UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T E.408

(05/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE E: EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

Gestión de red – Gestión de la red internacional

Requisitos de seguridad para las redes de telecomunicaciones

Recomendación UIT-T E.408

RECOMENDACIONES UIT-T DE LA SERIE E

EXPLOTACIÓN GENERAL DE LA RED, SERVICIO TELEFÓNICO, EXPLOTACIÓN DEL SERVICIO Y FACTORES HUMANOS

EXPLOTACIÓN DE LAS RELACIONES INTERNACIONALES	
Definiciones	E.100–E.103
Disposiciones de carácter general relativas a las Administraciones	E.104–E.119
Disposiciones de carácter general relativas a los usuarios	E.120–E.139
Explotación de las relaciones telefónicas internacionales	E.140–E.159
Plan de numeración del servicio telefónico internacional	E.160–E.169
Plan de encaminamiento internacional	E.170–E.179
Tonos utilizados en los sistemas nacionales de señalización	E.180–E.189
Plan de numeración del servicio telefónico internacional	E.190–E.199
Servicio móvil marítimo y servicio móvil terrestre público	E.200–E.229
DISPOSICIONES OPERACIONALES RELATIVAS A LA TASACIÓN Y A LA CONTABILIDAD EN EL SERVICIO TELEFÓNICO INTERNACIONAL	
Tasación en el servicio internacional	E.230–E.249
Medidas y registro de la duración de las conferencias a efectos de la contabilidad	E.260–E.269
UTILIZACIÓN DE LA RED TELEFÓNICA INTERNACIONAL PARA APLICACIONES NO TELEFÓNICAS	
Generalidades	E.300–E.319
Telefotografía	E.320–E.329
DISPOSICIONES DE LA RDSI RELATIVAS A LOS USUARIOS	E.330–E.349
PLAN DE ENCAMINAMIENTO INTERNACIONAL	E.350–E.399
GESTIÓN DE RED	
Estadísticas relativas al servicio internacional	E.400–E.404
Gestión de la red internacional	**E.405–E.419**
Comprobación de la calidad del servicio telefónico internacional	E.420–E.489
INGENIERÍA DE TRÁFICO	
Medidas y registro del tráfico	E.490–E.505
Previsiones del tráfico	E.506–E.509
Determinación del número de circuitos necesarios en explotación manual	E.510–E.519
Determinación del número de circuitos necesarios en explotación automática y semiautomática	E.520–E.539
Grado de servicio	E.540–E.599
Definiciones	E.600–E.649
Ingeniería de tráfico para redes con protocolo Internet	E.650–E.699
Ingeniería de tráfico de RDSI	E.700–E.749
Ingeniería de tráfico de redes móviles	E.750–E.799
CALIDAD DE LOS SERVICIOS DE TELECOMUNICACIÓN: CONCEPTOS, MODELOS, OBJETIVOS, PLANIFICACIÓN DE LA SEGURIDAD DE FUNCIONAMIENTO	
Términos y definiciones relativos a la calidad de los servicios de telecomunicación	E.800–E.809
Modelos para los servicios de telecomunicación	E.810–E.844
Objetivos para la calidad de servicio y conceptos conexos de los servicios de telecomunicaciones	E.845–E.859
Utilización de los objetivos de calidad de servicio para la planificación de redes de telecomunicaciones.	E.860–E.879
Recopilación y evaluación de datos reales sobre la calidad de funcionamiento de equipos, redes y servicios	E.880–E.899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T E.408

Requisitos de seguridad para las redes de telecomunicaciones

Resumen

En esta Recomendación se presentan una síntesis de los requisitos de seguridad y un marco que identifica las amenazas a la seguridad de las redes de telecomunicaciones en general (fijas y móviles; tanto voz como datos) y se dan orientaciones para la planificación de las contramedidas que se pueden prever para disminuir los riesgos que surgen de las amenazas.

Orígenes

La Recomendación UIT-T E.408 fue aprobada el 28 de mayo de 2004 por la Comisión de Estudio 2 (2001-2004) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. 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 Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

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

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T E.408

Requisitos de seguridad para las redes de telecomunicaciones

1 Introducción

1.1 Alcance

En esta Recomendación se presentan una síntesis y un marco que identifican las amenazas a la seguridad de las redes de telecomunicaciones en general (fijas y móviles; tanto voz como datos) y se dan orientaciones para la planificación de las contramedidas que se pueden prever para disminuir los riesgos que surgen de las amenazas.

Esta Recomendación es de naturaleza genérica y no identifica o aborda requisitos de redes específicas.

El objetivo de esta Recomendación no es definir nuevos servicios de seguridad sino que utiliza los servicios de seguridad existentes definidos en otras Recomendaciones del UIT-T y en normas pertinentes de otros organismos.

Con esta Recomendación se pretende facilitar la cooperación internacional en los siguientes campos en lo que se refiere a la seguridad de las redes de telecomunicaciones:

- uso compartido y diseminación de la información;
- coordinación de incidentes y respuesta en situaciones de crisis;
- reclutamiento y entrenamiento de personal profesional en materia de seguridad;
- coordinación de los responsables de hacer cumplir la ley;
- protección de infraestructura y servicios críticos;
- desarrollo de la legislación adecuada.

Para lograr dicha cooperación, es fundamental la aplicación a nivel nacional de los requisitos de la presente Recomendación en lo que concierne a los componentes nacionales de la red.

1.2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones.*

– Recomendación UIT-T M.3016 (1998), *Visión general de la seguridad en la red de gestión de las telecomunicaciones.*

– Recomendación UIT-T M.3400 (2000), *Funciones de gestión de la red de gestión de las telecomunicaciones.*

– Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y de atributos.*

– Recomendación UIT-T X.741 (1995) | ISO CEI 10164-9:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso.*

– Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones del CCITT*.

– Recomendación UIT-T X.802 (1995) | ISO CEI 13594:1995, *Tecnología de la información – Modelo de seguridad de capas inferiores.*

– Recomendación UIT-T X.803 (1994) | ISO CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores.*

– Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.

– Recomendación UIT-T X.810 (1995) | ISO CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general.*

– Recomendación UIT-T X.812 (1995) | ISO CEI 10181-3:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso.*

– Recomendación UIT-T X.813 (1996) | ISO CEI 10181-4:1997, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo.*

– Recomendación UIT-T X.814 (1995) | ISO CEI 10181-5:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de confidencialidad.*

– Recomendación UIT-T X.815 (1995) | ISO CEI 10181-6:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de integridad.*

– Recomendación UIT-T X.816 (1995) | ISO CEI 10181-7:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad.*

– ISO/CEI 9979:1999, *Information technology – Security techniques – Procedures for the registration of cryptographic algorithms*.

– IETF RFC 2535 (1999), *Domain Name System Security Extensions*.

– IETF RFC 2870 (2000), *Root Name Server Operational Requirements*.

– IETF RFC 3013 (2000), *Recommended Internet Service Provider Security Services and Procedures*.

1.3 Utilización del término "servicio"

El término "servicio" en la presente Recomendación no se refiere a ninguno de los servicios definidos por la UIT, sino que se utiliza como término genérico al tratar de cuestiones y/o funciones relativas a la seguridad, y se definirá ulteriormente.

1.4 Justificación

La necesidad de un marco genérico para seguridad de la red para las telecomunicaciones internacionales se ha originado a partir de distintas fuentes:

– **Los clientes/abonados** necesitan poder confiar en la red y en los servicios ofrecidos, incluida la disponibilidad de éstos (especialmente los servicios de emergencia) en caso de catástrofes de gran magnitud, incluidos los atentados terroristas.

