las funciones criptográficas utilizan criptovariables y operan sobre campos, unidad de datos, y/o en trenes de unidades de datos. Dos de estas criptovariables son la clave, que dirige las transformaciones específicas, y la variable de inicialización, requerida en algunos protocolos criptográficos para preservar el carácter aleatorio aparente del texto cifrado. La clave debe mantenerse generalmente confidencial y la función criptográfica así como la variable de iniciación pueden aumentar los retardos de transmisión y el consumo de anchura de banda. Esto complica las adiciones criptográficas «transparentes» o «drop-in» a los sistemas existentes.

Las variables criptográficas pueden ser simétricas o asimétricas para el cifrado y el descifrado. Las claves utilizadas en los algoritmos asimétricos están relacionadas matemáticamente; no se puede calcular una clave a partir de otra. Estos algoritmos se denominan algunas veces algoritmos «de claves públicas», pues una clave puede hacerse pública mientras que la otra puede mantenerse secreta.

El texto cifrado puede ser criptanalizado, cuando ello sea computacionalmente factible, para recuperar el texto claro sin conocer la clave. Esto puede suceder si se utiliza una función criptográfica débil o defectuosa. Las interceptaciones de los análisis de tráfico pueden conducir a ataques del criptosistema, que incluyen la inserción de mensaje/campo, la supresión y el cambio, la reproducción de un texto cifrado anteriormente válido y la usurpación de identidad.

Por tanto, se han concebido protocolos criptográficos para resistir a los ataques y a veces, al análisis del tráfico. Una contramedida específica de análisis de tráfico, la «confidencialidad del flujo de tráfico», tiende a ocultar la presencia o la ausencia de datos y sus características. Si el texto cifrado es relevado, la dirección debe estar en claro en los relevadores y cabeceras. Se dirá que la arquitectura utiliza un «cifrado enlace por enlace» si los datos sólo son cifrados en cada enlace y son descifrados (y por tanto son vulnerables) en el relevador o cabecera. Se dirá que la arquitectura utiliza un «cifrado de extremo a extremo» si sólo la dirección (y datos de control similares) están en claro en el relevador o cabecera. El cifrado de extremo a extremo es más conveniente desde el punto de vista de la seguridad, pero es mucho más complejo desde el punto de vista de la arquitectura, sobre todo si se incluye al mismo tiempo la distribución electrónica de claves dentro de banda (una función de la gestión de claves). El cifrado enlace por enlace se puede combinar con el cifrado de extremo a extremo para alcanzar varios objetivos de seguridad. La integridad de los datos se realiza a menudo calculando un valor de control criptográfico. El valor de control puede derivarse en una o varias etapas y es una función matemática de las criptovariables y de los datos. Estos valores de control están asociados a los datos que deben protegerse. Los valores de control criptográficos se denominan a veces códigos de detección de manipulación.

Las técnicas criptográficas pueden proporcionar, o ayudar a proporcionar, protección contra:

a) la observación y/o la modificación del flujo de mensajes;

b) el análisis del tráfico;

c) el repudio;

d) la falsificación;

e) la conexión no autorizada; y

f) la modificación de los mensajes.

A.4.2 *Aspectos de la gestión de claves*

La utilización de algoritmos criptográficos implica una gestión de claves. La gestión de claves abarca la producción, la distribución y el control de claves criptográficas. La elección de un método de gestión de claves se basa en la evaluación, por los participantes, del entorno en el cual debe utilizarse. Las consideraciones de este entorno comprenden las amenazas contra las cuales hay que protegerse (a la vez internas y externas a la organización), las tecnologías utilizadas, la arquitectura y la ubicación de los servicios criptográficos proporcionados, la estructura física y la ubicación de los proveedores de los servicios criptográficos.

Los puntos que deben considerarse en relación con la gestión de claves son:

a) la utilización, implícita o explícita, de un «tiempo de vida» basado en la duración, la utilización u otros criterios, para cada clave definida;

b) la identificación correcta de claves según su función, de modo que su utilización pueda reservarse únicamente a su función; por ejemplo, las claves previstas para ser utilizadas para un servicio de confidencialidad no deben utilizarse para un servicio de integridad y viceversa; y

c) consideraciones no relacionadas con la ISA, como la distribución física de las claves y su archivo.

