Unión Internacional de Telecomunicaciones

La seguridad de las telecomunicaciones y las tecnologías de la información

Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes

Diciembre de 2003

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

Unión Internacional de Telecomunicaciones

La seguridad de las telecomunicaciones y las tecnologías de la información

Visión general de asuntos relacionados con la seguridad de las telecomunicaciones y la implementación de las Recomendaciones UIT-T existentes

Agradecimientos

Este Manual ha sido preparado gracias a la contribución de numerosos autores, bien sea a través de la elaboración de las Recomendaciones UIT-T pertinentes o de su participación en las reuniones de las Comisiones de Estudio de este Sector, en sus cursillos y seminarios. En particular, se debe agradecer a: la Sra. Lakshmi Raman, por su contribución a la cláusula 6.4 y parte de la cláusula 2. En la revisión de esta última también participaron los Srs. Herbert Bertine y Rao Vasireddy. La cláusula 3, que trata sobre amenazas y riesgos, se inspira tanto en el trabajo del Sector como en la presentación de [Shannon]. La cláusula 5 y la cláusula 6.5 se basan en textos generales de [Wisekey] y en una amable contribución del Profesor David Chadwick, en particular en lo que respecta a la descripción de la aplicación *E-prescription* de Salford que se presenta en 6.5.2 (además de algún material proveniente de [Policy]). El texto relativo a VoIP y a los sistemas de la Rec. UIT-T H.323, que aparece en la cláusula 6.1, se basa en [Packetizer] y [Euchner], así como en la amable contribución del Sr. Martin Euchner. La cláusula 6.2 se basa en la Rec. UIT-T J.169 y en un estudio del Sr. Eric Rosenfeld en 6.1.2. El material disponible en las Recomendaciones UIT-T T.30 y T.36 sirvió como base para el texto de la cláusula 6.3. Conviene también agradecer a diversos participantes anónimos. El material presentado en el anexo C proviene de las respuestas de los Expertos de distintas Comisiones de Estudio del UIT-T al Cuestionario sobre Seguridad de la CE 17, mientras que el del anexo B se basa en las Recomendaciones relacionadas con el Compendio sobre la seguridad de los sistemas de comunicaciones que mantienen los Expertos del UIT-T en las Cuestiones 10/17, en particular el Sr. Sándor Mazgon.

© UIT 2004

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

Índice

Página

Agradecimientos

Índice iii

Prefacio v

Resumen ejecutivo vii

1 Alcance 1

2 Arquitectura y dimensiones básicas de seguridad 1

2.1 Privacidad y confidencialidad de datos 2

2.2 Autenticación 3

2.3 Integridad de datos 3

2.4 No repudio 3

2.5 Otras dimensiones definidas en X.805 3

3 Vulnerabilidades, amenazas y riesgos 4

4 Requisitos del marco de seguridad 5

5 PKI y gestión de privilegios según la Rec. UIT-T X.509 6

5.1 Criptografía de clave pública y secreta 7

5.2 Certificados de clave pública 7

5.3 Infraestructuras de clave pública 9

5.4 Infraestructura de gestión de privilegios 9

6 Aplicaciones 11

6.1 VoIP con sistemas H.323 12

6.1.1 Aspectos de seguridad relativos a multimedios y VoIP 16

6.1.2 Cómo se obtiene la seguridad en la VoIP 18

6.2 Sistema IPCablecom 20

6.2.1 Aspectos de seguridad IPCablecom 22

6.2.2 Mecanismos de seguridad de IPCablecom 22

6.3 Transmisión segura por fax 25

6.3.1 Seguridad en transmisiones de facsímil con HKM y HFX 26

6.3.2 Seguridad de facsímil con RSA 27

6.4 Aplicaciones de gestión de red 28

6.4.1 Arquitectura de gestión de red 29

6.4.2 Intersección entre plano de gestión y capa de infraestructura 30

6.4.3 Intersección entre capa de servicios y plano de gestión 31

6.4.4 Intersección del plano de gestión y la capa de aplicación 32

6.4.5 Servicios comunes de gestión de seguridad 34

6.5 Ciberrecetas médicas por Internet (E-prescriptions) 34

6.5.1 Aspectos relativos a la PKI y la PMI en aplicaciones de cibersalud 36

6.5.2 Sistema de ciberrecetas médicas de Salford 36

Página

7 Conclusiones 39

Referencias 40

Anexo A: Terminología relativa a la seguridad 41

A.1 Acrónimos relacionados con la seguridad que se utilizan frecuentemente 41

A.2 Definiciones relativas a la seguridad que se usan con frecuencia 50

A.3 Otras fuentes terminológicas del UIT-T 68

Anexo B: Catálogo de Recomendaciones UIT-T relacionadas con la seguridad 70

B.1 Aspectos de seguridad que se tratan en este manual 70

B.2 Aspectos de seguridad que no se tratan en este Manual (Fiabilidad y protección física de la planta externa) 89

Anexo C: Lista de Comisiones de Estudio y Cuestiones relativas al tema de la seguridad 94

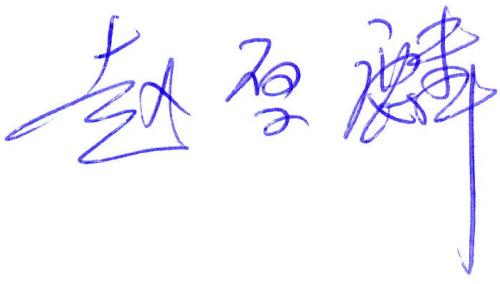
Prefacio

Si bien la seguridad digital estaba restringida en el pasado a ciertos ámbitos específicos como la banca, o las aplicaciones aeroespaciales o militares, ésta trasciende cada vez más dichas fronteras para devenir asunto de todos.

Aunque es posible que la importancia cada día mayor de la seguridad digital se deba a los titulares relacionados con la diseminación de virus informáticos por correo electrónico, o sobre los ciberdelincuentes que roban números de tarjetas de crédito, también es cierto que esto constituye sólo una parte de la historia. A medida que los ordenadores y las redes informáticas se convierten en parte importante de nuestra vida cotidiana, tal como el suministro de agua y electricidad, el tema de la seguridad digital no concierne solamente a los expertos sino también en un grado cada vez mayor a los gobiernos, las empresas y los consumidores. Siendo así, y al haber tantos aspectos comerciales y privados que dependen de los computadores y las redes, es evidente que estos sistemas han de funcionar con seguridad.

Asimismo, es evidente que la seguridad tiene que provenir de un proceso cuidadosamente desarrollado que contemple desde la concepción y el diseño del sistema, a través de su implementación, hasta las políticas y prácticas necesarias para su instalación, funcionamiento y utilización. Es indispensable que la seguridad esté presente desde un principio en el desarrollo de las normas y no durante su aplicación, pues los puntos vulnerables suelen aparecer desde el comienzo. Los Comités de normalización deben estar atentos al mercado y recopilar toda la documentación relativa a los problemas detectados, suministrar propuestas de soluciones (si las hubiere), y establecer especificaciones o directrices que permitan a los implementadores y usuarios lograr que los sistemas y servicios de comunicaciones sean tan robustos como se requiera.

Si bien desde hace muchos años el UIT-T ha tratado el tema de la seguridad de las telecomunicaciones y de las tecnologías de la información, no siempre ha sido fácil disponer del material elaborado al respecto o simplemente saber dónde encontrarlo. Con este Manual se pretende corregir este problema reuniendo toda la información disponible al respecto. Quiero manifestar mi agradecimiento a los ingenieros de la Oficina de Normalización de las Telecomunicaciones de la UIT quienes, junto con los Expertos de los Miembros de la UIT, han adelantado la mayoría de este trabajo. El Manual pretende convertirse en una guía para quienes se encargan de aspectos técnicos, los administradores, así como los reguladores, a fin de facilitar la puesta en marcha de la implementación de las funciones de seguridad. Se explican en él diversos aspectos relativos a la seguridad mediante ejemplos de aplicaciones, sin perder de vista cómo éstos son tratados en las Recomendaciones del UIT-T.