– **La comunidad pública/autoridades** exigen seguridad a través de directrices y legislación, a fin de garantizar la disponibilidad de servicios, la competencia equitativa y la protección de la vida privada.

– **Los propios operadores de red/proveedores de servicio** demandan seguridad para salvaguardar sus intereses de explotación y comerciales, y para poder cumplir sus obligaciones contraídas con los clientes y el público, a nivel nacional e internacional.

Los requisitos de seguridad para las redes de telecomunicación deben fundamentarse preferentemente en normas de seguridad acordadas internacionalmente ya que es recomendable reutilizar en lugar de crear nuevas normas. El suministro y utilización de servicios y mecanismos de seguridad pueden resultar bastante onerosos con relación al valor de las transacciones que se van a proteger. Por consecuencia, es importante tener la capacidad para personalizar la seguridad que se proporciona con relación a los servicios que se pretende proteger. Los servicios y mecanismos de seguridad que se utilicen deben proporcionarse de tal manera que permitan esa personalización. Debido a la gran cantidad de combinaciones posibles de características de seguridad, es deseable disponer de **perfiles de seguridad** (véase el apéndice II) que abarquen una amplia gama de servicios de red de telecomunicaciones.

La normalización facilitará la **reutilización de soluciones y productos**, lo que permitirá la introducción más rápida y a menor costo de la seguridad.

Para los proveedores y usuarios de sistemas parecidos, los beneficios importantes de las soluciones normalizadas son la economía de escala en el desarrollo de productos y el interfuncionamiento de componentes dentro de las redes de telecomunicación con relación a la seguridad.

Es indispensable disponer de servicios y mecanismos de seguridad para proteger las redes de telecomunicación contra ataques malintencionados tales como la negación de servicio, escucha clandestina, simulación, alteración de mensajes (modificación, retardo, supresión, inserción, reproducción, reencaminamiento, encaminamiento erróneo o resolicitud de mensajes), rechazo o falsificación. La protección incluye la prevención, detección y recuperación a partir de situaciones de ataque, así como la gestión de la información relativa a la seguridad. Además, la protección debe incluir medidas para evitar las interrupciones de servicio debidas a causas naturales (clima, etc.) o ataques malintencionados (acciones terroristas). Se deberá disponer de las previsiones necesarias para permitir la escucha clandestina y la supervisión conforme a las solicitudes de las autoridades jurídicas debidamente autorizadas.

2 Descripción del sistema

Para asegurar una red de manera eficaz, se recomienda implementar capas de seguridad. Mientras más capas se utilicen, más eficaz será la seguridad. Esta técnica por capas puede analizarse desde la más básica:

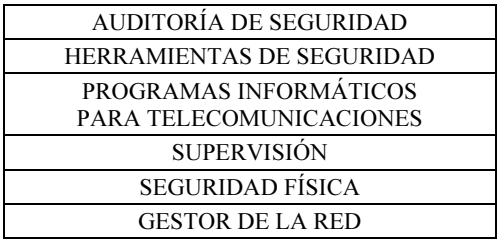

Figura 1/E.408 – Modelo de seis capas para seguridad de la red

El término "capa", tal como se utiliza en la presente Recomendación, es simplemente una descripción de algunas consideraciones de seguridad necesarias para organizar la seguridad de la red. No deben considerarse las capas en esta Recomendación como elementos de la arquitectura, ni confundirse con las capas de seguridad de la Rec. UIT-T X.805.

De la misma manera que los cimientos de una casa, la primera capa de gestor de la red será el recurso más importante de la organización para su seguridad. El gasto adicional anual en un buen gestor de red es 100 veces mejor que adquirir un cortafuegos costoso. Los buenos gestores de red conocen los sistemas operativos con los que trabajan y saben cómo proteger cada máquina de su red autorizando únicamente los puertos y los procesos que realmente son necesarios. La gestión debe ofrecer a sus administradores de red entrenamiento continuo y tiempo para mantenerse por delante de problemas de la red.

La segunda capa es la seguridad física. Cada atacante en el mundo sabe que la manera más sencilla para acceder a una red es desde el interior. Hay simplemente muchos casos de "ingeniería social", donde los atacantes simplemente llaman al servicio de atención al usuario y reportan haber olvidado su contraseña solicitando que la misma se cambie a xxxxx. La seguridad física incluye todo desde permitir que únicamente ciertas personas (administradores del sistema) accedan a las consolas, hasta políticas relativas a qué tipo de información se puede dar al público con relación a su red. Las buenas políticas sobre utilización aceptable, contraseñas e instalación de programas informáticos ayudan considerablemente a controlar el acceso a su red.

La tercera capa es la supervisión. Es muy raro que un ataque funcione en el primer intento. La mayoría de los ataques se podrán detener si alguien revisa simplemente la bitácora de registro del sistema una vez por día. Esto no debe tomar mucho tiempo como podría parecer inicialmente. El ojo humano es el mejor dispositivo para detectar patrones en los ficheros de registro. Hay diversos programas informáticos muy eficientes que permiten supervisar los ficheros de registro y aunque estos programas pueden ser muy útiles, el gestor del sistema debería revisar los registros de sus máquinas principales todos los días.

La cuarta capa es el programa informático para telecomunicaciones. Se debe evaluar cada programa informático que se instala en los servidores, teniendo en mente la seguridad. El gestor del sistema debe saber, por ejemplo, a cuáles puertos TCP y UDP estará vinculado el programa informático, con qué cuentas de usuario interactúa el mismo y los permisos de directorio que necesita. Además, se recomienda examinar los problemas de seguridad conocidos, antes de la adquisición. Esto se debe volver parte del proceso de evaluación de todas las compras de programas informáticos.

La quinta capa son las herramientas de seguridad. Después de que alguien ha establecido buenas políticas y prácticas para las cuatro capas anteriores, es necesario comenzar a analizar los

cortafuegos, los programas informáticos de detección de intrusión y los mandatarios (*proxies*). Instalar el mejor cortafuegos mientras se tengan malas políticas para su aplicación resulta peor que no tenerlo. Bastante a menudo es posible encontrar servidores de red con políticas de seguridad deficientes que dependen del cortafuegos para contener a los atacantes. Una vez que cede el cortafuegos, todos los servidores quedan totalmente expuestos al ataque.

La sexta capa es la auditoría de seguridad. La seguridad de la red es algo que evoluciona. Cada día, hay alguien en algún lugar que está tratando de encontrar un nuevo método para utilizarlo en perjuicio de otra persona. Es importante intentar regularmente penetrar en nuestra propia red. Un proceso de auditoría debe probar cada aspecto de la seguridad de la red. Se recomienda probar la seguridad física contra los ataques y hacer funcionar un escáner de números telefónicos (*war dialer*) utilizando todos los números telefónicos para asegurarse de que nadie haya instalado un módem en un ordenador individual sin conocimiento del gestor de la red. Se deben llevar a cabo auditorías del servidor de correo, servidor de nombres de dominio (DNS) y de los servidores de dominio, web y FTP.

2.1 Agentes y funciones

Para la finalidad de normalización de la red de telecomunicaciones, se debe considerar únicamente la seguridad técnica, lo que significa que los agentes pertinentes que se deben considerar son los agentes de telecomunicaciones (TA, *telecommunication actors*). Un TA es una persona (física o jurídica) o un proceso responsable de algunas operaciones de la red.

Cada vez que un TA realiza una operación, desempeñará una función. En algunos casos habrá una relación uno a uno entre un usuario TA y una función, es decir, el TA se mantendrá siempre en la misma función. En otros casos habrá una relación uno a muchos entre un usuario TA particular y las funciones posibles que puede desempeñar el TA.