Los puntos que han de tenerse en cuenta en la gestión de claves, en el caso de algoritmos de claves simétricos, son:

a) la utilización de un servicio de confidencialidad en el protocolo de gestión de claves, para transportar las claves;

b) la utilización de una jerarquía de claves. Podrían autorizarse diferentes situaciones:

   1) jerarquías de claves «planas», que sólo utilizan claves de cifrado de datos, seleccionadas implícita o explícitamente de un juego de claves, según la identidad o el índice de la clave;

   2) jerarquías de claves multicapa;

   3) nunca deberían utilizarse claves de cifrado de claves para proteger los datos y nunca deberían utilizarse claves de cifrado de datos para proteger claves de cifrado de claves;

c) la división de las responsabilidades, de modo que nadie tenga una copia completa de una clave importante.

Los puntos que han de tenerse en cuenta en la gestión de claves, en el caso de algoritmos de claves asimétricos son:

a) la utilización de un servicio de confidencialidad en el protocolo de gestión de claves, para transportar las claves privadas;

b) la utilización de un servicio de integridad, o de un servicio de no repudio con prueba del origen, en el protocolo de gestión de claves, para transportar las claves públicas. Estos servicios pueden prestarse utilizando algoritmos criptográficos simétricos y/o asimétricos.

A.4.3 *Mecanismos de firma digital*

El término «firma digital» designa una técnica particular que puede utilizarse para suministrar servicios de seguridad tales como el no repudio y la autenticación. Los mecanismos de firma digital requieren la utilización de algoritmos criptográficos asimétricos. La característica esencial del mecanismo de firma digital es que la unidad de datos firmada no puede crearse sin utilizar la clave privada. Esto significa que:

a) la unidad de datos firmada sólo puede ser creada por el tenedor de la clave privada;

b) el recibiente no puede crear la unidad de datos firmada.

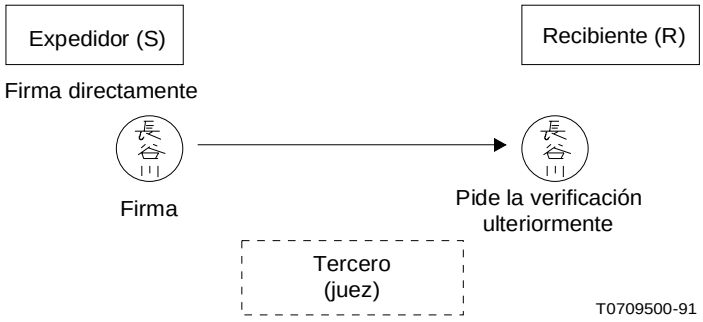
En consecuencia, utilizando sólo informaciones públicas, es posible identificar sin ambigüedad que el firmante de una unidad de datos es el tenedor de la clave privada. En caso de litigio ulterior entre los participantes es posible probar la identidad del firmante de una unidad de datos a un tercero fiable que será llamado a juzgar la autenticidad de la unidad de datos firmada. Este tipo de firma digital se denomina esquema de firma directa (véase la figura A-1/X.800). En los otros casos, puede ser necesaria además la propiedad indicada en el inciso c) siguiente:

c) el expedidor no puede negar haber enviado la unidad de datos firmada.

En este caso, un tercero fiable (árbitro) prueba al recibiente la fuente y la integridad de las informaciones. Este tipo de firma digital se denomina a veces esquema de firma arbitrada (véase la figura A-2/X.800).

Nota – El expedidor puede solicitar que el recibiente no pueda negar ulteriormente que ha recibido la unidad de datos firmada. Esto es realizable con un servicio de no repudio con prueba de la entrega, por medio de una combinación apropiada de los mecanismos de firma digital, de integridad de datos y de notarización.

