Unión Internacional de Telecomunicaciones

UIT-T M.3016.0

(05/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE M: GESTIÓN DE LAS TELECOMUNICACIONES, INCLUIDA LA RGT Y EL MANTENIMIENTO DE REDES

Red de gestión de las telecomunicaciones

Seguridad en el plano de gestión: Visión general

Recomendación UIT-T M.3016.0

UIT-T

ITU Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE M

GESTIÓN DE LAS TELECOMUNICACIONES, INCLUIDA LA RGT Y EL MANTENIMIENTO DE REDES

Introducción y principios generales de mantenimiento y organización del mantenimiento	M.10–M.299
Sistemas internacionales de transmisión	M.300–M.559
Circuitos telefónicos internacionales	M.560–M.759
Sistemas de señalización por canal común	M.760–M.799
Circuitos internacionales utilizados para transmisiones de telegrafía y de telefotografía	M.800–M.899
Enlaces internacionales arrendados en grupo primario y secundario	M.900–M.999
Circuitos internacionales arrendados	M.1000–M.1099
Sistemas y servicios de telecomunicaciones móviles	M.1100–M.1199
Red telefónica pública internacional	M.1200–M.1299
Sistemas internacionales de transmisión de datos	M.1300–M.1399
Designaciones e intercambio de información	M.1400–M.1999
Red de transporte internacional	M.2000–M.2999
Red de gestión de las telecomunicaciones	**M.3000–M.3599**
Redes digitales de servicios integrados	M.3600–M.3999
Sistemas de señalización por canal común	M.4000–M.4999

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

Recomendación UIT-T M.3016.0

Seguridad en el plano de gestión: Visión general

Resumen

En la presente Recomendación se expone una visión general y el marco de la seguridad en la red de gestión de las telecomunicaciones (RGT), en virtud de los cuales se identifican las amenazas a la seguridad de esta red, y se describe la manera de aplicar los servicios de seguridad disponibles en el contexto de la arquitectura funcional de la RGT.

Orígenes

La Recomendación UIT-T M.3016.0 fue aprobada el 22 de mayo de 2005 por la Comisión de Estudio 4 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

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 M.3016.0

Seguridad en el plano de gestión: Visión general

1 Alcance

En la presente Recomendación se expone una visión general y el marco de la seguridad de la red de gestión de las telecomunicaciones (RGT), en virtud de los cuales se identifican las amenazas a la seguridad de esta red, y se describe la manera de aplicar los servicios de seguridad disponibles en el contexto de la arquitectura funcional de la RGT, según figura en la Rec. UIT-T M.3010.

Esta Recomendación es de carácter genérico y en ella no se precisan ni se analizan los requisitos de una interfaz de la RGT específica.

No se pretende en la misma definir nuevos servicios de seguridad, sino que se hace referencia a los ya existentes definidos en otras Recomendaciones UIT-T y Normas de la ISO.

Esta Recomendación forma parte de las Recomendaciones UIT-T de la serie M.3016.x que tiene por objeto formular directrices y recomendaciones para la seguridad en el plano de gestión de las redes en evolución:

Rec. UIT-T M.3016.0 – *Seguridad en el plano de gestión: Visión general*.

Rec. UIT-T M.3016.1 – *Seguridad en el plano de gestión: Requisitos de seguridad*.

Rec. UIT-T M.3016.2 – *Seguridad en el plano de gestión: Servicios de seguridad*.

Rec. UIT-T M.3016.3 – *Seguridad en el plano de gestión: Mecanismo de seguridad*.

Rec. UIT-T M.3016.4 – *Seguridad en el plano de gestión: Formulario del perfil de seguridad*.

En las Recs. UIT-T M.3016.1, M.3016.2 y M.3016.3 se especifica un conjunto de requisitos, servicios y mecanismos, a fin de lograr la seguridad de las funciones de gestión necesarias para soportar la infraestructura de telecomunicaciones. En dichas Recomendaciones no se señala si un determinado requisito/servicio/mecanismo es obligatorio o facultativo ya que las distintas administraciones y organizaciones requieren niveles diferentes de soporte de seguridad.

El formulario definido en la Rec. UIT-T M.3016.4 tiene por objeto ayudar a las organizaciones, administraciones y otros organismos nacionales e internacionales a especificar el soporte obligatorio y facultativo de los requisitos, así como las gamas de valores, valores, etc., necesarios para aplicar sus políticas de seguridad.

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 E.408 (2004), *Requisitos de seguridad para las redes de telecomunicaciones*.

– Recomendación UIT-T M.3010 (2000), *Principios para una 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), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*

– Recomendación UIT-T X.741 (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 de interconexión de sistemas abiertos para aplicaciones del CCITT*.

– Recomendación UIT-T X.802 (1995), *Tecnología de la información – Modelo de seguridad de capas más bajas*.

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

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

– Recomendación UIT-T X.812 (1995), *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), *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo*.

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

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

– Recomendación UIT-T X.816 (1995), *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*.

3 Definiciones

En esta Recomendación no se define ningún nuevo término.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

CCITT Comité Consultivo Internacional Telegráfico y Telefónico (*international telegraph and telephone consultative committee*)

FC Clases funcionales (*functional classes*)

ISO Organización internacional de normalización (*international organization for standardization*)

LLA Arquitectura lógica por capas (*logical layered architecture*)

MF Función de mediación (*mediation function*)

NEF Función de elemento de red (*network element function*)

OSF Función de sistema de operaciones (*operation system function*)

OSI Interconexión de sistemas abiertos (*open system interconnection*)

PIN Número de identificación personal (*personal identification number*)

RCD Red de comunicación de datos

RGT Red de gestión de las telecomunicaciones

TF Función de transformación (*transformation function*)

TTP Tercera parte confiable (*trusted third party*)

UIT-T Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones

WSF Función de estación de trabajo (*workstation function*)

5 Fundamento

El requisito de seguridad en la RGT tiene su origen en diferentes fuentes:

– Los **clientes/abonados**, que necesitan poder confiar en la red y en los servicios ofrecidos incluida una facturación correcta.

– **La comunidad/las autoridades públicas**, que exigen seguridad mediante directrices y leyes, para garantizar la disponibilidad de servicios y la protección de la privacidad.

– Los propios **operadores de red/proveedores de servicio**, que necesitan seguridad para proteger sus actividades e intereses comerciales, y para cumplir sus obligaciones con los clientes y el público.