A continuación se presenta una clasificación de algunas de las funciones más comunes:

– Operadores de red (*públicos o privados*);
– Proveedores de servicio (*proveedores de servicio de portador o proveedores de servicio de valor añadido*);
– Abonados de servicio/clientes de servicio;
– Usuarios extremo de servicio;
– Proveedores de equipos y programas informáticos;
– Tercero interesado de confianza.

2.2 Dominios de seguridad de las redes de telecomunicaciones

Un *dominio de seguridad* se define como un conjunto de entidades y partes supeditadas a una política de seguridad y a una gestión de seguridad únicas.

El diseño de la seguridad de la red puede incluir distintos dominios y subdominios para rodear y delimitar las responsabilidades de la gestión de red y del control de seguridad.

Se deben considerar al menos los siguientes aspectos para la segregación de la red en dominios:

• las fronteras de la red física,
• las zonas de responsabilidad,
• los campos de funcionalidades,
• qué tan críticos son las aplicaciones y los datos que se comunican a través de las redes,
• límites geográficos potenciales (establecimientos, aduanas regionales, etc.)
• requisitos/disponibilidad de tráfico y de capacidad,
• requisitos de continuidad y recuperación

- dominio de aplicación comercial,
- dominio de soporte comercial (tarificación, gestión de recursos humanos, etc.),
- dominios de desarrollo y prueba,
- dominios de producción,
- dominio de gestión de alarmas,
- responsabilidades de seguridad de red en materia de gestión y de administración.

Las interfaces en la capa de la red troncal son una zona convencional donde cambian las responsabilidades. La interfaz entre un entorno de producción y un entorno de oficinas, o el entorno de pruebas, son fronteras de funcionalidad de red características. Cada punto de acceso a un dominio y subdominio necesita una pasarela que pueda proporcionar varios servicios de seguridad como control de tráfico, control de acceso, etc.

3 Objetivos de seguridad genéricos para las redes de telecomunicaciones

La finalidad de esta cláusula es describir el objetivo primordial de las medidas de seguridad que se toman en las redes de telecomunicaciones. El objetivo es describir los requisitos de seguridad que pueden lograrse, más que en la manera de hacerlo.

Los objetivos de seguridad para las redes de telecomunicaciones son:

– Únicamente los agentes legítimos deben poder acceder a las redes de telecomunicaciones y utilizarlas.

– Los agentes legítimos deben poder acceder e intervenir en los recursos a los que están autorizados.

– Las redes de telecomunicaciones deben proporcionar la privacidad al nivel fijado por las políticas de seguridad de la red.

– Todos los agentes deberán ser responsables únicamente de sus propias acciones en las redes de telecomunicaciones.

– Para garantizar la disponibilidad, las redes de telecomunicación deben protegerse contra acceso u operaciones no solicitadas.

– Debe ser posible recuperar información relativa a la seguridad de las redes de telecomunicaciones (pero únicamente los agentes legítimos deben poder recuperar dicha información).

– Si se detectan violaciones de la seguridad, éstas deberán manejarse de una forma controlada, de conformidad con el plan predefinido para minimizar los posibles daños.

– Cuando se detecte un problema de seguridad, deberá ser posible restablecer los niveles de seguridad normales.

– La arquitectura de seguridad de las redes de telecomunicaciones debe proporcionar cierta flexibilidad para soportar distintas políticas de seguridad, por ejemplo, diferente rigidez de los mecanismos de seguridad.

El término "acceder a recursos" se entiende no solamente como la posibilidad de realizar funciones sino también de leer información.

Los objetivos genéricos se expresan conforme al punto de vista y al lenguaje de la gestión de la empresa. Las siguientes cláusulas se deben expresar de una manera más técnica que conduzca a servicios y funciones de seguridad susceptibles de implementarse. La correspondencia entre los dos lenguajes no siempre es obvia.

Se puede demostrar que si se cumple con el siguiente conjunto de objetivos de seguridad se podrán satisfacer los primeros cinco objetivos de seguridad antes mencionados en esta subcláusula para las redes de telecomunicaciones:

– confidencialidad;
– integridad de los datos [por supuesto que también se requiere la integridad de los programas del sistema, o de lo contrario, se podría tener un ataque de negación de servicio (DoS)];
– contabilidad, incluyendo autenticación, no repudio y control de acceso;
– disponibilidad.

Las amenazas y los riesgos identificados en la cláusula 5, así como los requisitos funcionales de la cláusula 6 se fundamentarán en estos términos más formales. Véanse las definiciones la cláusula 5.

El resto de los objetivos tienen que ver con la supervisión y el control del estado de seguridad del sistema. Éstos se tratarán en las cláusulas pertinentes relativas a la gestión de recuperación, arquitectura y seguridad conforme a las políticas de seguridad implementadas.

4 Cuestiones relativas a la legislación

La infraestructura de seguridad de una red de telecomunicaciones debe tener la capacidad para dar cabida a limitaciones impuestas por la legislación gubernamental, la legislación contractual, los tratados y la reglamentación. Estas limitaciones pueden incluir servicios de seguridad obligatorios (como garantizar la intimidad de la información del cliente), la exclusión de ciertos mecanismos de seguridad (como algunos tipos de criptación) y/o el soporte de intervención secreta llevada a cabo por los organismos encargados de imponer el cumplimiento de la ley.

5 Amenazas y riesgos

La intención de esta cláusula es explorar las amenazas a las redes de telecomunicaciones y los riesgos a los que éstas hacen frente. No se pretende especificar la evaluación de los riesgos o el análisis de las amenazas relativos a tipos individuales de redes de telecomunicaciones. Éstas son cuestiones locales que pueden manejarse de distintas maneras a través de cada operador sin afectar el interfuncionamiento. Una amenaza es una violación potencial de la seguridad. Conforme a los objetivos de seguridad genéricos identificados, las amenazas pueden estar dirigidas a cuatro clases de objetivos distintos:

– **confidencialidad** (confidencialidad de información almacenada y transferida);
– **integridad de los datos** (protección de información almacenada y transferida);
– **integridad del sistema** (protección del sistema operativo);
– **responsabilización (identificación de responsable)** (toda entidad debe ser responsable de sus acciones iniciadas); y
– **disponibilidad** (todas las entidades legítimas deben disponer de acceso correcto a las redes de telecomunicaciones).

En la presente Recomendación se distinguen tres clases de amenazas:

– amenaza accidental: aquella cuyo origen no incluye ningún intento mal intencionado;
– amenaza administrativa: aquella que surge debido a la falta de gestión de seguridad; y
– amenaza intencional: aquella que incluye una entidad mal intencionada que puede atacar a la propia telecomunicación o a los recursos de la red.

Las amenazas accidentales y administrativas pueden tenerse en cuenta dentro del trabajo de normalización siempre que sus consecuencias sean las mismas de las amenazas intencionales. Para llevar a cabo un análisis más preciso de las amenazas, esta Recomendación se centra en las amenazas intencionales. El objetivo o es obtener una lista corta de amenazas que se pueda utilizar

directamente en el trabajo de normalización. Por consiguiente, un análisis de amenazas debe abordar las siguientes cuestiones, basándose en la Rec. UIT-T X.800:

– **impostura ("simulación")**: una entidad que finge ser una entidad distinta;

– **escucha clandestina**: violación de la confidencialidad al supervisar la telecomunicación;

– **acceso no autorizado**: una entidad que intenta acceder a los datos en violación de la política de seguridad vigente;

– **pérdida o corrupción de la información**: la integridad de los datos transferidos se pone en peligro por supresión, inserción, modificación, reordenación, reproducción o retardo no autorizados;

– **repudio**: una entidad que participa en un intercambio de telecomunicación posteriormente niega el hecho;

– **falsificación**: una entidad fabrica información y reivindica que la misma se recibió de otra entidad o se envió a otra entidad;

– **negación de servicio**: esto ocurre cuando una entidad no puede llevar a cabo su función o evita que otras entidades realicen las suyas. Por ejemplo, al saturar el tráfico de las redes de telecomunicación o de los componentes de una red se puede provocar la negación de acceso a éstas e impedir la telecomunicación. En una red compartida, esta amenaza se puede reconocer como una fabricación de tráfico suplementario que desborda la red, evitando que otros la utilicen mediante el retraso de su tráfico.