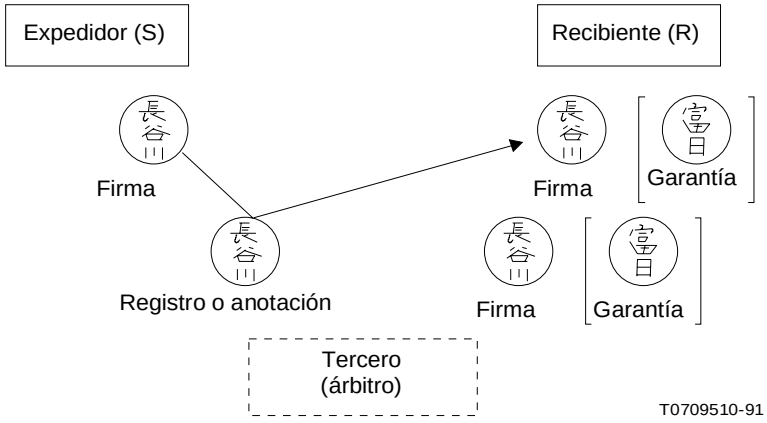
Expéditeur (E)



Nota — Verifica la firma cuando se plantea un conflicto entre los participantes (el expedidor puede no decir la verdad o el recibiente puede no decir la verdad).

FIGURA A-1/X.800

Esquema de firma directa



Nota — El tercero autentica la fuente [y da garantía (es decir, resultado positivo) para el recibiente]. La información necesaria para probar la fuente y la integridad de los datos es registrada por un tercero. En este caso, el expedidor no puede negar ulteriormente el envío de la unidad de datos firmada.

FIGURA A-2/X.800

Esquema de firma arbitrada

A.4.4 *Mecanismos de control de acceso*

Los mecanismos de control de acceso son los que se utilizan para aplicar una política de limitación del acceso a un recurso a los usuarios autorizados. Estas técnicas comprenden la utilización de listas o de matrices de control de acceso (que por lo general contienen las identidades de los ítems controlados y de los usuarios autorizados; estos usuarios son, por ejemplo, personas o procesos); estas técnicas utilizan también contraseñas y capacidades, etiquetas o testigos, cuya posesión puede emplearse para indicar derechos de acceso. Cuando se utilizan capacidades, éstas deben ser «inforzables» y transportarse de manera segura.

A.4.5 *Mecanismo de integridad de datos*

Los mecanismos de integridad de datos son de dos tipos: los que se utilizan para proteger la integridad de una sola unidad de datos y los que protegen a la vez la integridad de una sola unidad de datos y la secuencia de unidades de datos en el curso de una conexión.

A.4.5.1 *Detección de modificaciones del flujo de mensajes*

Las técnicas de detección de corrupciones, normalmente asociadas a la detección de errores de bit, de errores de bloque y de errores de secuenciación introducidos por los enlaces y redes de comunicación, pueden emplearse también para detectar las modificaciones del flujo de mensajes. Sin embargo, si los encabezamientos y remolques (trailers) no están protegidos por mecanismos de integridad, un intruso informado puede lograr contornear estos controles. Por tanto, sólo se puede detectar una modificación del flujo de mensajes utilizando técnicas de detección de corrupciones en relación con las informaciones relativas a la secuencia de datos. Esto no impedirá la modificación del flujo de mensajes, pero permitirá notificar los ataques.

A.4.6 *Mecanismos de intercambio de autenticación*

A.4.6.1 *Elección de los mecanismos*

La elección y las combinaciones de mecanismos de intercambio de autenticación apropiados para diferentes circunstancias son numerosos. Por ejemplo:

a) Cuando las entidades pares y los medios de comunicación son fiables, la identificación de una entidad par puede confirmarse mediante una contraseña. La contraseña protege contra errores, pero no es una garantía contra la malicia (en particular, contra la reproducción). La autenticación mutua puede hacerse utilizando una contraseña diferente en cada sentido.