Houlin Zhao

Director de la Oficina de Normalización
de las Telecomunicaciones

UIT

Ginebra, diciembre de 2003

Resumen ejecutivo

Al desarrollarse al ritmo de un entorno comercial cada vez más mundializado, la industria de las comunicaciones ha contribuido a incrementar la productividad y a interconectar las comunidades de todo el mundo, en prácticamente todos los ramos de la industria. Buena parte de este éxito se debe al desarrollo de las normas efectuado por organizaciones como el UIT-T. Si bien las normas existentes facilitan la eficacia de las redes actuales y preparan el terreno para las futuras, el incremento de la utilización de protocolos e interfaces abiertos, la variedad de nuevos actores, la impresionante diversidad de aplicaciones y plataformas y las implementaciones no siempre eficientemente probadas han provocado un incremento de la posibilidad de que se produzcan utilizaciones malintencionadas de las redes. En los años recientes, se ha venido observando un significativo aumento de violaciones de seguridad informática (por ejemplo, la diseminación de virus y la violación de la confidencialidad de datos almacenados) en las redes mundiales, lo que con frecuencia provoca efectos costosos. Así las cosas, cabe preguntarse cómo se puede soportar una infraestructura abierta de comunicaciones sin que se exponga su información a problemas de seguridad. La respuesta reposa en los esfuerzos de los grupos de normalización tendientes a combatir las amenazas a la seguridad en todas las áreas de infraestructura de telecomunicaciones, y que van desde detalles en las especificaciones de los protocolos y en las aplicaciones hasta la gestión de las redes. Con este Manual de seguridad se pretende resaltar de manera general las Recomendaciones desarrolladas por el UIT-T, en algunos casos en colaboración con otras SDO, para garantizar la infraestructura de telecomunicaciones y los servicios y aplicaciones correspondientes, además de presentar un corto resumen de cada una de ellas.

Con el fin de poder tratar las múltiples facetas que presenta el tema de la seguridad, se debe crear un marco de trabajo y una arquitectura para así disponer de una taxonomía común que permita discutir los conceptos correspondientes.

En la cláusula 2 se resumen los elementos arquitecturales definidos en la Rec. UIT-T X.805, junto con las ocho dimensiones de seguridad que se han establecido a fin de tratar el aspecto de la seguridad extremo a extremo en aplicaciones de red: privacidad, confidencialidad de datos, autenticación, integridad, no repudio, control de acceso, seguridad de las comunicaciones y disponibilidad. Estos principios generales se utilizan como guía para entender los detalles que se tratan en las otras secciones. Los elementos más importantes incluyen las capas de seguridad, los planos de seguridad y las dimensiones que se aplican a cualquier combinación de capas y planos.

En la cláusula 3 se introducen tres términos clave para el tema de la seguridad, a saber la vulnerabilidad, las amenazas y el riesgo. Se describen las características particulares de cada uno de ellos y se proporcionan ejemplos. Un aspecto básico de esta cláusula es señalar que un riesgo de seguridad resulta de la combinación de los conceptos de vulnerabilidad y amenaza.

En la cláusula 4 se completa la información suministrada en las dos anteriores a fin de definir los metarrequisitos necesarios para establecer un marco de seguridad. Para alcanzar la seguridad contra las amenazas es fundamental definir mecanismos y algoritmos asociados con medidas de seguridad del tipo autenticación, control de acceso y criptación de datos. En la cláusula 5 se definen estos mecanismos mediante los conceptos de clave pública e infraestructuras de gestión de privilegios, que pueden utilizarse en diversas aplicaciones de usuario extremo.

Además del marco, la arquitectura y los mecanismos, el Sector ha elaborado disposiciones de seguridad para diversos sistemas y servicios que se definen en sus Recomendaciones, por lo que en el presente Manual se hace énfasis particular en las aplicaciones, tal como se muestra en la cláusula 6. Esta primera edición contiene un ejemplo del conjunto de aplicaciones, que incluye las de voz y multimedios por IP (H.323 e IPCablecom), cuidado de la salud, y fax. Estas aplicaciones se describen en términos de la arquitectura necesaria para ponerlas en funcionamiento y de cómo se hayan definido los protocolos para satisfacer los requisitos de seguridad. No basta con ofrecer seguridad para la información de aplicación, sino que también se debe suministrar a la infraestructura de red y a la gestión de los servicios de ésta. En la cláusula 6 se incluyen también ejemplos de normas en las que hay disposiciones de seguridad que conciernen a los aspectos de gestión de red.

Además, en esta versión del Manual se presenta una lista de abreviaturas y definiciones relativas a la seguridad y a otros temas que se tratan en este documento, todos extraídos de las Recomendaciones UIT-T pertinentes y de otras fuentes (como por ejemplo la base de datos SANCHO del UIT-T y el Compendio sobre seguridad de los sistemas de comunicaciones desarrollado por la Comisión de Estudio 17). Todo esto se incluye como anexo A. Asimismo, en este Manual se proporciona la versión actual del Catálogo de Recomendaciones del UIT-T sobre aspectos de seguridad (la lista presentada en el anexo B es extensa y demuestra aún más la amplitud del trabajo del UIT-T sobre la seguridad). En el anexo C se resumen los trabajos relativos a la seguridad de cada una de las Comisiones de Estudio del UIT-T. Todo el material que se incluye en estos anexos se actualiza constantemente y por ello conviene consultar el sitio web www.itu.int/ITU-T.

Se puede concluir, entonces, que el UIT-T ha jugado un papel activo, no sólo en lo relativo a las tecnologías basadas en el IP sino también para satisfacer las necesidades de otros sectores de la industria, en los que los requisitos de seguridad varían significativamente. En este Manual se indica la disponibilidad de las soluciones en las Recomendaciones del UIT-T, tanto en términos de marco genérico y arquitectura como en lo que respecta a los sistemas y aplicaciones particulares que ya están implantados globalmente por los proveedores de servicios y redes.

1 Alcance

En este Manual se proporciona una visión global de los aspectos de seguridad de las telecomunicaciones y de las tecnologías de la información, se describen aspectos prácticos conexos, y se indica cómo se estudian en el UIT-T los diversos aspectos de seguridad de las aplicaciones actuales. Su carácter es didáctico: reúne material de diversas Recomendaciones del UIT-T sobre seguridad, explicando su interrelación. Esta primera edición no cubre todos los aspectos relativos a la seguridad, en particular aquellos que tienen que ver con la disponibilidad (sobre la que el UIT-T tiene mucha experiencia), y con el daño ambiental, tema en el que también trabaja el Sector. Además, sólo se cubren aspectos basados en el trabajo ya coincluido y no en el que está en curso, el cual se tratará en ediciones futuras del Manual.

Este Manual está destinado a los ingenieros, encargados de producto, estudiantes y en general a la academia, así como a los reguladores que deseen adquirir una mejor comprensión de los aspectos relativos a la seguridad en aplicaciones prácticas.

2 Arquitectura y dimensiones básicas de seguridad

En la Rec. UIT-T X.805 se define el marco para la arquitectura y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas. Si bien los principios y definiciones generales allí tratados son válidos para todas las aplicaciones, los detalles relativos a, por ejemplo, las amenazas y vulnerabilidades y las medidas para contarrestarlas o preverlas dependen de cada aplicación.

La arquitectura de seguridad se define teniendo en cuenta dos conceptos principales, a saber las capas y los planos. Las capas de seguridad tienen que ver con los requisitos aplicables a los elementos de red y sistemas que constituyen la red extremo a extremo. El sistema de capas proporciona una perspectiva jerárquica de la seguridad extremo a extremo de la red basada en la seguridad capa por capa. Hay tres capas de seguridad: la capa de infraestructura, la capa de servicios, y la capa de aplicaciones. Una de las ventajas del modelo de capas es que se garantiza la seguridad extremo a extremo aun cuando se utilicen diferentes aplicaciones. Cada capa tiene sus propias vulnerabilidades y, por tanto, se han de definir medidas para contrarrestarlas en cada una de ellas. La capa de infraestructura comprende los dispositivos de transmisión de red, así como los elementos que la componen. Por ejemplo, son parte de dicha capa los encaminadores, los centros de conmutación y los servidores, así como los enlaces de comunicación entre ellos. La capa de servicios tiene que ver con la seguridad de los servicios de red que los proveedores prestan a sus clientes, yendo desde servicios básicos de transporte y conectividad, como las líneas arrendadas, hasta los servicios de valor añadido como la mensajería instantánea. La capa de aplicaciones tiene que ver con la seguridad de las aplicaciones de red a las que acceden los usuarios, y que van desde las básicas como el correo electrónico hasta las sofisticadas como la colaboración en vídeo, en la que se utilizan transferencias de vídeo mucho más elaboradas, por ejemplo para la prospección petrolera, el diseño de automóviles, etc.