La finalidad de la RGT es gestionar la red de telecomunicaciones subyacente, y por consiguiente la seguridad de la RGT es esencial para el buen funcionamiento de la red de telecomunicaciones. Además, la red de telecomunicaciones puede tener características de seguridad que han de ser gestionadas por la RGT. La Rec. UIT-T.3400 contiene la relación de las funciones correspondientes de gestión de la seguridad.

De preferencia, las normas de seguridad de la RGT deberían basarse en las normas de seguridad acordadas a nivel internacional, ya que así basta con utilizar normas existentes en vez de tener que crear normas nuevas. El suministro y la utilización de servicios y mecanismos de seguridad puede resultar muy costoso en relación con el valor de las transacciones que se protegen. Por ello, es importante tener la capacidad de adaptar a las necesidades del cliente la seguridad de las transacciones RGT que se protegen. Los servicios y mecanismos de seguridad necesarios para asegurar las transacciones RGT deberán proporcionarse de un modo que permita esa adaptación a los requisitos del cliente. Habida cuenta del gran número de combinaciones posibles de las características de seguridad, conviene disponer de **perfiles de seguridad** (véase el apéndice I) que abarquen una amplia gama de aplicaciones de seguridad RGT.

La normalización facilitará la **reutilización de soluciones y productos**, gracias a lo cual la seguridad se podrá introducir más rápidamente y a un menor coste.

Entre los importantes beneficios que aportan las soluciones normalizadas, tanto para los vendedores como para los usuarios de los sistemas, figuran las economías de escala en la fabricación del producto y la interoperabilidad de los componentes dentro de un sistema RGT.

Es necesario proporcionar servicios y mecanismos de seguridad para proteger las transacciones entre entidades RGT (definidas en la Rec. UIT-T M.3010) contra agresiones ilícitas tales como las escuchas clandestinas, la simulación, la manipulación de mensajes (modificación, retardo, supresión, inserción, reproducción, reencaminamiento, encaminamiento erróneo o reordenación de mensajes), el repudio o la falsificación. La protección incluye la prevención y detección de las

agresiones, la recuperación después de las mismas, y la gestión de la información relacionada con la seguridad. Las normas deberán abarcar las interfaces dentro del dominio (Q y F) y entre dominios (X).

6 Descripción del sistema

El objetivo de esta Recomendación es efectuar una abstracción que permita evitar los numerosos detalles de las implementaciones prácticas y llegar a un consenso respecto a los resultados que podrían ser de utilidad cuando posteriormente se establezca su correspondencia con las implementaciones específicas.

La descripción de la RGT se hace en base a una arquitectura funcional, una arquitectura de información y una arquitectura física (Rec. UIT-T M.3010).

En la Rec. UIT-T M.3010 se admite la posibilidad de que los bloques de construcción de la RGT soportan otras interfaces, además de las Q, X y F. De manera similar, el equipo físico puede tener otras funcionalidades, además de las asociadas a la información recibida por las interfaces Q, X y F. Estas interfaces adicionales y las funcionalidades conexas no son de la incumbencia de la RGT y, por tanto, quedan fuera del ámbito de normalización de la seguridad en la RGT.

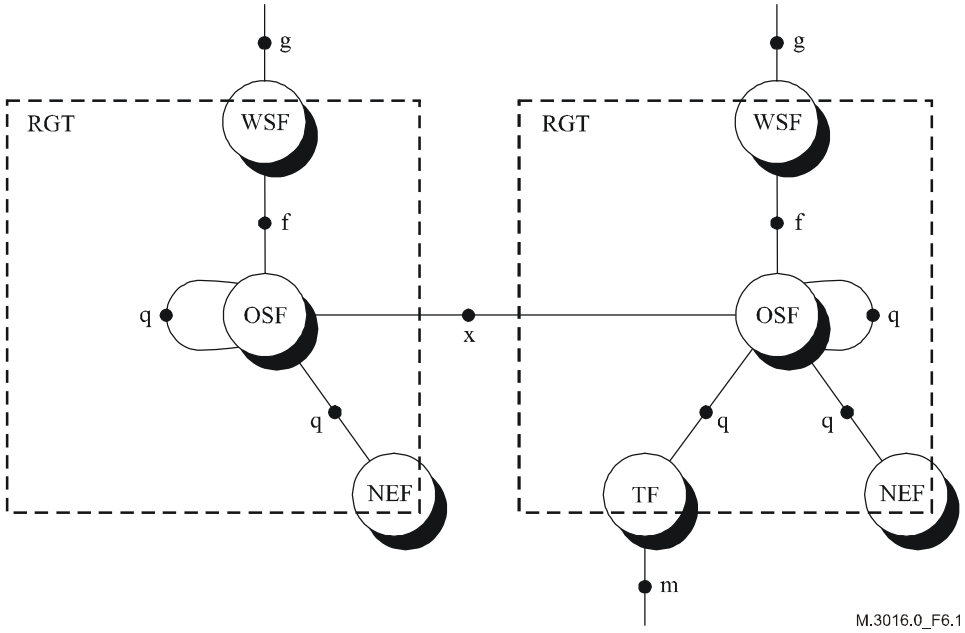

Figura 1/M.3016.0 – Arquitectura funcional de la RGT

6.1 Agentes y roles

A los efectos de la normalización de la seguridad en la RGT sólo se considerará la seguridad técnica, lo que significa que los actores que se han de tener en cuenta son los *usuarios de la RGT*. Un usuario de la RGT es una persona o un proceso que aplica los servicios de gestión de la RGT para realizar operaciones de gestión. Los usuarios de la RGT se pueden clasificar, además, en función de su pertenencia o no a la organización responsable del funcionamiento de la RGT (usuarios internos) o su acceso a la RGT como usuarios externos.

Cada vez que un usuario de la RGT accede a un servicio de gestión, el usuario de la RGT asume un rol. En ciertos casos habrá una relación unívoca entre el usuario de la RGT y el rol, es decir que el usuario de la RGT seguirá siempre desempeñando el mismo cometido. En otros casos existirá una relación polivalente entre determinado usuario RGT y los posibles cometidos que éste puede desempeñar.

La siguiente es una clasificación de alto nivel de algunos de los roles comunes:

– Operadores de red (*privados o públicos*).

– Proveedores de servicio (*proveedores de servicio portador o proveedores de servicio de valor añadido*).

– Abonados al servicio/clientes del servicio.

– Usuarios finales del servicio.

– Vendedores de equipos/soportes lógicos.