b) Cuando cada entidad confía en sus entidades pares pero no confía en los medios de comunicación, puede proporcionarse protección contra ataques activos mediante combinaciones de contraseñas y cifrado o por medios criptográficos. La protección contra la reproducción requiere tomas de contacto bidireccionales (con parámetros de protección) o un estampado de hora (con relojes fiables). La autenticación mutua con protección contra la reproducción puede realizarse en intercambios tridireccionales.

c) Cuando las entidades no confían (o piensan que no podrán confiar en el futuro) en sus entidades pares o en los medios de comunicación, pueden utilizarse servicios de no repudio. El servicio de no repudio puede prestarse utilizando un mecanismo de firma digital y/o de notarización. Estos mecanismos pueden utilizarse con los descritos en b).

A.4.7 *Mecanismos de relleno*

La producción de tráfico espurio y el relleno de unidades de datos de protocolo hasta una longitud fija puede suministrar una protección limitada contra el análisis del tráfico. Para ser eficaz, el nivel de tráfico espurio debe aproximarse al nivel máximo previsto del tráfico real más elevado. Además, el contenido de las unidades de datos de protocolo debe cifrarse o «disfrazarse» de modo que el tráfico espurio no pueda identificarse y diferenciarse del tráfico real.

A.4.8 *Mecanismo de control de encaminamiento*

La especificación de las restricciones de encaminamiento para la transferencia de datos (incluida la especificación de una ruta completa) puede utilizarse para asegurar que los datos sólo se encaminan por rutas físicamente seguras o para asegurar que las informaciones sensibles sólo se encaminan por rutas con un nivel de protección apropiado.

A.4.9 *Mecanismo de notarización*

El mecanismo de notarización se basa en el concepto de un tercero de confianza (un notario) para garantizar ciertas propiedades relativas a las informaciones intercambiadas entre dos entidades, tales como su origen, su integridad, o la hora en que se enviaron o recibieron.

A.4.10 *Seguridad física y personal*

Se necesitarán siempre medidas de seguridad física para garantizar una protección completa. La seguridad física es costosa, y a menudo se trata de minimizar su necesidad utilizando otras técnicas (más baratas). Las consideraciones relativas a la seguridad física y a la fiabilidad del personal están fuera del ámbito de la ISA, aunque en fin de cuentas, todos los sistemas reposan en una cierta forma de seguridad física y en la fiabilidad del personal que hace funcionar el sistema. Deberían definirse procedimientos de funcionamiento para garantizar un funcionamiento correcto y describir las responsabilidades del personal.

A.4.11 *Material/logicial de confianza*

Los métodos utilizados para confiar en el funcionamiento correcto de una entidad comprenden métodos de pruebas formales, verificación y validación, detección y registro de tentativas de ataque, así como la construcción de la entidad por un personal de confianza en un entorno seguro. Hay que cuidar también de que la entidad no sea modificada accidental o deliberadamente de modo que se comprometa la seguridad durante su vida útil, por ejemplo, durante el mantenimiento u operaciones de ampliación. Si debe mantenerse la seguridad, hay que fiarse del funcionamiento correcto de ciertas entidades. Los métodos utilizados para crear la confianza están fuera del ámbito de la ISA.

ANEXO B

Justificación de la ubicación de los servicios y mecanismos de seguridad especificados en el § 7

(Este anexo no forma parte de la presente Recomendación)

B.1 *Generalidades*

En el presente anexo se exponen algunas razones para la prestación de los servicios de seguridad identificados en las diferentes capas, según se indica en el § 7. Los principios de la distribución de la seguridad en capas expuestos en el § 6.1.1 de la presente Recomendación han gobernado este proceso de selección.

Un servicio de seguridad particular es suministrado por más de una capa si puede considerarse que el efecto sobre la seguridad general de la comunicación es diferente (por ejemplo, confidencialidad de la conexión en las capas 1 y 4). Sin embargo, si se consideran las funcionalidades existentes de la comunicación de datos de ISA (por ejemplo, los procedimientos multienlace, la función de multiplexación, las diferentes maneras de convertir un servicio en modo sin conexión en un servicio en modo conexión) y con el fin de permitir el funcionamiento de estos mecanismos de transmisión, puede ser necesario proporcionar un servicio particular en otra capa, aunque no pueda considerarse que el efecto sobre la seguridad sea diferente.