El segundo eje central del marco de trabajo tiene que ver con la seguridad de las actividades que se efectúan en una red. Para ello, se definen tres planos de seguridad que representan los tres tipos de actividades protegidas que se realizan en ella: 1) el plano de gestión, 2) el plano de control, y 3) el plano usuario de extremo. Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como a las de usuario de extremo. El plano de seguridad de gestión, que se discute con más detalle en la cláusula 6.4, tiene que ver con las actividades (OAM&P) relacionadas con, por ejemplo, la configuración de un usuario o una red, y otras. El plano de seguridad de control se relaciona con los aspectos de señalización necesarios para establecer (y modificar) la comunicación extremo a extremo a través de la red, sin importar el medio y la tecnología utilizados en ella. El plano de seguridad de usuario de extremo tiene que ver con la seguridad cuando se accede y utiliza la red; en este plano también se considera la seguridad de flujos de datos del usuario extremo.

Además de los dos ejes principales compuestos por las capas de seguridad y planos de seguridad (tres de cada uno de ellos), en el marco se definen también ocho dimensiones, descritas en las cláusulas siguientes, que tratan la seguridad de red. Desde un punto de vista puramente arquitectural, estas dimensiones se aplican a cada una de las componentes de la matriz 3 por 3 formada entre las capas y los planos, de tal manera que se puedan tomar medidas para contrarrestar los problemas de seguridad correspondientes. En la figura 1 se indican los planos, capas y dimensiones de seguridad de la arquitectura de seguridad. En la cláusula 6.4, que versa sobre el plano de gestión, se indica cómo se tratan en otras Recomendaciones del UIT-T las tres componentes de dicha matriz para el plano de gestión.

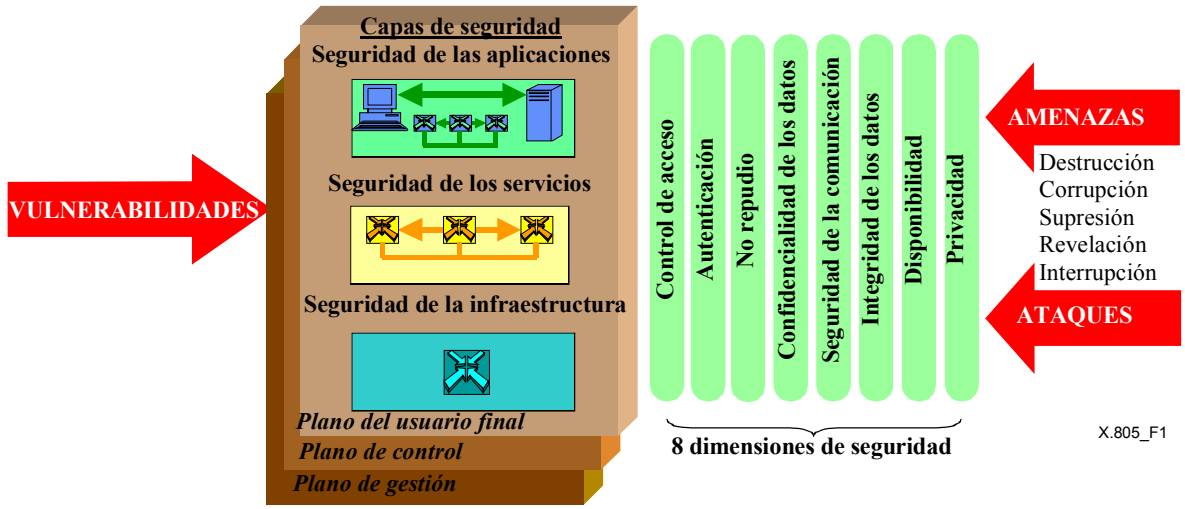


Figura 1
Elementos arquitecturales de la seguridad en la Rec. UIT-T X.805

2.1 Privacidad y confidencialidad de datos

Una de las razones principales para buscar la seguridad en las telecomunicaciones es el propio concepto de privacidad, algo que se conoce comúnmente como el derecho que tiene cada persona para controlar quién recopila y almacena información relacionada con ella, qué tipo de información y quién tiene acceso a ésta. Además, este concepto tiene que ver con los medios técnicos necesarios (por ejemplo, la criptografía) para garantizar que la información sólo llegue a los destinatarios deseados, de tal manera que solamente aquellas partes explícitamente autorizadas puedan recibirla e interpretarla.

En general, los términos privacidad y confidencialidad se confunden, aunque conviene anotar que la Rec. UIT-T X.805 establece una diferencia explícita entre la privacidad y la confidencialidad de datos, pues la primera tiene que ver con la protección de la asociación de la identidad de los usuarios y sus actividades (por ejemplo, compras en línea, sitios que visitan en la Internet, etc.), mientras que la segunda se refiere a la protección contra accesos no autorizados al contenido de los datos. Para garantizar la confidencialidad de datos se suele utilizar métodos del tipo criptación, listas de control de acceso y permisos de acceso a ficheros.

En las Recomendaciones UIT-T F.115, H.235, J.160, Q.1531, X.800 y X.805 se hace referencia al término privacidad.

2.2 Autenticación

La autenticación consiste en probar la veracidad de la identidad reclamada por una entidad. En este contexto, se consideran entidades no solamente a las personas sino también los mecanismos, servicios y aplicaciones. Con la autenticación se pretende también garantizar que una entidad no esté tratando de usurpar una identidad o de emitir una respuesta no autorizada a una comunicación previa. Existen dos tipos de autenticación, a saber la autenticación de origen de datos (es decir aquella necesaria en caso de asociación orientada a la conexión) y la autenticación de entidad par (es decir, aquella presente en una asociación sin conexión). La red debe garantizar que se establece un intercambio de datos con la entidad par destinataria (y no con una que trate de suplantar la identidad o de responder a una comunicación previa) y que el origen de los datos sea el que se reclama. En general, tras la identificación viene la autenticación. La red debe proteger la información que se utiliza para la identificación, la autenticación y la autorización.

En las Recomendaciones UIT-T F.500, F.851, F.852, H.235, J.160, J.93, J.95, M.60, X.217, X.217*bis*, X.509, X.800, X.805 y X.811 se hace referencia al término Autenticación.

2.3 Integridad de datos

Propiedad que consisten en que los datos no han sido alterados de una manera no autorizada. Además, la integridad de los datos garantiza que la información esté protegida contra las siguientes operaciones no autorizadas: modificación, supresión, creación, y copia de los datos. Se proporciona también un indicador de estas actividades no autorizadas.

En las Recomendaciones UIT-T H.235, J.160, J.93, J.95, Q.1290, Q.1531, X.800 y X.815 se hace referencia al término Integridad.

2.4 No repudio

Capacidad de evitar que un usuario niegue más adelante haber efectuado una acción. Entre éstas se incluyen la creación, origen, recepción y entrega de contenidos, por ejemplo envío o recepción de mensajes, establecimiento o recepción de llamadas, la participación en conferencias de audio y vídeo, etc.

Gracias a los requisitos de no repudio que se imponen, es posible colectar pruebas infalsificables del envío y/o recepción de datos a fin de evitar que el remitente niegue haber enviado un mensaje o el destinatario haberlo recibido. En la red se puede implementar esta característica mediante cualquiera o ambos de los dos métodos siguientes: se suministra a quien recibe la información prueba del origen de ésta, de tal manera que el remitente no pueda negar haberla enviado o rehusar su contenido; se proporciona al remitente una prueba de la entrega de los datos, de tal manera que el destinatario no pueda negar más adelante haberlos recibido.