En el cuadro 1 se presenta un esquema de las amenazas y los objetivos.

Cuadro 1/E.408 – Correspondencia de las amenazas y los objetivos

Amenazas	Objetivos			
	Confidencialidad	**Integridad del sistema o de los datos**	**Responsabilización**	**Disponibilidad**
Impostura	x	x	x	x
Escucha clandestina	x			
Acceso no autorizado	x	x	x	x
Pérdida o corrupción de información (transferida)		x		x
Repudio			x	
Falsificación		x	x	
Negación de servicio				x

Una amenaza potencial a un sistema no es perjudicial a menos que haya un punto débil correspondiente en el sistema y un instante en el que se aprovecha esa debilidad. Cada amenaza implica un riesgo. La evaluación del riesgo puede dividirse en la evaluación de la probabilidad de cada amenaza y una evaluación de la repercusión que pueda tener. La evaluación de la amenaza y del riesgo debe formar parte de un proceso iterativo. Pueden surgir nuevas amenazas cuando se establecen las contramedidas, por ejemplo, amenazas a las claves criptográficas cuando se utilizan medidas criptográficas.

6 Requisitos de seguridad

En la figura 2 se describen las relaciones entre objetivos de seguridad, amenazas, riesgos, requisitos de seguridad y servicios. Se describe el proceso para deducir los "requisitos de seguridad" a partir

de las "amenazas" y los "objetivos de seguridad", que a su vez se lograrán mediante un conjunto de servicios de seguridad. Estos "servicios" que contrarrestan las amenazas, utilizarán mecanismos que a su vez emplearán "algoritmos de seguridad". Este proceso se indica en la figura 2.

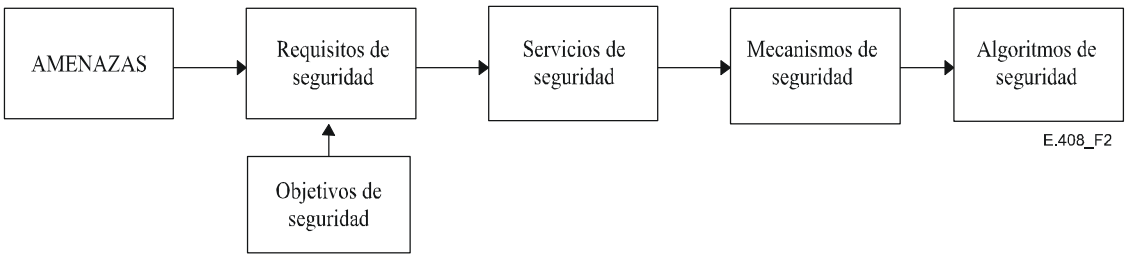

Figura 2/E.408 – Requisitos de seguridad

En la cláusula 6.1 se relacionan los requisitos de seguridad. A menos que se indique lo contrario, en esta Recomendación la palabra "requisito" no significa que alguna funcionalidad es siempre obligatoria en cada red de telecomunicaciones; por el contrario, significa que una funcionalidad puede volverse obligatoria a través de un gestor de red para algunos servicios específicos, aplicaciones y/o interfaces de esa red. La elección efectiva dependerá de los objetivos de seguridad establecidos en las políticas de seguridad del operador.

Además de los requisitos y servicios de seguridad, en esta cláusula también se establecen algunos requisitos genéricos para la gestión de servicios de seguridad (véase 6.2) y requisitos de arquitectura que rigen la integración de los servicios de seguridad en una arquitectura de red genérica (véase 6.3). Los requisitos de gestión y de ciclo vital son importantes pero no afectarán a la arquitectura y se dejan fuera de esta cláusula.

Los requisitos de seguridad pueden aplicarse a cada aspecto de seguridad de la arquitectura de seguridad normalizada en la Rec. UIT-T X.805. Las dimensiones de seguridad (también de la Rec. UIT-T X.805) están previstas para cumplir los requisitos de seguridad en todos los casos. Los servicios de seguridad, mecanismos de seguridad y algoritmos de seguridad que se tratan en la presente Recomendación deben considerarse partes integrantes de cada dimensión de seguridad.

6.1 Requisitos de seguridad y servicios correspondientes

En esta cláusula se describe un conjunto de requisitos funcionales genéricos y los servicios correspondientes que pueden utilizarse para contrarrestar las amenazas a las redes de comunicación.

6.1.1 Correspondencia de requisitos funcionales, amenazas y objetivos de seguridad

En esta cláusula se identifican los requisitos de seguridad funcionales que abarcan las amenazas indicadas en la cláusula 5, como se muestra en el cuadro 2. A partir de este cuadro se han hecho corresponder los requisitos de seguridad (cuadro 3) a los objetivos de seguridad determinados en la cláusula 3. La relación se limita a los requisitos que son de naturaleza genérica y que tienen una repercusión considerable en los componentes y en la arquitectura.

Cuadro 2/E.408 – Correspondencia de los requisitos funcionales y las amenazas

Requisitos funcionales	Amenazas						
	Impostura	**Escucha clandestina**	**Acceso no autorizado**	**Pérdida o corrupción de información**	**Repudio**	**Falsificación**	**Negación de servicio**
Verificación de identidades	x		x				
Control de acceso y autorización			x				x
Protección de confidencialidad		x	x				
Protección de la integridad de los datos				x			
Identificación de entidad responsable					x	x	
Registro de la actividad	x		x		x	x	x
Informe de alarmas	x		x	x			x
Auditoría	x		x		x	x	x

Los objetivos que se emplean son los cuatro formales definidos en la cláusula 3, a cada uno de los cuales corresponde una columna en el cuadro 3, que indica el conjunto de requisitos funcionales necesarios para satisfacer el objetivo en cuestión.

6.1.2 Descripción de los requisitos funcionales y de las funciones correspondientes

Los requisitos funcionales de los cuadros 2 y 3 se examinan con mayor detalle en el texto a continuación y se identifican las funciones de seguridad correspondientes a cada uno de los requisitos. Obsérvese que los requisitos para cualquiera de estas funciones no invocan de manera automática un servicio de seguridad como lo define ISO. Si bien, en la práctica, hay coincidencia en algunos casos.

Cuadro 3/E.408 – Correspondencia de los objetivos de seguridad y de los requisitos funcionales

Requisitos funcionales	Objetivos de seguridad			
	Confidencialidad	**Integridad del sistema o de los datos**	**Responsabilización**	**Disponibilidad**
Verificación de las identidades	x	x	x	
Control de acceso y de autorización	x	x	x	x
Protección de confidencialidad	x	x		
Protección de la integridad del sistema o de los datos		x		
Responsabilización			x	
Registro de la actividad			x	x
Informe de alarmas	x	x	x	x
Auditoría			x	x

NOTA – Se considera que mantener la confidencialidad de los datos es una condición suficiente para conservar la integridad de los datos, es decir, si se pueden mantener los datos confidenciales al mismo tiempo se protegerán contra su alteración. No obstante, la protección contra su alteración no los protege necesariamente contra su divulgación.