– Tercera parte confiable (es decir, un tercero en el que las dos partes confían y que funciona con arreglo a la legislación y la reglamentación nacionales pertinentes a fin de poder suministrar servicios de certificación, autenticación y otros servicios conexos).

Para que la RGT, sea segura no basta con controlar el comportamiento de sus usuarios conocidos. Ha de considerarse también la posibilidad de que un intruso trate de acceder ilegalmente a la RGT.

Algunas medidas de seguridad exigen que los agentes asuman el rol de tercera parte confiable (TTP, *trusted third party*). Uno de los aspectos importantes de la seguridad consiste en determinar cómo debería permitirse a esos agentes interactuar con la RGT.

6.2 Dominios de seguridad

La Rec. UIT-T M.3010 introduce el concepto de arquitectura estratificada lógica (LLA, *logical layered architecture*), en la que la funcionalidad de gestión está dividida en capas. Cada capa está relacionada con un subconjunto claramente definido de la actividad de gestión en su totalidad. Cada una de las capas funcionales será un *dominio de gestión* distinto bajo el control de una función de sistema de operaciones (OSF, *operation system function*) llamada dominio OSF. Las funciones de elemento de red (NEF, *network element function*) controladas por la OSF formarán parte del dominio OSF. Una RGT, como tal, estará compuesta de uno o varios dominios OSF, y los diferentes dominios OSF podrán estar desunidos interactuando, superponiéndose o contenidos.

Un *dominio de seguridad* se define como un conjunto de entidades y partes que están sujetas a una misma política de seguridad y a la misma administración de seguridad. Normalmente se supone que una RGT constituye un único dominio de seguridad. Aunque a menudo sea éste el caso, convendría no generalizar tal suposición. En las RGT más grandes, compuestas por numerosos sistemas de gestión diferentes, distintas partes de la red podrían estar sujetas a diferentes políticas y requisitos de seguridad. Por tanto, sería más apropiado decir que un dominio de seguridad RGT abarca un solo dominio OSF o un conjunto de dominios OSF.

Partiendo de esa premisa, se aplicarán las siguientes relaciones entre dominios de seguridad e interiores a un dominio de seguridad:

Posibles relaciones interiores a un dominio de seguridad:

– q (OSF-NEF, OSF-OSF).

Posibles relaciones entre dominios de seguridad:

– x (OSF-OSF);

– f (WSF-OSF, WSF-MF);

– q (OSF-OSF, OSF-TF).

Se señala que las relaciones anteriores se refieren a dominios de seguridad y no a dominios de gestión. Es importante observar que tanto en las relaciones dentro de un dominio de seguridad como en las relaciones entre dominios de seguridad puede participar un punto de referencia q. Una diferencia principal entre las relaciones dentro de un dominio y las relaciones entre dominios es el grado de confianza que existe entre las entidades en cuestión.

7 Objetivos de seguridad genéricos de la RGT

La finalidad de esta cláusula es describir el objetivo último de las medidas de seguridad adoptadas en un entorno conforme a la RGT. Se trata sobre todo de determinar el tipo de seguridad de que se dispondrá finalmente y no la manera de conseguirlo.

Los objetivos de seguridad se deberán establecer en función de los intereses del operador y otros agentes, las relaciones comerciales, las limitaciones jurídicas y normativas, las limitaciones contractuales, etc.

En el caso de la RGT, los objetivos de seguridad son los siguientes:

– Sólo los agentes legitimados deberán tener acceso a los activos y derecho a la explotación de los mismos en una RGT.

– Los agentes legitimados deberán tener acceso a los activos y derecho a la explotación de los activos a los que estén autorizados a acceder.

– Los agentes deberán ser responsables exclusivamente de sus propias acciones en la RGT.

– Se ha de proteger la disponibilidad de la RGT contra la explotación o el acceso no solicitados.

– Ha de ser posible recuperar de la RGT la información relacionada con la seguridad.

– Si se detectan violaciones de la seguridad, se deberá hacer frente a las mismas de manera controlada, para reducir al mínimo los daños causados.

– Si se detecta un fallo de la seguridad, deberá ser posible restablecer los niveles normales de la misma.

– La arquitectura de seguridad de la RGT debe proporcionar una cierta flexibilidad, para que sean posibles distintas políticas de seguridad, esto es, diferentes grados de intensidad en los mecanismos de seguridad.

Se entiende que la expresión "tener acceso a los activos" entraña no sólo la posibilidad de realizar funciones, sino también de leer información.

Los objetivos genéricos se formulan de conformidad con los criterios y el lenguaje de los directivos de la empresa. Las cláusulas siguientes deben expresarse en términos más técnicos, de tal modo que de ellas se deriven servicios y funciones de seguridad aplicables. La correspondencia entre los dos lenguajes no siempre es obvia.

Puede demostrarse que, si se alcanza el siguiente conjunto de objetivos de seguridad, se satisfarán también los cinco primeros objetivos de seguridad de la RGT mencionados en la presente cláusula:

– confidencialidad;

– integridad de los datos;

– responsabilidad;

– disponibilidad.

Las amenazas y riesgos que se indican en la cláusula 9 y los requisitos funcionales descritos en la cláusula 6 se basarán en estos términos, más formales. Para las definiciones, véase la cláusula 9.

8 Cuestiones de legislación

La infraestructura de seguridad de una RGT debe ser capaz de ajustarse a las constricciones que imponen las leyes gubernamentales, la legislación contractual, los tratados y los reglamentos. Entre dichas constricciones puede figurar la obligatoriedad de los servicios de seguridad (por ejemplo, asegurar la privacidad de la información del cliente), la exclusión de ciertos mecanismos de seguridad (por ejemplo, algunos tipos de criptación) y/o el apoyo de la interceptación clandestina de comunicaciones por los organismos encargados de hacer cumplir la ley.

9 Amenazas y riesgos

La finalidad de esta cláusula es explorar las amenazas y riesgos a los que está expuesta una RGT. No se pretende especificar una evaluación de los riesgos o un análisis de las amenazas en casos concretos. Ésa es una cuestión local a la que cada proveedor puede hacer frente de distinta manera sin afectar el interfuncionamiento.

Una amenaza es una potencial violación de la seguridad. Según los objetivos de seguridad genéricos identificados en la RGT, las amenazas pueden dirigirse a cuatro tipos diferentes de objetivos:

– **confidencialidad** (confidencialidad de la información almacenada y transferida);

– **integridad de datos** (protección de la información almacenada y transferida);

– **imputabilidad** (una entidad debe ser responsable de cualquier acción iniciada); y

– **disponibilidad** (todas las entidades legitimadas deben gozar de un acceso adecuado a las facilidades RGT).