En las Recomendaciones UIT-T F.400, F.435, F.440, J.160, J.93, J.95, M.60, T.411, X.400, X.805, X.813 y X.843 se hace referencia al término no repudio.

2.5 Otras dimensiones definidas en X.805

Además de la privacidad y la confidencialidad de datos, la autenticación, la integridad y el no repudio, esta Recomendación define otras tres dimensiones de seguridad: control de acceso, seguridad de la comunicación, y disponibilidad.

La dimensión de seguridad del *control de acceso* protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. El control de acceso se define en la cláusula 6.3/X.810 y en la Rec. UIT-T X.812. Aunque tiene que ver con la autenticación, está fuera del alcance de ésta.

La dimensión de seguridad *comunicación* es una nueva dimensión que se define en la Rec. UIT-T X.805 y que garantiza que los flujos de información sólo circulan entre los puntos extremos autorizados. Está relacionada con las medidas para controlar los flujos de tráfico de red tendientes a evitar la desviación y la interceptación de la información que circula.

La dimensión de seguridad *disponibilidad* garantiza que una interrupción de la red no impida el acceso autorizado a los elementos de ésta, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de desastre y para restablecimiento de la red.

3 Vulnerabilidades, amenazas y riesgos

Suele ocurrir que ante el imperativo deseo de poner en marcha la solución IT más ventajosa o de querer determinar cuál de las últimas aplicaciones, servidores y bases de datos en Internet se acomodan mejor a los objetivos de una organización, se deje en un segundo plano la protección de la información que contienen todos estos elementos. Es probable que en muchas empresas se piense erróneamente que al no haber sido aún víctimas de algún intento de ataque, no existe ninguna amenaza para ellos.

Los organismos de normalización poseen capacidades y responsabilidades únicas para tratar el tema de las vulnerabilidades de la seguridad en los protocolos. Hay algunas medidas inmediatas y relativamente simples que éstos pueden emprender a fin de mejorar la seguridad de todos los protocolos que se están normalizando actualmente.

Una *vulnerabilidad de seguridad* es un defecto o debilidad en el diseño, implementación o funcionamiento de un sistema que podría ser utilizado para violar su seguridad (RFC 2828). Una vulnerabilidad de seguridad no es un riesgo, amenaza o ataque.

Hay cuatro tipos de vulnerabilidades: vulnerabilidad *modelo de amenaza*, que resulta de la dificultad para prever amenazas futuras (por ejemplo en el sistema de señalización N.º 7); vulnerabilidad *diseño y especificación*, producida de errores o descuidos en el diseño del protocolo que lo hacen inherentemente vulnerable (por ejemplo la norma WEP 802.11b del IEEE, también conocida como WiFi); vulnerabilidad *implementación*, que se produce como resultado de errores en la implementación del protocolo; y para terminar, vulnerabilidad *funcionamiento y configuración*, que resulta de la utilización errónea de opciones en las implementaciones o de políticas insuficientes de instalación (por ejemplo, cuando el administrador de red no facilita la utilización de la criptación en una red WiFi, o cuando escoge un cifrado de trenes que no es suficientemente robusto).

Conforme a la Rec. UIT-T X.800, una *amenaza de seguridad* es una violación potencial de la seguridad, que puede ser activa, es decir que existe la posibilidad de un cambio deliberado y no autorizado del estado del sistema, o pasiva, cuando hay amenaza de revelación no autorizada de la información sin que se modifique el estado del sistema. Ejemplos de amenazas activas son la usurpación de identidad, como entidad autorizada, y la negación de servicio. Un ejemplo de amenaza pasiva es la escucha clandestina tendiente a robar contraseñas no criptadas. Estas amenazas pueden provenir de piratas informáticos, terroristas, vándalos, del crimen organizado, o pueden tener origen en alguna entidad estatal, pero en muchas ocasiones provienen del interior mismo de la organización.

Un *riesgo de seguridad* ocurre cuando se combinan una vulnerabilidad y una amenaza de seguridad. Por ejemplo, un problema de programación que origine desbordamiento en una aplicación de sistema operativo (es decir una vulnerabilidad) que se asocie con el conocimiento de un pirata, y las herramientas y acceso correspondientes (es decir, una amenaza) puede degenerar en un riesgo de ataque al servidor Internet. Las consecuencias de los riesgos de seguridad son las pérdidas, y corrupción de datos, la pérdida de privacidad, el fraude, el tiempo fuera de servicio, y la disminución de la confianza del público.

Aunque las amenazas cambien, siempre habrá vulnerabilidades de seguridad durante toda la vida de un protocolo. Si se trata de protocolos normalizados, los riesgos de seguridad basados en el protocolo pueden ser bastante importantes y de escala global, por lo que es importante entender e indificar las vulnerabilidades en los protocolos.

4 Requisitos del marco de seguridad

Los requisitos necesarios para contar con un marco de seguridad de red genérico se originan de cuatro fuentes diferentes:

- Los clientes/abonados deben confiar en la red y los servicios que ofrece, incluida la disponibilidad de éstos (en particular, los de urgencia) en caso de grandes catástrofes (incluidos los atentados terroristas).

- Las autoridades exigen un nivel de seguridad mediante normas y leyes, a fin de garantizar la disponibilidad de los servicios, la libre competencia y proteger la privacidad.

- Los operadores de red y los proveedores de servicios necesitan seguridad para salvaguardar su funcionamiento e intereses comerciales, y cumplir con sus obligaciones ante los clientes y el público.

Conviene que los requisitos de seguridad de las redes y servicios de telecomunicaciones se basen en normas de seguridad internacionalmente aceptadas, puesto que así se incremente el interfuncionamiento y se evita la duplicación de esfuerzos. Puede ocurrir que la prestación y utilización de servicios y mecanismos de seguridad sea bastante costosa con respecto al valor de las transacciones que se protegen, por lo que debe encontrarse un equilibrio entre el costo de las medidas de seguridad y los efectos financieros potenciales de posibles fallos en ella. Siendo así, es importante ser capaz de adaptar la seguridad disponible con los servicios que se protegen, y para ello se deben suministrar mecanismos y servicios de seguridad que permitan dicha adaptación. Debido a la gran cantidad de combinaciones posibles de las características de seguridad, cabe esperar que haya perfiles de seguridad que cubran una amplia gama de servicios de redes de telecomunicaciones.

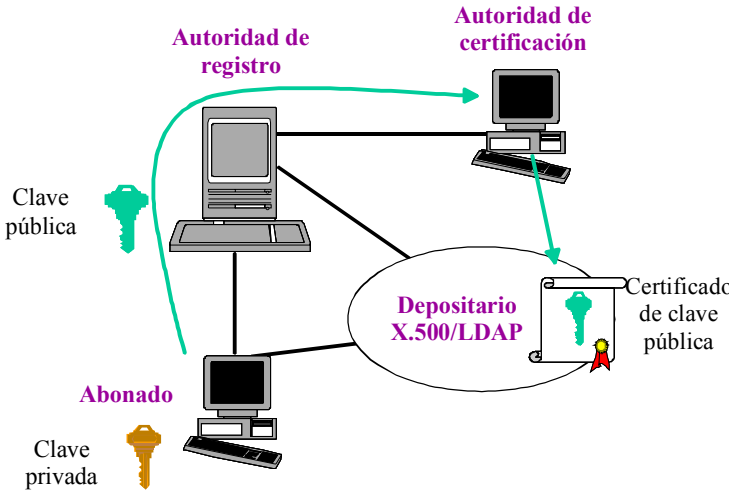
Gracias a la normalización, se podrán reutilizar más fácilmente las soluciones y productos, lo que implica lograr la seguridad de una manera más rápida y a un menor costo.

Tanto los fabricantes como los usuarios de sistemas gozan de importantes beneficios gracias a las soluciones normalizadas: la economía de escala en el desarrollo del producto y el interfuncionamiento de los componentes en la red de telecomunicaciones en lo que respecta a la seguridad.