6.1.2.1 Verificación de las identidades

Una red de telecomunicación debe disponer de las capacidades necesarias para establecer y verificar la identidad pretendida de cualquier agente en la red de telecomunicaciones.

Los agentes pueden ser usuarios físicos o entidades dentro de la red de telecomunicaciones. La verificación de las identidades proporciona la base de la identificación de responsable y es fundamental para satisfacer la mayoría de los requisitos de seguridad relacionados en esta subcláusula.

El servicio de seguridad para soportar el requisito es la **autenticación**. La función de autenticación proporciona la prueba de que la identidad de un objeto o sujeto es realmente la que se pretende. En función del tipo de agente y de la finalidad de la identificación, pueden ser necesarias las siguientes clases de autenticación:

– autenticación de usuario, que establece la prueba de la identidad del usuario físico o del proceso de solicitud de acceso;

– autenticación de la entidad par, que establece la prueba de la identidad de la entidad par durante una relación de telecomunicación;

– autenticación del origen de los datos, que establece la prueba de la identidad del responsable de una unidad de datos particular.

La utilización de la función de autenticación establece la prueba durante un determinado periodo de tiempo. Para garantizar la prueba continua, se tiene que repetir la autenticación o vincularse a un servicio de integridad.

Algunos ejemplos de mecanismos utilizados para implementar el servicio de autenticación son las contraseñas y los números de identificación personal (PIN, *personal identification numbers*) (autenticación simple) y los métodos criptográficos (autenticación sólida).

6.1.2.2 Control de acceso y autorización

Una red de telecomunicación debe disponer de las capacidades necesarias para garantizar que se pueda evitar que los agentes accedan a información o recursos a los que no están autorizados.

El servicio de seguridad necesario para satisfacer este requisito es el **control de acceso**. Este servicio proporciona los medios para garantizar que sólo personas autorizadas acceden a los recursos. Los recursos en cuestión pueden ser el sistema físico, el sistema informático, las aplicaciones y los datos. La función de control de acceso puede definirse e implementarse en distintos niveles de precisión de la red de telecomunicaciones: a nivel de agente, a nivel de objeto o a nivel de atributo. Las limitaciones de acceso se establecen en la información de control de acceso, que especifica:

– los medios para determinar qué entidades están autorizadas para acceder;

– qué clase de acceso está permitido (lectura, escritura, modificación, creación, supresión).

Más específicamente, el control de acceso a la red de telecomunicaciones puede dividirse en tres tipos:

– *Control de acceso a la asociación de gestión*

  Permite el control de acceso al nivel de asociación de gestión, lo que significa que los derechos de acceso están relacionados con la propia asociación, es decir, el derecho a establecer la asociación.

– *Control de acceso a la notificación de gestión*

  Permite el control de acceso relativo a las notificaciones, es decir, para garantizar que las notificaciones se revelen únicamente a las entidades autorizadas para recibirlas.

– *Control de acceso a los recursos gestionados*

  Ofrece el control de acceso relativo a los propios recursos.

Se debe verificar la identidad de la entidad que intenta acceder antes de que se conceda el acceso al recurso. Esto significa que la utilización del control de acceso siempre está vinculada a la utilización de un servicio de autenticación.

6.1.2.3 Protección de la confidencialidad

Una red de telecomunicación debe disponer de las capacidades necesarias para garantizar la confidencialidad de los datos almacenados y comunicados.

Los servicios de seguridad necesarios para soportar el recurso son: **control de acceso** a los sistemas, **control de acceso** a datos almacenados y **confidencialidad de los datos** telecomunicados.

La infracción a un sistema de confidencialidad no debe pasarse por alto ya que en muchos casos es la señal precursora a los ataques a la integridad del sistema o de los datos (permite que los atacantes encuentren vulnerabilidades del tipo DoS).

El servicio de confidencialidad proporciona la protección contra la revelación no autorizada de datos almacenados o intercambiados. Se distinguen las siguientes clases de confidencialidad:

– confidencialidad de sistema (incluye información tan diversa como la información de arquitectura y de configuración, algoritmos que se emplean, números de versión de los programas informáticos, tipos de los equipos utilizados, etc.);

– confidencialidad de campo selectivo;

– confidencialidad de conexión;

– confidencialidad de flujo de datos.

6.1.2.4 Protección de la integridad del sistema y de los datos

Una red de telecomunicación debe poder garantizar la integridad de los sistemas y de los datos almacenados y comunicados.

Los servicios de seguridad necesarios para soportar el requisito son: **control de acceso** a los sistemas, **control de acceso** a los datos almacenados e **integridad de los datos** comunicados.

El servicio de integridad proporciona los medios para garantizar la exactitud de los ficheros del sistema y de los datos intercambiados, protegiéndolos contra modificación, supresión, creación (inserción) y reproducción. Se distinguen las siguientes clases de integridad:

– integridad del sistema operativo;
– integridad del campo selectivo;
– integridad de conexión sin recuperación;
– integridad de conexión con recuperación.

6.1.2.5 Responsabilización

Una red de telecomunicación debe disponer de la capacidad necesaria para que una entidad no pueda negar la responsabilidad de cualquiera de sus acciones así como de sus efectos. *Por ejemplo, una red de telecomunicaciones debe proporcionar las pruebas de que una entidad ha llevado a cabo una acción concreta.*

El requisito se soporta mediante el servicio de **no repudio** que vincula al individuo (o entidad) con la operación ejecutada. Los servicios de no repudio ofrecen los medios para probar que realmente se efectuó un intercambio de datos y que los usuarios están conscientes del contexto legal que protege la utilización del servicio o producto (por ejemplo, conscientes de que la utilización está siendo supervisada, etc., que típicamente se logra a través de la utilización de rótulos durante el proceso de conexión). Existen tres formas:

– no repudio: prueba de origen;
– no repudio: prueba de entrega;
– no repudio: prueba de conocimiento del contexto jurídico.

Se puede lograr otra realización de la contabilidad más general y posiblemente menos estricta a través de combinaciones adecuadas de los servicios de **autenticación**, **control de acceso** y **registro de auditoría**.

6.1.2.6 Actividad de registro, informe de alarmas y auditorías

Estos requisitos tienen que ver con la necesidad de almacenar y analizar la información relativa a las actividades pertinentes a la seguridad dentro de la red de telecomunicaciones. Los servicios apropiados son **registro de actividad**, **registro de auditoría** e **informe de alarmas**. Cada uno de estos requisitos se analiza más adelante de forma detallada.

6.1.2.6.1 Registro de actividad

Una red de telecomunicaciones debe disponer de la capacidad necesaria para almacenar información relativa a las actividades que se realizan en el sistema con la posibilidad de rastrear esta información hasta las personas o entidades que las ejecutan.

Un registro es un depósito de eventos: ésta es la abstracción de OSI de los recursos de registro en los sistemas abiertos reales. Los eventos contienen la información que se registra.

Para la finalidad de muchas funciones de gestión, es necesario poder preservar la información relativa a los eventos ocurridos o a las operaciones que se han realizado o intentado a través de distintos recursos o en ellos.

Además, cuando esa información se recupera de un registro, el gestor debe ser capaz de determinar si se perdieron algunos eventos o si las características de los eventos almacenados en el registro sufrieron modificaciones en algún momento.

Ya que los ficheros de registro constituyen parte de los datos del sistema, este requisito también tendrá necesidad del requisito 6.1.2.4 y posiblemente del 6.1.2.3.