En esta Recomendación se hace una distinción entre tres tipos de amenazas:

– amenaza accidental: amenaza que no está originada por ninguna intención maliciosa;

– amenaza administrativa: amenaza provocada por la falta de administración de la seguridad; y

– amenaza intencional: amenaza en la que participa una entidad malintencionada que puede atacar a la propia comunicación o a los recursos de la red.

En la labor de normalización de la RGT pueden tenerse en cuenta las amenazas accidentales y administrativas, en la medida en que sus consecuencias son las mismas que las de las amenazas intencionales. Para hacer un análisis más preciso de las amenazas teniendo en cuenta la arquitectura de la RGT, esta Recomendación se centra en las amenazas intencionales que entrañan la comunicación entre diferentes agentes de la RGT. El objetivo de este enfoque es obtener una lista más breve de las amenazas que pueden utilizarse directamente en los trabajos de normalización de la RGT. En un análisis de las amenazas a la RGT se deben analizar por tanto los siguientes puntos, en base a la Rec. UIT-T X.800:

– **usurpación de identidad ("simulación")**: pretensión de una entidad de ser una entidad diferente.

– **escucha clandestina**: violación de la confidencialidad mediante el control de una comunicación.

– **acceso no autorizado**: intento de una entidad de acceder a datos violando la política de seguridad vigente.

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

– **repudio**: una entidad participante en un intercambio de comunicación niega a continuación ese hecho.

– **falsificación**: una entidad fabrica información y afirma que esa información fue recibida de otra entidad o enviada a otra entidad.

– **denegación de servicio**: esto ocurre cuando una entidad no desempeña su función o impide que otras entidades desempeñen las suyas. Ejemplos al respecto son la denegación del acceso a la RGT y la denegación de una comunicación saturando la RGT. En una red compartida, esta amenaza se reconoce por la creación de tráfico adicional que inunda la red, lo que impide a otros utilizarla al retardar su tráfico.

El cuadro 1 contiene un diagrama de las amenazas y objetivos.

Cuadro 1/M.3016.0 – Correspondencia entre amenazas y objetivos

Amenaza	Confidencialidad	Integridad de los datos	Imputabilidad	Disponibilidad
Usurpación de identidad	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	
Denegación de servicio				x

Una amenaza potencial no será perjudicial para un sistema a menos que éste adolezca de una debilidad correspondiente y en un momento se explote esa debilidad. Toda amenaza entrañará un riesgo. La evaluación del riesgo puede dividirse en la evaluación de la probabilidad de cada amenaza y la evaluación del efecto que podría tener esa amenaza. La evaluación de la amenaza y el riesgo debe formar parte de un proceso iterativo: pueden surgir nuevas amenazas si se adoptan contramedidas, por ejemplo, amenazas a las claves de criptografía cuando se utilizan medidas criptográficas.

10 Requisitos y servicios de seguridad

En la figura 2 se muestran las relaciones entre amenazas y objetivos, requisitos y servicios de seguridad. Se describe en ella la manera de deducir cuáles son los "requisitos de seguridad" a partir de las "amenazas" y los "objetivos de seguridad", los cuales se materializarán aplicando una serie de servicios de seguridad. Estos "servicios", que contrarrestan las amenazas, utilizarán "mecanismos" que, por su parte, emplean "algoritmos de seguridad".

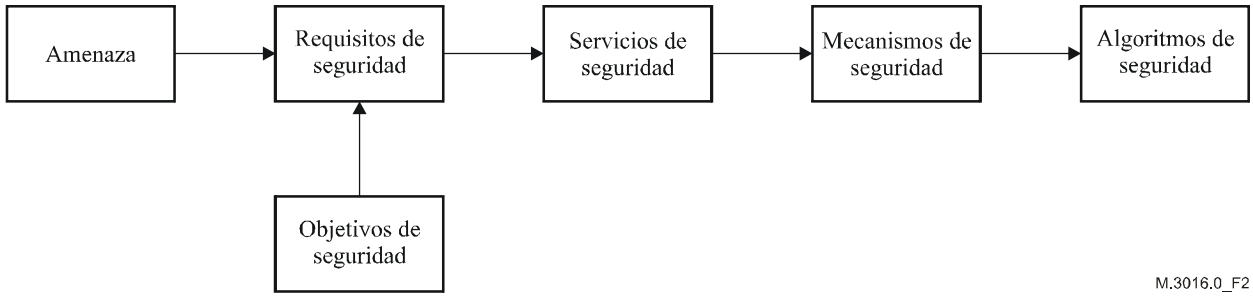

Figura 2/M.3016.0 – Marco en materia de seguridad

En la cláusula 10.1 se enumeran estos requisitos de seguridad. A menos que se especifique de otro modo, la palabra "requisito" no significa en esta Recomendación que en cada RGT haya alguna funcionalidad que sea siempre obligatoria, sino, más bien, que una administración de RGT puede dar carácter obligatorio a una funcionalidad para ciertas aplicaciones y/o interfaces específicas de esa RGT. La decisión final dependerá de los objetivos de seguridad consignados en la política de seguridad del operador.

Además de los requisitos y servicios de seguridad, en esta cláusula se estipulan algunos requisitos genéricos para la gestión de los servicios de seguridad (véase 10.2) y los requisitos arquitecturales que rigen la integración de los servicios de seguridad en la arquitectura de la RGT (véase 10.3).

Aunque los requisitos administrativos y de vida útil son importantes, no afectan a la arquitectura y por tanto no se abordan en la presente cláusula.

10.1 Requisitos de seguridad y servicios correspondientes

En esta cláusula se describe una serie de requisitos funcionales genéricos y los correspondientes servicios que pueden utilizarse para contrarrestar las amenazas a una RGT.

10.1.1 Correspondencia de los requisitos funcionales, amenazas y objetivos de seguridad

En esta cláusula se identifican los requisitos de seguridad funcionales para hacer frente a las amenazas enumeradas en la cláusula 9, según se indica en el cuadro 2. A partir de este cuadro se ha establecido la correspondencia entre requisitos de seguridad (cuadro 3) y objetivos de seguridad consignados en la cláusula 7. La lista se circunscribe a los requisitos que tienen carácter genérico y un efecto considerable en los componentes y la arquitectura.