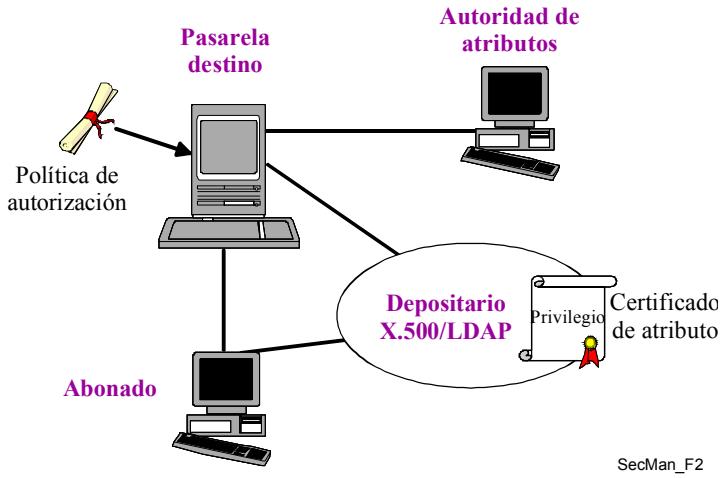
Los servicios y mecanismos de seguridad que se pueden suministrar a las redes de telecomunicaciones o a los proveedores de servicios tienen que ver con la protección contra ataques malintencionados, como por ejemplo la negación de servicio, la escucha clandestina, la simulación, la manipulación de mensajes (modificación, retardo, supresión, inserción, reenvío, reencaminamiento, encaminamiento erróneo, o reordenamiento de mensajes), el repudio o la falsificación. La protección incluye la prevención, detección y recuperación tras ataques, medidas para prever cortes de servicio debido a eventos naturales (clima, etc.) así como la gestión de la información relativa a la seguridad. Es necesario prever disposiciones que permitan la intercepción legal cuando las autoridades correspondientes así lo demanden.

5 PKI y gestión de privilegios según la Rec. UIT-T X.509

La infraestructura de clave pública (PKI) de la Rec. UIT-T X.509 proporciona una norma para autenticación robusta, que se basa en certificados de clave pública y en autoridades de certificación. Gracias a ella se tiene una metodología adaptable para autenticar los mensajes entre las partes que se comunican. Una PKI está compuesta fundamentalmente por la tecnología de criptografía de clave pública, por lo que ésta se describe en primera instancia. Además, en la Rec. UIT-T X.509 también se propone una infraestructura de gestión de privilegios (PMI), que define una norma para la autorización robusta basándose en certificados de atributos y autoridades de atributos. Esta infraestructura se utiliza para establecer los derechos y privilegios de los usuarios. En la figura 2 se muestran los componentes de la PKI y la PMI.



(a) Componentes de una infraestructura de claves públicas



(b) Componentes de una infraestructura de gestión de privilegios

Figura 2
Componentes de una PKI y una PMI

5.1 Criptografía de clave pública y secreta

Por criptografía *simétrica* (o *clave secreta*) se entiende un sistema criptográfico en que las claves de cifrado y descifrado son iguales, tal como se muestra en la figura 3(a). En estos sistemas es necesario que los participantes compartan una clave secreta única desde un principio, la misma que debe ser distribuida a éstos a través de medios seguros, puesto que su conocimiento implica el de la clave de descifrado y viceversa.

Como se muestra en la figura 3(b), un sistema de criptografía *asimétrica* (o de *clave pública*) involucra un par de claves, a saber una pública y una privada. Como su nombre lo indica, una se hace pública mientras que la otra se mantiene secreta. Ambas son diferentes y aunque exista una relación matemática entre ellas no es posible calcular la clave privada a partir de la pública. Si bien las claves públicas se consiguen con facilidad, las privadas siempre se mantienen secretas (por ejemplo, en una tarjeta inteligente o en una llave, así como en un futuro en un PDA o en un teléfono móvil). Normalmente, un usuario encripta datos confidenciales utilizando la clave pública del destinatario para enviárselos a otra persona, mientras que quien los recibe los descifra con su clave privada correspondiente. A fin de poder enviar información autenticada, el remitente la cripta con su clave privada, y el destinatario la autentica con la clave pública correspondiente al primero. No obstante, esta criptación asimétrica tiene un par de desventajas. En primer lugar, la criptación de clave pública consume demasiados recursos de computación, por lo que no es eficiente para mensajes completos. En segundo lugar, no se pueden encaminar mensajes hacia los recipientes si están completamente criptados, puesto que los nodos intermedios no son capaces de determinar a quién van dirigidos. Por consiguiente, por lo general la criptación asimétrica se utiliza solamente para criptar partes pequeñas de los mensajes. Siempre que se requiera un cierto nivel de confidencialidad, se cripta el mensaje mediante la criptación simétrica tradicional, y se cripta asimétricamente la clave simétrica utilizando la clave pública del destinatario. De requerirse la autenticación, se aplica al mensaje una función hash segura unidireccional, como por ejemplo SHA1 o MD5, y el resultado de 160 ó 128 bits se cripta asimétricamente mediante la clave privada del remitente y se anexa al mensaje (que se envía sin criptar) antes de la transferencia. Esta suma de control criptográfica es lo que se conoce como una firma digital, algo importante en el comercio electrónico.

La criptografía de clave pública depende de que la gente tenga las claves públicas correctas de cada titular de clave privada que participa en la comunicación. Si, por ejemplo, Víctor cree erróneamente que tiene la clave pública de Lourdes, cuando en realidad tiene la de Juana, pensará que los mensajes con firma digital de esta última provienen de Lourdes (lo que permitiría a Juana suplantar a Lourdes). Más aun, si Víctor desea enviar un mensaje confidencial a Lourdes, Juana podría interceptarlo y descifrarlo, mientras que Lourdes simplemente no podría leerlo. Es entonces importantísimo que las personas puedan comprobar a quién pertenece en realidad una clave pública.

5.2 Certificados de clave pública

También conocidos como "certificados digitales" son una manera de validar a quien pertenece un par de claves asimétricas. Un certificado de clave pública vincula fuertemente una clave pública al nombre de su propietario, y viene firmado digitalmente por la autoridad de confianza que atestigua esta vinculación. Ésta es la autoridad de certificación (CA). En la norma X.509 se define el formato normalizado reconocido internacionalmente para los certificados de clave pública, es decir uno que contenga una clave pública, un identificador del algoritmo asimétrico que debe utilizarse con ella, el nombre del propietario del par de claves, el nombre de la CA que atestigua la propiedad, el número de serie y la duración de la validez del certificado, el número de la versión de la Rec. UIT-T X.509 a la que es conforme el certificado, y un conjunto facultativo de campos de extensión que mantienen información

sobre la política de certificación de la CA. Luego, se firma digitalmente todo el certificado utilizando la clave privada de la CA, tras lo cual se puede publicar el certificado X.509 en, por ejemplo, un sitio web, un directorio LDAP, o en la Vcard adjunta a los mensajes de correo electrónico, puesto que la firma de la CA garantiza que su contenido no puede ser alterado sin que se sepa.