B.2 *Autenticación de la entidad par*

- *Capas 1 y 2:* No, la autenticación de la entidad par no se considera útil en estas capas.
- *Capa 3:* Sí, en subredes individuales y para encaminamiento y/o en el interfuncionamiento combinado de redes.
- *Capa 4:* Sí, la autenticación de sistema extremo a sistema extremo en la capa 4 puede servir para autenticar dos o más entidades de sesión, antes que comience una conexión y mientras dure la misma.
- *Capa 5:* No, no hay ningún interés en proporcionar este servicio en la capa 4 y/o superiores.

– *Capa 6:* No, pero los mecanismos de cifrado pueden soportar este servicio en la capa de aplicación.

– *Capa 7:* Sí, la capa de aplicación debería proporcionar la autenticación de la entidad par.

B.3 *Autenticación del origen de los datos*

– *Capas 1 y 2:* No, la autenticación del origen de los datos no se considera útil en estas capas.

– *Capas 3 y 4:* La autenticación del origen de los datos puede ser proporcionada de extremo a extremo por la función de relevo y de encaminamiento de la capa 3 y/o la capa 4, como sigue:

  a) la provisión de la autenticación de la entidad par en el momento del establecimiento de la conexión con autenticación continua basada en el cifrado, durante la vida de una conexión, suministra, de hecho, el servicio de autenticación de origen de los datos;

  b) aunque no se proporcione a), puede suministrarse la autenticación del origen de los datos basada en el cifrado, con pocos gastos suplementarios, además de los relacionados con los mecanismos de integridad de los datos ya situados en estas capas.

– *Capa 5:* No, no hay ningún interés en suministrar este servicio en la capa 4 o en la capa 7.

– *Capa 6:* No, pero los mecanismos de cifrado pueden soportar este servicio en la capa de aplicación.

– *Capa 7:* Sí, eventualmente en relación con mecanismos de la capa de presentación.

B.4 *Control de acceso*

– *Capas 1 y 2:* Los mecanismos de control de acceso no pueden suministrarse en las capas 1 y 2 en un sistema conforme a los protocolos completos de ISA, puesto que no hay facilidades de extremo disponibles para este tipo de mecanismo.

– *Capa 3:* Los mecanismos de control de acceso pueden ser impuestos a la función de acceso a la subred por las exigencias de una subred particular. Cuando son aplicados por la función de relevo y encaminamiento, los mecanismos de acceso de la capa de red pueden utilizarse a la vez para controlar el acceso a las subredes por las entidades relevadoras y para controlar el acceso a los sistemas extremos. Evidentemente, la granularidad del acceso es bastante gruesa; sólo se distingue entre las entidades de la capa de red.

  El establecimiento de una conexión de red puede traducirse a menudo por una tarificación por la administración de la subred. El control de acceso y la aceptación de cobro revertido o la elección de otros parámetros de red o subred pueden minimizar los costos.

– *Capa 4:* Sí, pueden utilizarse mecanismos de control de acceso, sobre la base de una conexión de transporte de extremo a extremo.

– *Capa 5:* No, no hay ningún interés en suministrar este servicio en la capa 4 y/o la capa 7.

– *Capa 6:* No, este mecanismo no es apropiado para la capa 6.

– *Capa 7:* Sí, los protocolos de aplicación y/o los procesos de aplicación pueden suministrar facilidades de control de acceso, orientadas a la aplicación.

B.5 *Confidencialidad de todos los datos de usuario (N) en una conexión (N)*

– *Capa 1:* Sí, debería proporcionarse dado que la inserción eléctrica de pares transparentes de dispositivos de transformación puede asegurar una confidencialidad completa en una conexión física.

– *Capa 2:* Sí, pero esto no aumenta la seguridad en las capas 1 ó 3 por encima de la confidencialidad en la capa 1 o en la capa 3.