Cuadro 2/M.3016.0 – Correspondencia entre requisitos funcionales y amenazas

Requisitos funcionales	Usurpación de identidad	Escucha clandestina	Acceso no autorizado	Pérdida o corrupción de información	Repudio	Falsificación	Denegación de servicio
Verificación de identidades	x		x				
Acceso controlado y autorización			x				x
Protección de la confidencialidad		x	x				
Protección de la integridad de los datos				x			
Imputabilidad					x	x	
Inclusión de actividades en el fichero registro cronológico	x		x		x	x	x
Notificación de alarma de seguridad	x		x	x			x
Auditoría de seguridad	x		x		x	x	x

Los objetivos utilizados son los cuatro objetivos formales definidos en la cláusula 3, cada uno de los cuales encabeza una columna en el cuadro 3, indicando el conjunto de requisitos funcionales que se han de cumplir para alcanzar el objetivo en cuestión.

10.1.2 Descripción de los requisitos funcionales y los servicios correspondientes

En el texto que sigue se analizan los requisitos funcionales indicados en los cuadros 2 y 3, y se identifican los servicios de seguridad correspondientes a cada uno de esos requisitos. Se señala que los requisitos de cualquiera de esas funciones no invocan automáticamente un servicio de seguridad definido por la ISO. En la práctica no obstante, se produce una coincidencia en algunos casos.

Cuadro 3/M.3016.0 – Correspondencia entre objetivos de seguridad y requisitos funcionales

Requisito funcional	Confidencialidad	Integridad de los datos	Imputabilidad	Disponibilidad
Verificación de identidades	x	x	x	
Acceso controlado y autorización	x	x	x	x
Protección de la confidencialidad	x			
Protección de la integridad de los datos		x		
Imputabilidad			x	
Inclusión de actividades en el fichero registro cronológico			x	x
Notificación de alarma de seguridad	x	x	x	x
Auditoría de seguridad			x	x

10.1.2.1 Verificación de identidades

Una RGT debe ofrecer la posibilidad de establecer y verificar la identidad declarada por cualquier agente que participe en la red.

Los agentes pueden ser usuarios humanos o entidades en el seno de la RGT. Las identidades verificadas sirven de base para establecer la imputabilidad y son fundamentales para el cumplimiento de los requisitos de seguridad que se indican en esta cláusula.

El servicio de seguridad que soporta el requisito verificación de identidades es el de **autenticación**. El servicio de autenticación proporciona la prueba de que un objeto o sujeto tiene verdaderamente la identidad que declara. En función del tipo de agente y de la finalidad de la identificación, se pueden necesitar los siguientes tipos de autenticación:

– autenticación del usuario, con la que se demuestra la identidad del usuario humano o el proceso de aplicación;
– autenticación de entidad par, con la que se demuestra la identidad de la entidad par durante una relación de comunicación;
– autenticación del origen de los datos, con la que se demuestra la identidad del responsable de una unidad de datos específica.

El servicio de autenticación establece la prueba de la identidad en un momento determinado. Para establecer una prueba permanente, se ha de repetir o vincular la autenticación a un servicio de integridad.

Como ejemplos de los mecanismos utilizados para implementar el servicio de autenticación cabe citar las contraseñas y los números de identificación personal (PIN, *personal identification number*) (autenticación simple) y los métodos criptográficos (autenticación fuerte).

10.1.2.2 Acceso controlado y autorización

Una RGT debe ofrecer la posibilidad de asegurar que ningún agente tiene acceso a información o recursos a los que no se le ha autorizado a acceder.

El servicio de seguridad que soporta el requisito acceso controlado y autorización es el de **control de acceso**. El servicio de control de acceso proporciona una manera de garantizar que los sujetos acceden a los recursos únicamente de forma autorizada. Esos recursos pueden ser el sistema físico, el soporte lógico, las aplicaciones y los datos del sistema. El servicio de control puede definirse e

implementarse a diferentes niveles de granularidad en la RGT: a nivel de agente, objeto o atributo. Las limitaciones de acceso se estipulan en la información de control de acceso, la cual especifica:

– la manera de determinar qué entidades están autorizadas a acceder;

– el tipo de acceso que se autoriza (lectura, escritura, modificación, creación, supresión).

Los servicios más específicos de control de acceso a la RGT se pueden dividir en tres tipos:

– *Control de acceso de asociación de gestión*

  Este servicio permite el control de acceso a 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 de notificación de gestión*

  Este servicio permite el control de acceso con respecto a las notificaciones, es decir, permite garantizar que las notificaciones sólo se revelan a entidades autorizadas para recibirlas.

– *Control de acceso de recurso gestionado*

  Este servicio permite el control de acceso con respecto a los propios recursos.

La identidad de la entidad que trata de obtener acceso debe comprobarse antes de otorgar el acceso al recurso. Esto significa que la utilización del control de acceso siempre está vinculada a la utilización de un servicio de autenticación.

10.1.2.3 Protección de la confidencialidad

Una RGT debe ofrecer la posibilidad de asegurar la confidencialidad de los datos almacenados y comunicados.

Los servicios de seguridad que soportan el requisito protección de la confidencialidad son el de **control de acceso** para los datos almacenados y el de **confidencialidad de datos** para los datos comunicados. La **confidencialidad de datos** también puede ser necesaria para algunas clases de datos que se almacenan como es el caso de las contraseñas.

El servicio de confidencialidad ofrece protección contra la divulgación no autorizada de los datos intercambiados. Cabe distinguir los siguientes tipos de servicio de confidencialidad:

– confidencialidad de campo selectiva;

– confidencialidad de conexión;

– confidencialidad de flujo de datos.

10.1.2.4 Protección de la integridad de los datos

Una RGT debe ser capaz de garantizar la identidad de los datos almacenados y comunicados.

Los servicios de seguridad que soportan el requisito protección de la integridad de los datos son el de **control de acceso** e **integridad de datos** para los datos almacenados y el de **integridad de datos** para los datos comunicados.

El servicio de integridad ofrece la manera de garantizar la corrección de los datos intercambiados, y brinda protección contra la modificación, supresión, creación (inserción) y reproducción de los datos intercambiados. Cabe distinguir los siguientes tipos de servicio de integridad:

– integridad de campo selectiva;

– integridad de conexión sin recuperación;

– integridad de conexión con recuperación.

10.1.2.5 Imputabilidad

Una RGT debe ofrecer la posibilidad de impedir que una entidad niegue su responsabilidad en cualquiera de las acciones que realice, así como en sus efectos.