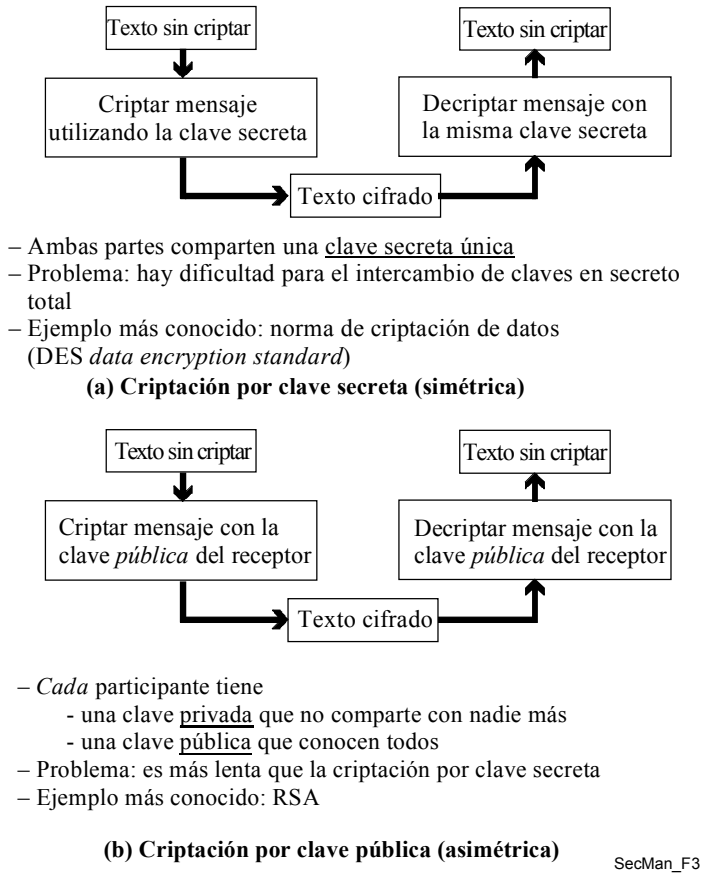


Figura 3
Procesos de criptación de clave simétrica (o privada) y asimétrica (o pública) y sus características principales

Es evidente que para poder validar un certificado de clave pública de un usuario, una persona ha de tener acceso a la clave pública válida de la CA que emitió dicho certificado, a fin de poder verificar la firma que aparece en el certificado del usuario. Al mismo tiempo, puede ocurrir que la CA haya certificado su clave pública ante otra CA (de orden superior), o lo que es lo mismo el proceso de validación de claves públicas se vuelve recursivo a medida que nos desplazamos en la cadena de certificación. Esto, por supuesto, debe tener un fin, lo que en general ocurre cuando se llega al certificado autofirmado de la CA que es nuestra "raíz de confianza". Las claves públicas CA raíz se distribuyen como certificados autofirmados (la CA raíz certifica que se trata de su propia clave pública). Con esta firma, es posible garantizar que la clave y el nombre de la CA no han sido manipulados desde que se creó el certificado. No obstante, al ser la misma CA quien inserta el nombre en el certificado autofirmado, no se puede tomar éste al pie de la letra. En otras palabras, en una

estructura de clave pública es fundamental distribuir seguramente las claves públicas de la CA raíz (como certificados autofirmados), de manera que se pueda garantizar que la clave pública pertenece realmente a la CA raíz mencionada en el certificado autofirmado. Sin ello, no se podría garantizar que alguien no esté suplantando a la CA raíz.

5.3 Infraestructuras de clave pública

El objetivo principal de una PKI es emitir y gestionar certificados de clave pública, incluido el certificado autofirmado de la CA raíz. La gestión de claves incluye la creación de pares de claves, la creación y la revocación de certificados de clave pública (por ejemplo, cuando la clave privada de un usuario haya sido violada), el almacenamiento y archivo de claves y certificados y su destrucción una vez que lleguen al final de su validez. Cada CA funcionará conforme a un conjunto de políticas, y la norma X.509 aporta los mecanismos para distribuir (una parte) esta información relativa a las políticas en los campos de extensión de los certificados X.509 emitidos por dicha CA. Se suelen definir las reglas y procedimientos de las políticas a seguir por una CA en una política de certificados (CP, *certificate policy*) y en una declaración de prácticas de certificación (CPS, *certification practice statement*), que son documentos publicados por la CA, y que ayudan a garantizar una base de calidad común para la evaluación de la confianza que se puede tener en los certificados de clave pública emitidos por las CA, internacionalmente y entre los diferentes sectores. Asimismo, estos mecanismos nos facilitan (una parte) el marco jurídico necesario para el establecimiento de la confianza entre organizaciones así como para la especificación de los límites relativos a la utilización de dichos certificados.

Cabe observar que a fines de autenticación, cuando se utilizan certificados de clave pública, es necesario que los puntos extremo suministren firmas digitales mediante el valor de la clave privada correspondiente. El solo intercambio de certificados de clave pública no protege contra los ataques de intermediarios.

5.4 Infraestructura de gestión de privilegios

En la primera versión de la Rec. UIT-T X.509 se especifican los elementos básicos de las infraestructuras de clave pública (PKI), incluida la definición de los certificados de clave pública. En la versión de 2000 se amplía significativamente el concepto de "Certificados de Atributo" y se proporciona un marco para la infraestructura de gestión de privilegios. De esta manera, es posible fijar privilegios de acceso de usuario en un entorno en que hay equipos de múltiples fabricantes y se cuenta con diversas aplicaciones.

Aunque existen varias similitudes entre los conceptos de PMI y PKI, el primero de ellos tiene que ver con la autorización mientras que el segundo se concentra en la autenticación. En la figura 2 y el cuadro 1 se indican las similitudes entre ambas infraestructuras.

Cuadro 1
Comparación entre las características de las infraestructuras de la gestión de privilegios y la clave pública

Infraestructura de gestión de privilegios	Infraestructura de clave pública
Autoridad fuente (SoA)	Autoridad de certificación raíz (vínculo de confianza)
Autoridad de atributos (AA)	Autoridad de certificación
Certificado de atributo	Certificado de clave pública
Lista de revocación de certificados de atributo	Lista de revocación de certificados
Lista de revocación de autoridad para PMI	Lista de revocación de autoridad para PKI

Al atribuir privilegios a los usuarios se garantiza que éstos sigan una política de seguridad preestablecida por la autoridad fuente. Dicha información relativa a la política está vinculada al nombre de usuario en el certificado de atributo y contiene diversos elementos, como se muestra en la figura 4.

Versión
Titular
Emisor
Firma (ID de algoritmo)
Número de serie de certificado
Periodo de validez
Atributos
ID único de emisor
Extensiones

Figura 4
Estructura de un certificado de atributo X.509

Hay cinco componentes para el control de una PMI que se describen en la Rec. UIT-T X.509, a saber el afirmador de privilegios, el verificador de privilegios, el método de objeto[1], la política de privilegios, y las variables ambientales (véase la figura 5). Con estas técnicas el verificador de privilegios puede controlar el acceso al método de objeto mediante el afirmador de privilegios, de conformidad con la política de privilegios.

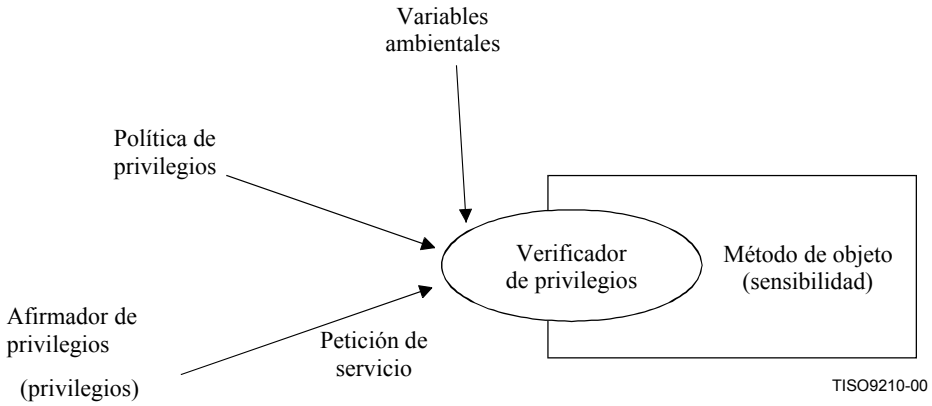


Figura 5
Modelo de control PMI X.509

[1] Un método objeto es una acción que puede ser invocada en un recurso (por ejemplo, un sistema de ficheros puede haber leído, escrito y ejecutado métodos objeto).

Cuando sea necesario delegar el privilegio en una implementación en la Rec. UIT-T X.509, existen cuatro componentes del modelo de delegación para PMI, a saber el verificador de privilegios, la SoA, otras AA y el afirmador de privilegios (véase la figura 6).