6.1.2.6.2 Notificación de alarmas de seguridad

Una red de telecomunicaciones debe disponer de la capacidad necesaria para generar notificaciones de alarmas relativas a eventos seleccionados. El usuario debe tener la capacidad para definir los criterios de selección.

La función de control de auditoría de seguridad es una función de gestión de los sistemas que describe el proceso de notificación de la recopilación de eventos de seguridad. La notificación de alarmas de seguridad definida por esta función de gestión de los sistemas proporciona información relativa a la condición de funcionamiento relacionada a la seguridad.

6.1.2.6.3 Auditoría de seguridad

Una red de telecomunicaciones debe disponer de la capacidad necesaria para analizar datos de registro relativos a los eventos pertinentes de seguridad a fin de verificarlos con referencia a las violaciones de las políticas de seguridad.

Una auditoría se debe considerar como una revisión y examen independientes de los registros y actividades del sistema para probar si los controles del sistema son adecuados, garantizar la conformidad a la política y procedimientos operacionales de seguridad establecidos y para detectar las infracciones en los sistemas de seguridad. El resultado de la auditoría permitirá identificar los cambios de control, de política y de procedimientos.

En el cuadro 4 se presenta una síntesis de la relación entre los requisitos y los servicios de seguridad. En esta cláusula se definen únicamente los servicios de seguridad considerados por las soluciones normalizadas; otros servicios posibles (por ejemplo, detección o negación de servicio) se consideran fuera de su alcance.

Cuadro 4/E.408 – Correspondencia de los requisitos de seguridad y los servicios de seguridad

Requisito funcional	Servicio de seguridad
Verificación de identidades	Autenticación de usuario Autenticación de entidad par Autenticación de origen de los datos
Control de acceso y autorización	Control de acceso
Protección de la integridad del sistema	Control de acceso
Protección de la confidencialidad – datos almacenados	Control de acceso
Protección de la confidencialidad – datos transferidos	Confidencialidad
Protección de la integridad de los datos – datos almacenados	Control de acceso
Protección de la integridad de los datos – datos transferidos	Integridad
Responsabilización	No repudio
Registro de actividad	Registro de auditoría
Notificación de alarmas de seguridad	Alarma de seguridad
Auditoría de seguridad	Registro y recuperación de auditoría

NOTA – Los siguientes requisitos no son del mismo tipo que se expresó antes del cuadro 4 y no se pueden considerar como candidatos obvios para ser objeto de una Recomendación. Sin embargo, se deben tener en cuenta durante la fase de diseño junto con la implantación de los requisitos de seguridad principales de la red de telecomunicaciones antes expresados.

6.1.2.6.4 Integridad del sistema

Es esencial que el entorno de programas informáticos y equipo de las funciones de seguridad implementadas mantengan el nivel de seguridad solicitado.

Esto incluye la configuración precisa de los sistemas operativos y la eliminación de los defectos del sistema.

Estos aspectos no forman parte del propio perfil de seguridad funcional, pero tienen que establecerse junto con esas especificaciones para garantizar la firmeza de las funciones en el entorno del mundo real.

6.1.2.6.5 Comentarios sobre la disponibilidad

Un requisito relativo a la disponibilidad no tiene un conjunto simple o limitado de servicios de seguridad que puedan satisfacerlo. Todos los servicios de seguridad relacionados en este documento deben constituir un conjunto congruente que pueda mantener la disponibilidad. Si bien, los servicios de seguridad solos nunca podrán garantizar la disponibilidad que también es una cuestión de fiabilidad del equipo y de los programas informáticos (desde un punto de vista de diseño y de implementación).

6.2 Requisitos sobre la gestión de la seguridad

Una red de telecomunicación debe incluir modelos de información y capacidades de gestión para los servicios utilizados para la seguridad de la red de telecomunicaciones.

Los requisitos pormenorizados relativos a la gestión de seguridad determinan qué aplicaciones de gestión se deben introducir y cómo se deben diseñar. Esto se lleva a cabo para dotar al gestor con las herramientas de seguridad adecuadas para supervisar y controlar los servicios de seguridad de una manera eficaz y correcta. Los objetivos y las metas del gestor de seguridad se presentan en tres niveles distintos de un sistema de telecomunicaciones, que corresponden a la gestión de la seguridad del sistema, los servicios de seguridad y los mecanismos de seguridad, respectivamente.

Se ha de soportar la recuperación a un estado seguro del sistema después de una infracción a la seguridad.

Cuando se produce una infracción a la seguridad, la red de telecomunicaciones debe ser capaz de manejar esa tentativa de un modo controlado, lo que significa que el intento no debe dar por resultado una degradación grave de la red de telecomunicaciones en términos de disponibilidad.

Las operaciones y la información relativa a la gestión de los servicios de seguridad en la red de telecomunicaciones necesitan una consideración especial desde un punto de vista de seguridad. Las claves secretas de encripción, la información de autenticación y las relaciones de control de acceso son ejemplos en los que la rigidez necesaria de la protección puede ser superior que aquella para la gestión de red.

6.3 Servicios de seguridad y capas OSI

En esta cláusula se describe cuáles son las capas de OSI que se utilizan para proporcionar servicios de seguridad y por consiguiente se muestra cómo se pueden aprovechar en las redes de telecomunicaciones de una manera significativa.

Se supone que si una capa ofrece un servicio de seguridad, el mismo se proporciona a la capa por encima de la capa considerada. La prestación de servicios por capas que se establece en la Rec. UIT-T X.800 se utiliza como la base para limitar las posibilidades.

6.3.1 Autenticación (entidad par y origen de los datos)

Las siguientes capas pueden proporcionar este servicio (conforme a la Rec. UIT-T X.800):

– capa de red (corroboración de la identidad de las entidades pares de la capa de transporte);

– capa de transporte (corroboración de la identidad de las entidades pares de la capa de sesión);

– capa de aplicación (corroboración de la identidad de los procesos de aplicación);

– fuera de OSI: en el propio proceso de aplicación.

6.3.2 Control de acceso

– *Control de acceso a la asociación de gestión*

Este servicio es útil en aquellos niveles en los que existe una asociación; esto será en la capa de aplicación (control de acceso para los procesos de aplicación) o en el propio proceso de aplicación.

El control de acceso a la asociación se puede proporcionar en la capa de red. Por consiguiente, el control de acceso a la asociación se puede proporcionar en la capa de aplicación o en el propio proceso de aplicación.

– *Control de acceso a la notificación de gestión*

Este servicio se puede utilizar en la capa de aplicación o en el propio proceso de aplicación, ya que es el mismo proceso de aplicación el que discrimina entre (proceso de aplicación) entidades como los gestores y los agentes.

– *Control de acceso a los recursos gestionados*

Este servicio se puede utilizar en la capa de aplicación o en el propio proceso de aplicación, ya que es el mismo proceso de aplicación el que discrimina entre (proceso de aplicación) entidades como los gestores y los agentes.

6.3.3 Alarmas de seguridad, registro y recuperación de auditoría

Estos servicios están vinculados a otros servicios y por consiguiente están presentes en aquellas capas donde existen los otros servicios.

6.3.4 Integridad

– *Integridad de campo selectiva*

Este servicio se puede utilizar en la capa de aplicación o en el propio proceso de aplicación, ya que es el proceso de aplicación que puede discriminar entre campos.

– *Integridad de conexión con recuperación*

Se puede proporcionar en la capa de transporte, en la capa de aplicación o en el proceso de aplicación.