El servicio de seguridad que soporta el requisito imputabilidad es el de **no repudio**, que vincula al individuo (o la entidad) con la acción realizada. El servicio de no repudio proporciona una manera de demostrar que realmente tuvo lugar el intercambio de datos. Se presenta en dos formas:

– no repudio: prueba de origen;

– no repudio: prueba de entrega.

Otra posible manera de aplicar la imputabilidad, más general y quizás menos estricta, consistiría en combinar adecuadamente los servicios de **autenticación**, **control de acceso** y **registro de auditoría**.

10.1.2.6 Inclusión de actividades en el fichero registro cronológico, notificación de alarma de seguridad y auditoría de seguridad

Estos requisitos responden a la necesidad de almacenar y analizar la información sobre actividades relativas a la seguridad dentro de la RGT. Además, se deberían generar notificaciones de alarma en determinados eventos ajustables. Los servicios correspondientes son los de **registro de auditoría** y **notificación de alarmas**. A continuación se examina con algún detalle cada uno de los requisitos mencionados.

10.1.2.6.1 Inclusión de actividades en el fichero registro cronológico

Una RGT debe ofrecer la posibilidad de almacenar información sobre las actividades del sistema, con la posibilidad de rastrear esa información hasta los particulares o las entidades.

Un fichero registro cronológico es un repertorio de registros, es la abstracción OSI de la inclusión de los recursos en el fichero registro cronológico de los sistemas abiertos reales. Los registros contienen la información que se incluye en el fichero.

Para el desempeño de numerosas funciones de gestión es necesario estar en condiciones de preservar la información sobre los eventos que han ocurrido o las operaciones realizadas o intentadas por o en los diferentes recursos.

Además, cuando esa información se recupera de un fichero registro cronológico, el gestor debería ser capaz de determinar si se perdió algún registro o si se modificaron en algún momento las características de los registros almacenados.

10.1.2.6.2 Notificación de alarma de seguridad

Una RGT debe ofrecer la posibilidad de generar notificaciones de alarma al producirse determinados eventos. El usuario deberá establecer los criterios de selección.

La función control de auditoría de seguridad es una función de gestión de sistemas que describe cómo se notifican los eventos de seguridad para su compilación. La notificación de alarma de seguridad definida por esta función de gestión de sistemas proporciona información sobre las condiciones operacionales relacionadas con la seguridad.

10.1.2.6.3 Auditoría de seguridad

Una RGT debe ofrecer la posibilidad de analizar los datos incluidos en el registro de eventos de seguridad pertinentes, para verificarlos a fin de detectar posibles violaciones de la política de seguridad.

La auditoría debe considerarse como un análisis y examen independiente de los registros y las actividades del sistema para comprobar la idoneidad de los controles del sistema, asegurar el cumplimiento de la política de seguridad establecida y los procedimientos operacionales, así como

para detectar fallos en el sistema de seguridad. Como resultado de la auditoría, se identificarán los cambios a introducir en materia de control, política y procedimientos.

El cuadro 4 que figura a continuación da una visión general de las relaciones entre los requisitos y los servicios de seguridad. En esta cláusula sólo se definen los servicios de seguridad para los que existen soluciones normalizadas, y se dejan de lado otros posibles servicios (por ejemplo, el de detección de denegación de servicio).

Cuadro 4/M.3016.0 – Correspondencia entre los requisitos de seguridad y los servicios de seguridad

Requisito funcional	Servicio de seguridad
Verificación de identidades	autenticación del usuario autenticación de entidad par autenticación del origen de los datos
Acceso controlado y autorización	control de acceso
Protección de la confidencialidad – datos almacenados	control de acceso confidencialidad
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
Imputabilidad	no repudio
Inclusión de actividades en el fichero registro cronológico	registro de auditoría
Notificación de alarma de seguridad	alarma de seguridad
Auditoría de seguridad	registro de auditoría
Protección de la RCD	inspección de paquetes

NOTA – Los requisitos siguientes no son los mismos que los indicados anteriormente (cuadro 4) y pueden no ser considerados como candidatos evidentes a la normalización. No obstante, se deberían tener en cuenta durante la fase de diseño junto con la implementación de los requisitos básicos de la RGT antes indicados.

10.1.2.6.4 Integridad del sistema

Es fundamental que el entorno de soportes lógicos y físicos de las funciones de seguridad implementadas mantengan el nivel de seguridad solicitado.

En lo anterior se incluye la configuración correcta de los sistemas que están en funcionamiento y la eliminación de defectos en dichos sistemas.

Estos aspectos no forman parte del perfil de seguridad funcional propiamente dicho, pero se deben estipular junto con esas especificaciones para asegurar la firmeza de las funciones en un entorno real.

10.1.2.6.5 Observaciones sobre disponibilidad

No existe una serie única o una serie limitada de servicios de seguridad con la que se pueda cumplir el requisito de disponibilidad. Todos los servicios de seguridad aquí mencionados deben formar un conjunto coherente capaz de mantener la disponibilidad. No obstante, los servicios de seguridad por sí solos nunca podrán garantizar la disponibilidad: se trata también de una cuestión de fiabilidad de los soportes físicos y lógicos (tanto desde el punto de vista del diseño como de la implementación).

10.1.2.7 Protección de la red de comunicación de datos (RCD)

Una RGT debe proporcionar la protección de la RCD contra el tráfico de los clientes y de la red par.

Una RGT debe permitir el aislamiento del tráfico de la RCD con respecto a otros tipos de tráfico, particularmente en una RCD basada en paquetes.

10.2 Requisitos de la gestión de la seguridad

Una RGT debe contener modelos de información y capacidades de gestión de los servicios utilizados para asegurar la red.

En los requisitos detallados sobre gestión de seguridad se indican las aplicaciones de gestión que deberían introducirse y se describe la manera de diseñarlas. La finalidad de todo ello es proporcionar al administrador de seguridad los instrumentos adecuados para supervisar y controlar los servicios de seguridad de manera eficaz y correcta. Los objetivos y metas de la gestión de seguridad se presentan a tres niveles diferentes de un sistema de telecomunicaciones, que corresponden a la gestión de la seguridad de los sistemas, los servicios de seguridad y los mecanismos de seguridad, respectivamente.

Las operaciones y la información relacionadas con la gestión de los servicios de seguridad en la RGT han de ser objeto de una atención especial desde una perspectiva de seguridad. Las claves de criptación secretas, la información de autenticación y las listas de control de acceso son ejemplos de elementos de seguridad en los que puede necesitarse un nivel de protección superior al de la gestión de red.