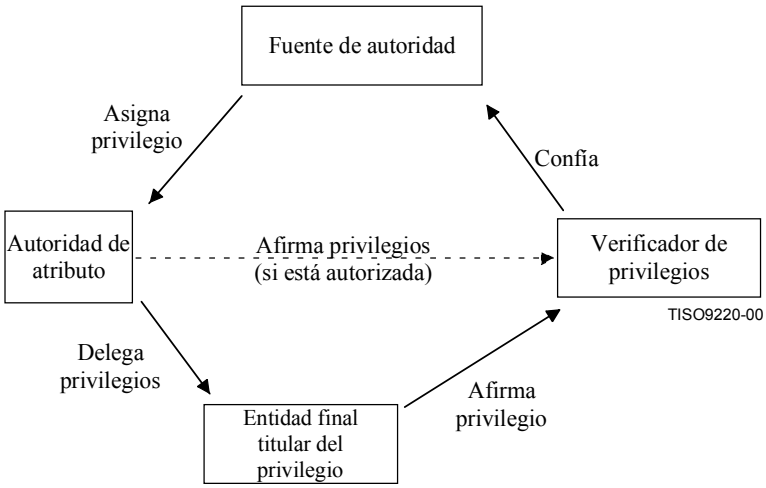


Figura 6
Modelo de delegación de PMI X.509

En algunas implementaciones de los métodos de autorización que siguen el modelo de control de acceso basado en las funciones (RBAC, *role-based access control*) se considera que se asigna una función al usuario. La política de autorización hace corresponder un conjunto de permisos a dicha función. Al acceder a un recurso, la función del usuario se compara con la política a fin de permitir toda acción subsiguiente. En la cláusula 6.5.2 se muestra la utilización de un sistema RBAC: la aplicación de recetas médicas por Internet (*e-prescriptions*).

6 Aplicaciones

En esta cláusula se tratan aplicaciones de dos clases diferentes. La primera, incluye las aplicaciones de usuario extremo, como por ejemplo la VoIP, para la que se describen la arquitectura y los componentes de red utilizados para proporcionar dicha aplicación de usuario extremo. Se discuten aspectos de seguridad y soluciones relacionados con los tres planos que soportan las aplicaciones multimedios, para las que la VoIP constituye un caso particular. Además, se consideran otras aplicaciones de usuario extremo como el sistema IPCablecom, con el que se ofrecen servicios basados en el IP en tiempo real por una red de cable, y la transmisión por fax. También se tratan algunas aplicaciones que no son específicas de la industria de las telecomunicaciones, como por ejemplo los servicios de salud por Internet, en particular un sistema para las *e-prescriptions*. La segunda clase de aplicaciones tiene que ver con las de gestión de red. La seguridad es importante a fin de poder cumplir con los requisitos de calidad e integridad de los servicios ofrecidos por los proveedores. Es decir, las actividades de gestión han de ser ejecutadas con los privilegios y la autorización correspondientes.

6.1 VoIP con sistemas H.323

La VoIP, también conocida como telefonía IP, consiste en la prestación de los servicios que tradicionalmente se ofrecen a través de la red telefónica pública conmutada (RTPC) con conmutación de circuitos mediante una red que utilice el protocolo IP (en el que también se basa la Internet). Estos servicios incluyen antes que nada el tráfico de voz, y los servicios suplementarios correspondientes tales como la conferencia vocal (puenteada), reenvío de llamada, llamada en espera, multilínea, desviación de llamada, depósito y extracción de llamada, consulta, y seguimiento de llamada, entre otros servicios de red inteligente, y así como para algunos datos de la banda vocal. La voz por Internet es un caso particular de la VoIP, en el que el tráfico vocal se hace pasar a través de la red troncal pública de Internet.

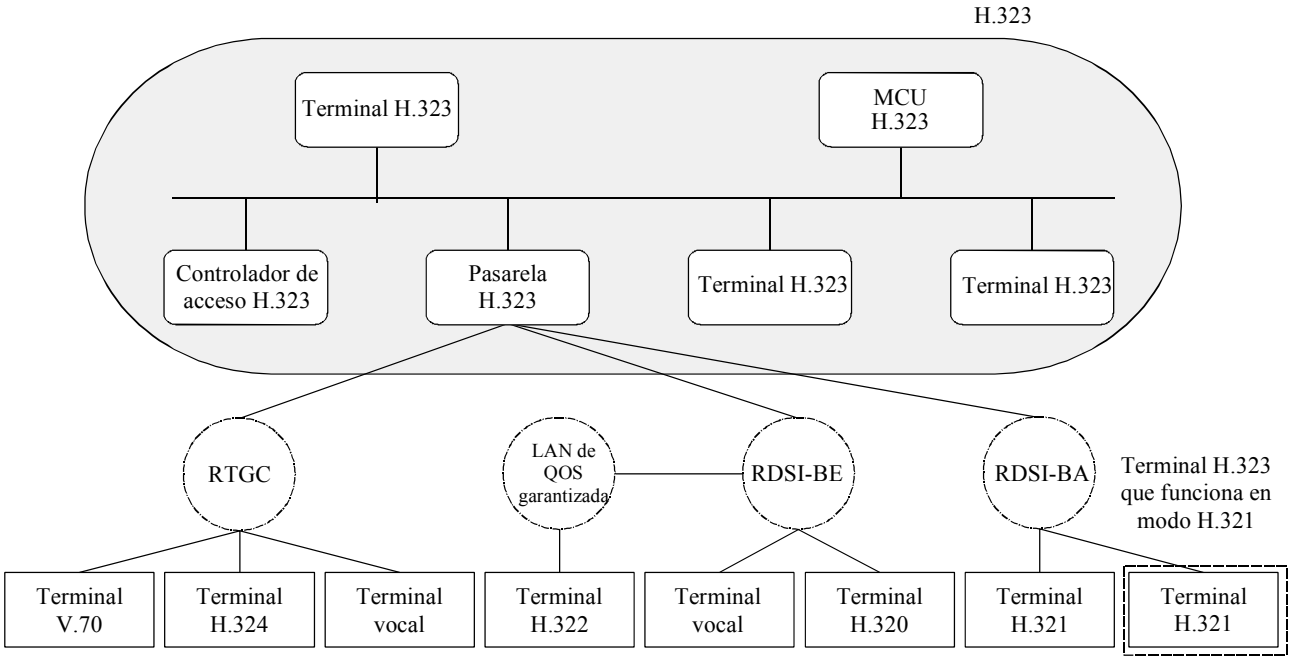
La Rec. UIT-T H.323 es una Recomendación UIT-T general que proporciona los fundamentos de las comunicaciones de audio, vídeo y datos por redes de área local (LAN), o a través de redes basadas en el IP, incluida Internet, que no proporcionan una calidad de servicio (QoS) garantizada. Este tipo de redes son las que se imponen en la industria hoy en día y entre ellas se encuentran las redes TCP/IP con conmutación de paquetes y la IPX por Ethernet, Ethernet rápido y las tecnologías de red en anillo con paso de testigo (*token ring*). Al conformarse a la Rec. UIT-T H.323, los productos y aplicaciones multimedios de los diferentes fabricantes pueden interfuncionar entre ellos, permitiendo así que los usuarios se comuniquen sin tener que preocuparse por los aspectos de compatibilidad. El primer protocolo VoIP que se definió fue el H.323, considerado como la piedra angular de los productos basados en las LAN para aplicaciones destinadas al usuario individual, a las empresas, al entretenimiento y a los profesionales. Las principales Recomendaciones que forman parte del sistema H.323 son:

- H.323 – Documento "general" que describe la utilización de H.225.0, H.245 y otros documentos conexos para la distribución de servicios de conferencia multimedios basados en paquetes.
- H.225.0 – Describe tres protocolos de señalización (RAS, señalización de llamada y "anexo G").
- H.245 – Protocolo de control para comunicaciones multimedios (común para H.310, H.323 y H.324).
- H.235 – Seguridad en los sistemas basados en H.245.
- H.246 – Interfuncionamiento con la red telefónica pública conmutada (RTPC).
- H.450.x – Servicios suplementarios.
- H.460.x – Diversas extensiones del protocolo H.323.
- H.501 – Protocolo para la gestión de movilidad y la comunicación intradominio e interdominio en los sistemas multimedios.
- H.510 – Movilidad de usuario, de terminal y de servicio.
- H.530 – Especificación de seguridad para H.510.