– *Capa 3:* Sí, para una función de acceso a la subred en subredes individuales y para funciones de relevo y encaminamiento en el funcionamiento combinado de redes.

– *Capa 4:* Sí, dado que la conexión de transporte asegura un mecanismo de transporte de extremo a extremo y puede suministrar el aislamiento de las conexiones de sesión.

– *Capa 5:* No, dado que esto no mejora la confidencialidad en las capas 3, 4 y 7. No parece apropiado suministrar este servicio en esta capa.

– *Capa 6:* Sí, dado que estos mecanismos de cifrado sólo proporcionan transformaciones puramente sintácticas.

– *Capa 7:* Sí, junto con mecanismos de las capas inferiores.

B.6 *Confidencialidad de todos los datos de usuario (N) en una UDS en modo sin conexión (N)*

La justificación es la misma que para la confidencialidad de todos los datos de usuario (N), salvo para la capa 1, donde no hay servicio sin conexión.

B.7 *Confidencialidad de campos seleccionados en los datos del usuario (N) de una UDS*

Este servicio de confidencialidad es suministrado por el mecanismo de cifrado en la capa de presentación y es invocado por mecanismos de la capa de aplicación según la semántica de los datos.

B.8 *Confidencialidad del flujo de tráfico*

La confidencialidad total del flujo de tráfico sólo puede realizarse en la capa 1 por la inserción física de un par de dispositivos de cifrado en el canal de transmisión físico. Se supone que el canal de transmisión será bidireccional simultáneo y síncrono, de modo que la inserción de los dispositivos hace irreconocibles todas las transmisiones (incluso su presencia) en los soportes físicos.

Por encima de la capa física, no es posible tener una seguridad total del flujo de tráfico. Algunos de sus efectos pueden obtenerse en parte utilizando un servicio completo de confidencialidad de las UDS en una capa e inyectando tráfico espurio en una capa superior. Este tipo de mecanismo es costoso y puede consumir una gran cantidad de la capacidad de portadoras y de conmutación.

Si se suministra la confidencialidad del flujo de tráfico en la capa 3, se utilizará el relleno y/o el control de encaminamiento. El control de encaminamiento puede suministrar una confidencialidad limitada del flujo de tráfico si se encaminan los mensajes contorneando los enlaces o redes poco seguros. Sin embargo, la incorporación de relleno de tráfico en la capa 3 permite utilizar mejor la red, por ejemplo, evitando un relleno inútil y la congestión de la red.

En la capa de aplicación puede suministrarse una confidencialidad limitada del flujo de tráfico mediante la generación de tráfico espurio junto con confidencialidad para impedir la identificación de dicho tráfico espurio.

B.9 *Integridad de todos los datos de usuario (N) en modo con conexión (con recuperación tras error)*

– *Capas 1 y 2:* Las capas 1 y 2 no pueden suministrar este servicio. La capa 1 no tiene ningún mecanismo de detección o de recuperación. El mecanismo de la capa 2 sólo funciona punto a punto y no de extremo a extremo; en consecuencia, no se considera útil la prestación de este servicio.

– *Capa 3:* No, dado que la recuperación tras error no está disponible universalmente.

– *Capa 4:* Sí, dado que este servicio suministra la verdadera conexión de transporte de extremo a extremo.

– *Capa 5:* No, dado que la recuperación tras error no es una función de la capa 5.

– *Capa 6:* No, pero los mecanismos de cifrado pueden soportar este servicio en la capa de aplicación.

– *Capa 7:* Sí, junto con mecanismos de la capa de presentación.

B.10 *Integridad de todos los datos de usuario (N) en modo con conexión (sin recuperación tras error)*

– *Las capas 1 y 2* no pueden suministrar este servicio. La capa 1 no tiene ningún mecanismo de detección o de recuperación, y el mecanismo de la capa 2 sólo funciona punto a punto y no de extremo a extremo. En consecuencia, no se considera útil la prestación de este servicio.