La gestión de la seguridad debe ser compatible con las funciones de gestión de la seguridad definidas en la Rec. UIT-T M.3400.

Se debería soportar la recuperación del sistema a un estado seguro tras una agresión al sistema de seguridad.

Siempre que se produzca una agresión al sistema de seguridad, la RGT deberá ser capaz de hacer frente a esa tentativa de manera controlada, de tal modo que el intento no provoque una sensible degradación de la RGT en lo que se refiere a su disponibilidad.

10.3 Requisitos arquitectónicos

Los requisitos más importantes que se han de satisfacer mediante la adopción de medidas de seguridad para estar en consonancia con el marco de la RGT son los siguientes:

- Las medidas deberán basarse en los principios del modelo funcional de la RGT.
- Las medidas deberán estar en conformidad con el modelo de información y de datos orientados al objeto de la RGT.
- Las medidas deberán ser aplicables a todos los dominios de la RGT en los sectores público y privado.
- Las soluciones deberán poder ajustarse a RGT pequeñas y grandes.
- Las soluciones deberán ser compatibles con la arquitectura interna de los puntos de referencia de la RGT considerados.
- Las soluciones deberán contemplar los intereses de todos los usuarios internos y externos de la RGT.
- Las soluciones deberán considerar aspectos relativos a la solidez.
- Las soluciones deberían soportar la reconfiguración a través de la incorporación o supresión de usuarios o aplicaciones.

Es probable que surjan discrepancias entre el área de seguridad y otras áreas funcionales. Por ejemplo, se ha de compatibilizar la integridad y la confidencialidad de los datos de tasación con los requisitos de circulación del enorme volumen de información necesario para contabilizar las llamadas a larga distancia. Un conjunto fiable de requisitos de seguridad deberá tener en cuenta los efectos sobre las características de otras áreas funcionales.

Cuando se analicen situaciones concretas de la RGT es posible que se planteen otros requisitos en materia de arquitectura de la red.

10.4 Servicios de seguridad y capas OSI

En esta cláusula se describen las capas OSI que se utilizan para prestar servicios de seguridad, y se indica por tanto cómo se pueden proporcionar esos servicios en una RGT de manera significativa.

Se supone que si una capa proporciona un servicio de seguridad, ese servicio se proporciona a la capa superior a la considerada. Para limitar las posibilidades se utiliza como base la prestación de servicios por las capas a las que se refiere la Rec. UIT-T X.800.

10.4.1 Autenticación del usuario

Este servicio depende de la interacción con el usuario y, por lo tanto, está fuera del modelo OSI.

10.4.2 Autenticación (de entidad par y del origen de los datos)

Este servicio lo pueden proporcionar las siguientes capas (de conformidad con 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 la OSI: en el propio proceso de aplicación.

Teniendo en cuenta que la RGT deberá cumplir el requisito de identificar y autenticar a los gestores y agentes, así como el vínculo de la autenticación con el control de acceso, las posiciones recomendadas con respecto a la pila OSI son la capa de aplicación y el proceso de aplicación.

10.4.3 Control de acceso

– *Control de acceso a asociación de gestión*

  Este servicio se puede utilizar a los niveles en los que existe una asociación, ya sea en la capa de aplicación (control de acceso para procesos de aplicación) o en el propio proceso de aplicación.

  El control de acceso a asociación se puede proporcionar en la capa de red, por ejemplo utilizando el servicio de grupo cerrado de usuarios X.25. En la capa de aplicación o en el propio proceso de aplicación se puede proporcionar un mayor control de acceso a asociación.

– *Control de acceso a notificación de gestión*

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

– *Control de acceso a recurso gestionado*

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

10.4.4 Alarma de seguridad, registro de auditoría y recuperación

Estos servicios están vinculados a otros servicios y por tanto están presentes en las capas en las que también lo están los otros servicios.

10.4.5 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 el que puede discriminar entre campos.

– *Integridad de la conexión con recuperación*

  Este servicio 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, la capa de transporte, la capa de aplicación o el proceso de aplicación.

10.4.6 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 el que puede discriminar entre campos.

– *Confidencialidad con conexión y sin conexión*

  Considerando que se necesita confidencialidad de extremo a extremo, lo que excluye a la capa física y a la capa de enlace de datos, la confidencialidad puede proporcionarse en la capa de red, la capa de transporte, la capa de presentación, la capa de aplicación o en el proceso de aplicación.

– *Confidencialidad de flujo de tráfico*

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

10.4.7 No repudio

– No repudio – prueba de envío;

– No repudio – prueba de entrega.

  Este servicio se puede utilizar en las capas de presentación y aplicación, o en propio proceso de aplicación.

En el cuadro 5 se presenta de forma resumida todo lo anterior.

Cuadro 5/M.3016.0 – Vínculos entre los servicios de seguridad y el modelo de referencia OSI

	Capa						
Servicio	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Autenticación del usuario	–	–	–	–	–	–	+
Autenticación de entidad par	–	–	+	+	–	–	+
Autenticación del origen de datos	–	–	+	+	–	–	+
Control de acceso a asociación de gestión	–	–	+	–	–	–	+
Control de acceso a notificación de gestión	–	–	–	–	–	–	+
Control de acceso a recurso gestionado	–	–	–	–	–	–	+
Alarma de seguridad, registro de auditoría y recuperación	+	+	+	+	+	+	+
Integridad de campo selectiva	–	–	–	–	–	–	+
Integridad de la conexión con recuperación	–	–	–	+	–	–	+
Integridad de la conexión sin recuperación	–	–	+	+	–	–	+
Confidencialidad de campo selectiva	–	–	–	–	–	–	+
Confidencialidad con conexión y sin conexión	–	–	+	+	–	+	+
Confidencialidad de flujo de tráfico	–	–	+	+	–	+	+
No repudio – prueba de envío	–	–	–	–	–	+	+
No repudio – prueba de entrega	–	–	–	–	–	+	+

10.5 Gestión de la seguridad

La gestión de la seguridad comprende todas las actividades encaminadas a establecer, mantener y terminar los aspectos relativos a la seguridad de un sistema.

Se contemplan los siguientes aspectos:

– gestión de los servicios de seguridad;
– instalación de mecanismos de seguridad;
– gestión de claves (parte de administración);
– establecimiento de identidades, claves, información sobre control de acceso, etc.;
– gestión del registro de auditoría de seguridad y de las alarmas de seguridad.