– *Integridad de la conexión sin recuperación*

Se puede proporcionar en la capa de red, en la capa de transporte, en la capa de aplicación o en el proceso de aplicación.

6.3.5 Confidencialidad

– *Confidencialidad de campo selectiva*

Este servicio se puede utilizar en la capa de aplicación o en el propio proceso de aplicación, ya que es el proceso de aplicación que puede discriminar entre campos.

– *Confidencialidad con conexión y sin conexión*

Considerando que se necesita la confidencialidad extremo a extremo, que excluye la capa física y la capa de enlace de datos, la confidencialidad se puede proporcionar en la capa de

red, en la capa de transporte, en la capa de presentación, en la capa de aplicación o en el proceso de aplicación.

– *Confidencialidad de flujo de tráfico*

  Este servicio se puede proporcionar en las capas de red, de transporte o de aplicación, o en el proceso de aplicación.

6.3.6 No repudio

– no repudio – prueba de emisión;

– no repudio – prueba de entrega.

  Este servicio se puede utilizar en la capa de presentación, en la capa de aplicación o en el propio proceso de aplicación.

Esto se resume en el cuadro 5. El cuadro 5 no es idéntico al cuadro 2 de la Rec. UIT-T X.800, dada la diferencia de ámbito de aplicación de ambas Recomendaciones.

Cuadro 5/E.408 – Vinculación de los servicios de seguridad y el modelo de referencia OSI

	Capa						
Servicio	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Autenticación de usuario	–	–	–	–	–	–	+
Autenticación de entidad par	–	–	+	+	–	–	+
Autenticación de origen de los datos	–	–	+	+	–	–	+
Control de acceso a la asociación de gestión	–	–	+	–	–	–	+
Control de acceso a la notificación de gestión	–	–	–	–	–	–	+
Control de acceso a los recursos gestionados	–	–	–	–	–	–	+
Alarmas de seguridad, registro y recuperación de auditoría	+	+	+	+	+	+	+
Integridad de campo selectivo	–	–	–	–	–	–	+
Integridad de conexión con recuperación	–	–	–	+	–	–	+
Integridad de conexión sin recuperación	–	–	+	+	–	–	+
Confidencialidad de campo selectivo	–	–	–	–	–	–	+
Confidencialidad con conexión/sin conexión	–	–	+	+	–	+	+
Confidencialidad de flujo de tráfico	–	–	+	+	–	+	+
No repudio – prueba de emisión	–	–	–	–	–	+	+
No repudio – prueba de entrega	–	–	–	–	–	+	+

6.4 Gestión de seguridad

La gestión de seguridad consta de todas las actividades para establecer, mantener y terminar los aspectos de seguridad de un sistema.

Los temas abarcados son:

– gestión de los servicios de seguridad;

– instalación de los mecanismos de seguridad;

– gestión de claves (parte de gestión);

– determinación de identidades, claves, información de control de acceso, y otros;

– gestión de registro de auditoría de seguridad y alarmas de seguridad;
– sensibilidad a la seguridad y entrenamiento;
– estrategia de seguridad;
– políticas y reglamentos de seguridad;
– gestión de seguridad colaborativa.

Apéndice I

Cuestiones jurídicas

I.1 Introducción

En esta cláusula se describen las cuestiones jurídicas que pueden tener influencia sobre la normalización de la seguridad en la red de telecomunicaciones y además se presentan algunas consecuencias de dichas cuestiones.

I.2 Cuestiones jurídicas aplicables

Se han identificado las siguientes cuestiones jurídicas con posible influencia en la normalización de la seguridad de la red de telecomunicaciones:

Privacidad

– "Privacidad de carta": mantiene la información intercambiada entre clientes fuera del alcance de terceros no autorizados.
– Limitaciones en la recopilación, almacenamiento y procesamiento de datos personales: los datos personales solamente pueden recopilarse, almacenarse y procesarse si existe una relación entre los datos y la prestación real de los servicios.
– Difusión: obligación de un operador de red a mantener la información relativa a los clientes fuera del alcance de terceros no autorizados.
– "Inspección y corrección": derecho del cliente a inspeccionar y corregir información relativa a él mismo que se encuentra almacenada por el operador de red, siempre y cuando esté justificado.

La cuestión sobre la privacidad tendrá influencia principalmente sobre los requisitos de seguridad relativos al control de acceso, integridad y confidencialidad.

Contractual

– Posibilidad de utilizar información relativa a la telecomunicación entre entidades en caso de una controversia en un tribunal.
– Reconocimiento de un contrato entregado electrónicamente en un tribunal.

Los requisitos de seguridad relativos a la integridad y al no repudio serán los más afectados.

Seguridad internacional y orden público nacional

– Demandas relativas a la protección apropiada de información e infraestructura: garantiza la disponibilidad e integridad de la red de telecomunicación.
– Restricciones relativas a la utilización de métodos criptográficos: algunos países tienen leyes que restringen la utilización de criptación.
– Obligación de los operadores de red a cooperar y suministrar información en caso de intercepción lícita en el marco de investigaciones criminales.

Esta cuestión puede tener repercusión en los requisitos de seguridad. La repercusión de la cuestión de intercepción jurídica sobre los requisitos es poco clara. No obstante, hay una relación con la privacidad, por ejemplo, sólo se debe proporcionar información relativa a la persona que está siendo investigada.

I.3 Fuentes de legislación

En la cláusula anterior, las cuestiones jurídicas se categorizaron por temas. A continuación se identifican algunas de sus fuentes y su repercusión posible en la seguridad de la red de telecomunicación.

– *Constituciones nacionales*

  Abarca la confidencialidad de la correspondencia, el derecho de privacidad, el derecho de la libertad personal, y otros. No todas las constituciones se refieren específicamente a las telecomunicaciones.

– *Tratados internacionales*

  Los tratados de Roma y de Maastricht son dos ejemplos. En el presente documento hay dos cuestiones jurídicas importantes para telecomunicaciones: la primera es relativa al mercado europeo (denominada "primer pilar"), que trata de la competencia en el mercado (telecomunicaciones): lo que resulta importante en materia de seguridad son los "requisitos esenciales" relativos a la seguridad y a la integridad de las redes y a la protección de los datos. La segunda área ("tercer pilar") está relacionada con la cooperación europea en el campo de la justicia: los puntos principales de esta cuestión relativos a la seguridad son los requisitos sobre la intercepción legal. Estos requisitos incluyen el contenido de la llamada, los datos asociados con la llamada y la ubicación del objetivo. Algunos aspectos importantes relativos a la seguridad de la red de telecomunicaciones podrían ser los siguientes: *es preciso disponer de disposiciones específicas para confidencialidad, integridad y auditoría durante el proceso de intercepción*.

– *Otros convenios internacionales*

  Muchos de estos convenios tratan de los derechos humanos, relativos a las telecomunicaciones; la privacidad y la confidencialidad son los más importantes. Los derechos de autor no se consideran importantes para la seguridad de la red de telecomunicaciones.

– *Leyes nacionales*

  De manera similar las leyes aplicables tratan de la privacidad, confidencialidad e intercepción legal.

– *Normas emitidas por el organismo de reglamentación de las telecomunicaciones nacional* (NTR, *national telecommunications regulator*)

  El organismo de reglamentación es el organismo nacional (designado a través de la ley nacional) al que se le otorga la autoridad para que emita reglas y reglamentos en materia de telecomunicaciones. Dichas reglas pueden incluir cuestiones de seguridad.

– *Códigos de prácticas*

  Políticas acordadas entre las empresas de telecomunicaciones y las organizaciones para abordar las cuestiones de seguridad. En el caso de la seguridad de la red de telecomunicaciones, estos códigos de prácticas pueden convertirse en una cuestión importante cuando se interconectan redes de telecomunicaciones.