– *Capa 3:* Sí, para la función de acceso a la subred a través de subredes individuales y para las funciones de encaminamiento y de relevo en el funcionamiento combinado de redes.

– *Capa 4:* Sí, para los casos en que es aceptable detener la comunicación tras la detección de un ataque activo.

– *Capa 5:* No, dado que este servicio no aporta un beneficio adicional con respecto a la integridad de los datos suministrada en las capas 3, 4 ó 7.

– *Capa 6:* No, pero mecanismos de cifrado pueden soportar este servicio en la capa de aplicación.

– *Capa 7:* Sí, junto con los mecanismos de la capa de presentación.

B.11 *Integridad de campos seleccionados de los datos de usuario (N) de UDS (N) en el modo de conexión (sin recuperación)*

La integridad de campos seleccionados puede ser suministrada por el mecanismo de cifrado en la capa de presentación junto con mecanismos de invocación y de control en la capa de aplicación.

B.12 *Integridad de todos los datos de usuarios (N) de una UDS (N) en modo sin conexión*

Con el fin de minimizar la duplicación de funciones, la integridad de las transferencias en modo sin conexión sólo debería proporcionarse en las mismas capas que la integridad sin recuperación, es decir, en las capas de red, de transporte y de aplicación. Deberá tenerse en cuenta que estos mecanismos de integridad sólo pueden tener una eficacia muy limitada.

B.13 *Integridad de campos seleccionados en una sola UDS (N) en modo sin conexión*

La integridad de campos seleccionados puede ser suministrada por mecanismos de cifrado en la capa de presentación junto con mecanismos de invocación y de control en la capa de aplicación.

B.14 *No repudio*

Los servicios de no repudio con prueba del origen y de la entrega pueden ser suministrados por un mecanismo de notarización que comprenderá un relevo en la capa 7.

La utilización del mecanismo de firma digital para el servicio de no repudio requiere una cooperación estrecha entre las capas 6 y 7.

ANEXO C

Elección de la posición del mecanismo de cifrado para las aplicaciones

(Este anexo no forma parte de la presente Recomendación)

C.1 La mayoría de las aplicaciones no necesitan cifrado en más de una capa. La elección de la capa depende de ciertos elementos importantes que se describen a continuación:

1) Si se exige confidencialidad total del flujo de tráfico, se elegirá el cifrado o la seguridad de transmisión en la capa física (por ejemplo, técnicas apropiadas de espectro ensanchado). Una seguridad física adecuada, un encaminamiento de confianza, así como una funcionalidad similar en el nivel en los relevos pueden satisfacer todas las exigencias de confidencialidad.

2) Si se exige una alta granularidad de protección (es decir, potencialmente, una clave separada para cada asociación de aplicación), el no repudio o la protección de campos seleccionados, se elegirá el cifrado en la capa de presentación. La protección de campos seleccionados puede ser importante porque los algoritmos de cifrado consumen grandes cantidades de potencia de procesamiento. El cifrado en la capa de presentación puede suministrar la integridad sin recuperación, el no repudio y la confidencialidad total.

3) Si se desea una protección bruta simple de todas las comunicaciones de sistema extremo a sistema extremo y/o un dispositivo de cifrado externo (por ejemplo, para garantizar una protección física del algoritmo y de las claves o una protección contra un logicial defectuoso), se elegirá el cifrado en la capa de red. Esto puede proporcionar la confidencialidad y la integridad sin recuperación.

   Nota – Aunque no se suministre la recuperación en la capa de red, los mecanismos normales de recuperación de la capa de transporte pueden utilizarse para una recuperación tras los ataques detectados por la capa de red.

4) Si se exige la integridad con recuperación, con una alta granularidad de protección, se elegirá el cifrado en la capa de transporte. Esto puede suministrar la confidencialidad y la integridad con o sin recuperación.

5) No se recomienda el cifrado en la capa de enlace de datos para las realizaciones futuras.

C.2 Cuando varios de estos criterios se consideran importantes, puede ser necesario proporcionar el cifrado en más de una capa.