Apéndice I

Clases funcionales y subperfiles de seguridad

I.1 Agrupación de medidas de seguridad

Las medidas de seguridad pueden agruparse en clases funcionales (FC, *functional classes*). En la siguiente definición no se tiene en cuenta la intensidad de la medida de seguridad.

Una clase funcional es un conjunto coherente de medidas de seguridad con las que satisfacer los requisitos de niveles funcionales variables.

I.1.1 Utilización de las clases funcionales entre dominios

La seguridad de una RGT no debería verse afectada negativamente como resultado de las actividades entre dominios. Se deberían establecer las normas para la interacción de unos dominios con otros en el marco de una política de seguridad entre dominios. En esas normas se deberían definir las medidas de seguridad a utilizar en cada caso. Para facilitar el acuerdo entre los dominios interactuantes, podría hacerse referencia a esas medidas de seguridad como a una clase funcional específica.

I.1.2 Utilización de clases funcionales dentro de un dominio

Cuando se trata de actividades dentro de un dominio, las clases funcionales pueden facilitar la definición de la seguridad. Las FC pueden utilizarse también para garantizar la seguridad. A tal fin, deberían asociarse al nivel de seguridad declarado por el fabricante de productos de gestión. Este tema guarda una estrecha relación con los criterios de evaluación formal.

Puede darse el caso de que, a efectos de la interacción entre dominios, un operador exija la aplicación de una FC particular para el caso dentro de un dominio del otro operador. Una razón para ello podría ser el hecho de que no se pueda hacer frente con eficacia a todas las amenazas en la interfaz entre los dos dominios. En tal caso, una posible solución consistiría en asegurar la existencia de un nivel mínimo de seguridad interna para la interacción de las RGT. En las normas de seguridad de las RGT no se debería prescribir la necesidad de clases funcionales, sino más bien facilitar la posibilidad de requerir determinadas FC, mediante la definición de los elementos de selección apropiados.

I.2 Clases funcionales

Las clases funcionales se utilizan para definir un grupo reducido de servicios de seguridad con el que se pretende conseguir un cierto nivel de seguridad. En esta cláusula se expone un conjunto de clases funcionales que sirve de ejemplo de cómo se pueden definir las FC. Las clases funcionales *para la interfaz X* se proponen a tres niveles de seguridad distintos:

1) Clase funcional mínima: (FC 1);
2) Clase funcional básica: (FC 2);
3) Clase funcional avanzada: (FC 3).

Por motivos de tipo práctico, el número de FC no debe ser demasiado elevado. Por otro lado, ha de ser posible la concordancia con los requisitos de numerosas organizaciones diferentes. Las clases funcionales pueden modificarse de la siguiente manera:

– Las clases funcionales definidas únicamente para la interfaz X podrán incluir también las interfaces Q.
– Se supone que la confidencialidad es una característica facultativa de todas las clases funcionales, por dos razones:
  • es un requisito menos severo;

- su obligatoriedad en una clase funcional puede tener consecuencias jurídicas en la utilización de esa clase.

El cuadro I.1 da una visión general de las clases funcionales.

Cuadro I.1/M.3016.0 – Clases funcionales de servicios de seguridad

FC 1	FC 2	FC 3
Insistencia en la integridad de los recursos gestionados almacenados	Insistencia en la integridad de los recursos gestionados almacenados y en la integridad de los datos transferidos	FC 2 además de imputabilidad de las actividades de gestión
• Autenticación (de entidad y usuario par) • Control de acceso a asociación de gestión • Control de acceso a recurso gestionado • Alarma de seguridad, auditoría y recuperación	• Autenticación (de entidad y usuario par) • Control de acceso a asociación de gestión • Control de acceso a recurso gestionado • Autenticación del origen de los datos • Integridad de campo selectiva • Integridad de la conexión • Alarma de seguridad, auditoría y recuperación	• Autenticación (de entidad y usuario par) • Control de acceso a asociación de gestión • Control de acceso a recurso gestionado • Autenticación del origen de los datos • Integridad de campo selectiva • Integridad de la conexión • No repudio del origen • No repudio del destino • Alarma de seguridad, auditoría y recuperación
Facultativa: • Integridad de la conexión • Confidencialidad de la conexión	Facultativa: • Confidencialidad de la conexión • Confidencialidad de campo selectiva	Facultativa: • Confidencialidad de la conexión • Confidencialidad de campo selectiva

Además, se deberá hacer una distinción entre las FC aplicables al caso entre dominios y las FC aplicables dentro de un dominio. Los requisitos variarán según el caso, y por ese motivo las medidas de seguridad también podrían ser diferentes.

A continuación se da una visión general de los diferentes casos para facilitar la selección de las FC que se necesitan y son pertinentes.

Suposición

Para cada dominio existe una autoridad responsable de decidir cuáles son las medidas de seguridad que se deberían aplicar en el dominio.

Cabe distinguir tres casos:

1) Las FC las define una autoridad de dominio y son aplicables al propio dominio (dentro del dominio).
2) Las FC las define una autoridad de dominio y son aplicables a las interacciones de dominio (entre dominios). Estas FC serán el resultado de un acuerdo entre las autoridades de los dominios interactuantes.
3) Las FC las define una autoridad de dominio como requisito para la seguridad interna del otro dominio.

En cada uno de esos casos, se puede determinar el número de FC para los diferentes niveles de seguridad.

El número de niveles de seguridad queda en estudio.

El conjunto de medidas de seguridad que forman una clase funcional también queda en estudio.

Las FC de los diferentes casos podrían ser las mismas, reduciendo así el número total de FC.

Cabría considerar asimismo una compensación recíproca entre los diferentes casos, por ejemplo cuando la seguridad entre dominios es de alto nivel, los requisitos de seguridad interna en el otro dominio podrían ser bajos, y viceversa. Otra posibilidad sería que la clase funcional representase un conjunto mínimo de medidas de seguridad que pudiera ampliarse con medidas adicionales, según procediera.

I.3 Perfiles de seguridad

Las clases funcionales no exigen la utilización de mecanismos de seguridad normalizados; puede aplicarse cualquier mecanismo que cumpla los requisitos.

Para facilitar la interacción entre las medidas de seguridad en los diferentes dominios, dichas medidas deben estar en conformidad con las normas. Un perfil de seguridad es la prescripción del uso de determinadas normas que, en conjunto, constituyen una clase funcional.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
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	**Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes**
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, comunicaciones de sistemas abiertos y seguridad
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, 2005