I.4 Posibles consecuencias de la normalización de la seguridad de la red de telecomunicaciones

En el caso de la normalización de la seguridad de la red de telecomunicaciones, se prevén y se deben tener en cuenta las siguientes consecuencias relativas a las cuestiones jurídicas:

– Las cuestiones jurídicas pueden dar por resultado requisitos con relación a la firmeza y a la disponibilidad de los servicios de seguridad. En las cláusulas anteriores se presentaron algunas indicaciones relativas a estos requisitos.

– Necesidad de disponer de un determinado nivel de integridad de la red de telecomunicaciones.

– Posibilidad de soportar la intercepción jurídica y el acceso a los datos de gestión por parte de los departamentos de justicia. Periodo de tiempo en el que los datos necesitan estar almacenados, y los procesos para garantizar que los datos se destruyan cuando proceda.

– La legislación puede dar por resultado la inhibición de la utilización de la criptación en algunos países.

– La legislación no será la misma en distintos países. Eso significa que pueden surgir diferentes requisitos para distintos países.

Apéndice II

Clases funcionales y subperfiles de seguridad

II.1 Agrupación de las medidas de seguridad

Las medidas de seguridad se pueden agrupar en "clases funcionales" (FC, *functional classes*). La siguiente definición no incluye la severidad de la medida de seguridad:

Una clase funcional es un conjunto coherente de medidas de seguridad para satisfacer los requisitos de seguridad de diversos niveles funcionales.

II.1.1 Utilización de las clases funcionales en el caso entre dominios

La seguridad de la red de telecomunicaciones no se debe ver afectada negativamente como resultado de las actividades entre dominios. Las reglas para la interacción entre dominios debe definirse en una política de seguridad entre éstos. Estas reglas definirán qué medidas de seguridad se deben utilizar en cada caso. Para facilitar el acuerdo entre los dominios que interactúan, estas medidas de seguridad se pueden referir como una clase funcional particular.

II.1.2 Utilización de las clases funcionales en el caso interno a un dominio

En el caso interno a un dominio, las clases funcionales pueden facilitar la definición de la seguridad. Además, las clases funcionales pueden utilizarse para la finalidad de garantizar la seguridad. Para lograrlo, las clases funcionales deben asociarse a un nivel de garantía pretendida por el fabricante de los productos de gestión. Este tema tiene fuertes relaciones con los criterios de evaluación formal.

Puede ser posible que, para los fines de interacción entre dominios, un operador requiera la aplicación de una clase funcional particular para el caso dentro del dominio del otro operador. La razón podría ser que no todas las amenazas se pueden manejar eficientemente en la interfaz entre dos dominios. La garantía de que existe un nivel de seguridad interno mínimo para las redes de telecomunicaciones que interactúan puede ser una solución para lo anterior. Una norma de seguridad de red de telecomunicaciones no debe recomendar que se requieren clases funcionales, sino que debe permitir la posibilidad de solicitar determinadas clases funcionales, definiendo los puntos adecuados para la selección.

II.2 Clases funcionales

Las clases funcionales se utilizan para definir un grupo concreto de servicios de seguridad orientados a satisfacer un nivel de seguridad determinado. En esta cláusula se desarrolla un conjunto de clases funcionales que sirve como un ejemplo sobre cómo se pueden definir las clases funcionales. Las clases funcionales *para la interfaz X* se proponen entre tres niveles de seguridad distintos:

1) clase funcional mínima: (FC 1);

2) clase funcional básica: (FC 2);

3) clase funcional avanzada: (FC 3).

Para fines prácticos, el número de clases funcionales no debe ser demasiado alto. Por otro lado, debe ser posible hacer corresponder los requisitos de muchas organizaciones distintas. Las clases funcionales se pueden modificar de las siguientes maneras:

– Las clases funcionales definidas únicamente para la interfaz X también pueden incluir las interfaces Q.

– Se supone que la confidencialidad es una característica facultativa para todas las clases por dos razones:

  • es un requisito menos estricto;

  • la inclusión obligatoria en una clase funcional puede tener repercusiones jurídicas para la posibilidad de uso de la clase.

En el cuadro II.1 se presenta una síntesis de las clases funcionales.

Cuadro II.1/E.408 – Clases funcionales de los servicios de seguridad

FC 1	FC 2	FC 3
Énfasis en la integridad de los recursos gestionados almacenados	Énfasis en la integridad de los recursos gestionados almacenados y en la integridad de los datos transferidos	Clase funcional 2 y la contabilidad de las operaciones de gestión
• Autenticación (entidad y usuario pares) • Control de acceso a la asociación de gestión • Control de acceso a los recursos gestionados • Alarmas de seguridad, auditoría y recuperación	• Autenticación (entidad y usuario pares) • Control de acceso a la asociación de gestión • Control de acceso a los recursos gestionados • Autenticación del origen de los datos • Integridad de campo selectiva • Integridad de conexión • Alarmas de seguridad, auditoría y recuperación	• Autenticación (entidad y usuario pares) • Control de acceso a la asociación de gestión • Control de acceso a los recursos gestionados • Autenticación del origen de los datos • Integridad de campo selectiva • Integridad de conexión • No repudio del origen • No repudio del destino • Alarmas de seguridad, auditoría y recuperación
Facultativo: • Integridad de la conexión • Confidencialidad de la conexión	Facultativo: • Confidencialidad de la conexión • Confidencialidad selectiva de campo	Facultativo: • Confidencialidad de la conexión • Confidencialidad selectiva de campo

Adicionalmente, se debe efectuar una distinción entre las clases funcionales aplicables a los casos entre dominios y a los casos internos a un dominio. Los requisitos serán distintos en ambos casos y por esa razón las medidas de seguridad también podrían ser distintas.

En la siguiente parte se da una síntesis de los distintos casos de modo que se pueda encontrar qué clases funcionales son necesarias y cuáles son pertinentes.

Suposición

Para cada dominio, existe una autoridad responsable de decidir cuáles medidas de seguridad se deben aplicar en él.

Se distinguen tres casos:

1) FC definidas por una autoridad de dominio y aplicables al propio dominio (interno al dominio).
2) FC definidas por una autoridad de dominio y aplicables a las interacciones entre dominios. Estas FC serán el resultado de un acuerdo entre las autoridades de los dominios que interactúan.
3) Las FC definidas por una autoridad de dominio como requisitos para la seguridad interna del otro dominio.

En cada caso, se puede identificar el número de FC para distintos niveles de seguridad.

La cantidad de niveles de seguridad queda en estudio.

El conjunto de medidas de seguridad que constituyen una FC queda en estudio.

En los distintos casos las FC podrían ser iguales, reduciendo así el número total de FC.

Se puede considerar una relación de compromiso entre los distintos casos, por ejemplo, cuando la seguridad entre dominios se encuentra en un nivel superior, los requisitos relativos a la seguridad interna en el otro dominio podrían estar en un nivel inferior y viceversa. Otra posibilidad puede ser que una FC represente un conjunto mínimo de medidas de seguridad que se pueden ampliar con medidas adicionales según proceda.

II.3 Perfiles de seguridad

Las clases funcionales no tienen necesidad de utilizar mecanismos de seguridad normalizados; se puede aplicar cualquier mecanismo que satisfaga los requisitos.

Para facilitar la interacción entre las medidas de seguridad en distintos dominios, las medidas deben ser conformes a las normas. Una recomendación de la utilización de normas particulares que conjuntamente constituyen una clase funcional se denomina un perfil de seguridad.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2004