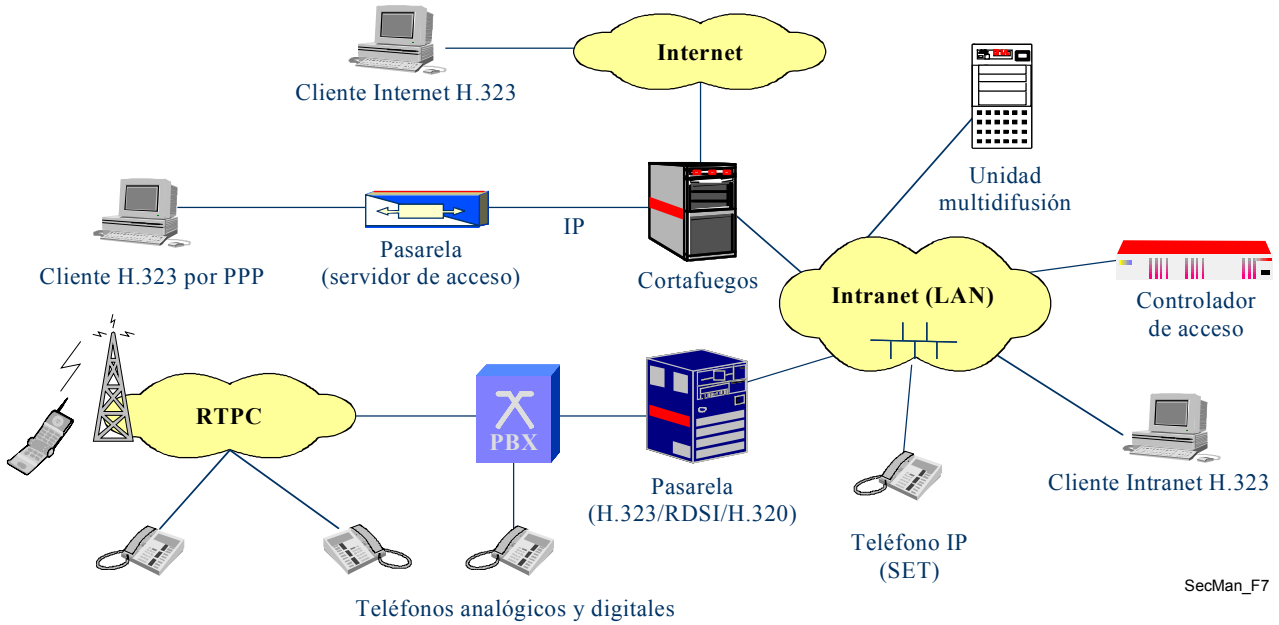
En 1996, el UIT-T aprobó la primera versión de la Rec. UIT-T H.323, mientras que la segunda fue aprobada en enero de 1998 y la actual (versión 5) en julio de 2003. Dicha norma es bastante amplia en cuanto a su alcance e incluye tanto dispositivos autónomos como tecnología de computadores personales integrada, así como las conferencias punto a punto y multipunto. De igual manera, en dicha Recomendación se tratan el control de llamada, la gestión de multimedios y la gestión de ancho de banda así como las interfaces entre las LAN y otras redes.

La Rec. UIT-T H.323 forma parte de una serie más general de normas de comunicaciones con las que se permiten las videoconferencias a través de toda una gama de redes diferentes. Esta serie, conocida como H.32X, incluye las Recomendaciones UIT-T H.320 y H.324, sobre las comunicaciones RDSI y RTPC, respectivamente. En este Manual se presenta un resumen general de la norma H.323, de sus beneficios, arquitectura y aplicaciones.

En dicha Recomendación se definen cuatro componentes principales de un sistema de comunicaciones basado en redes: terminales, pasarelas, controladores de acceso y unidades de control multipunto. Además, se permiten los elementos de frontera o pares. En la figura 7 se pueden ver todos estos elementos.



(a) Sistemas H.323 y sus componentes [Packetizer]



(b) Casos de implementación H.323 [Euchner]

Figura 7
Sistema H.323: componentes y casos de implementación

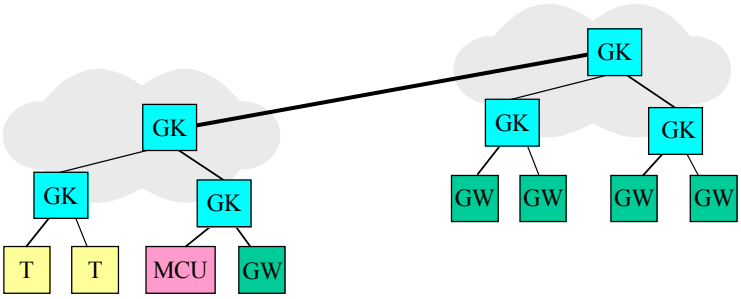
Los *terminales (T)* son los puntos extremos del cliente en la red troncal IP que proporcionan comunicaciones bidireccionales. Los terminales H.323 deben soportar comunicaciones vocales y pueden soportar códecs de vídeo, protocolos de conferencia de datos T.120, y capacidades MCU. Algunos ejemplos son: los teléfonos IP, los teléfonos con vídeo, los dispositivos IVR, los sistemas de correo vocal, los "teléfonos informatizados" (por ejemplo, NetMeeting™).

La *pasarela (GW)* es un elemento facultativo a toda conferencia H.323, que proporciona diferentes servicios, entre ellos el de actuar como función de traducción entre los puntos extremos de la conferencia H.323 y otros tipos de terminal. En esta función se incluye la traducción entre los formatos de transmisión (por ejemplo de H.225.0 a H.221) y entre los procedimientos de comunicación (por ejemplo de H.245 a H.242). Además, la pasarela también efectúa la traducción entre los códecs de audio y vídeo y realiza el establecimiento y liberación de llamada tanto en el lado de la LAN como en el de la red con conmutación de circuitos.

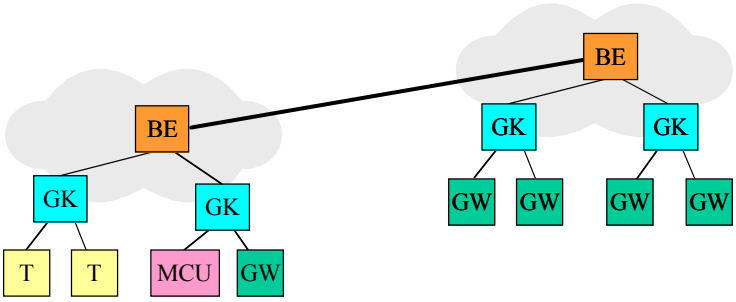
El *controlador de acceso (GK)* es la parte fundamental de toda red en la que se utiliza la H.323. Actúa como punto central para todas las llamadas dentro de su zona y suministra los servicios de control de llamada a todos los puntos extremos registrados. Cabe decir que un controlador de acceso H.323 se comporta como una central virtual ya que realiza el control de admisión, la resolución de la dirección, y puede permitir que una llamada se establezca directamente entre puntos extremos o encaminar la señalización de llamada a través de sí mismo realizando así funciones del tipo sígueme/encuéntreme (follow-me/find-me), reenvío en caso de ocupado, etc. Hay elementos de frontera *(BE, border elements)*, (o pares) asociados con los controladores de acceso, que se encargan de intercambiar información de direccionamiento y participar en la autorización de llamada entre los dominios administrativos. Gracias a esta funcionalidad se podrá también intercomunicar las diferentes redes o "islas" H.323. Esto se logra a través del intercambio de una serie de mensajes, como se muestra en la figura 8.

Una *unidad de control multipunto (MCU)* soporta conferencias entre tres o más puntos extremos. Conforme a la Rec. UIT-T H.323, una MCU tiene que incluir un controlador multipunto, mientras que puede o no tener varios procesadores multipunto. El controlador multipunto se encarga de la señalización de llamada aunque no tiene que ver directamente con ninguno de los trenes de medios, lo que se deja a los procesadores multipunto, que se encargan de mezclar, conmutar y procesar los bits de audio, vídeo y/o datos. Las capacidades de controlador multipunto y procesador multipunto pueden venir incorporadas en un componente específico para ello o ser parte de otros componentes H.323.

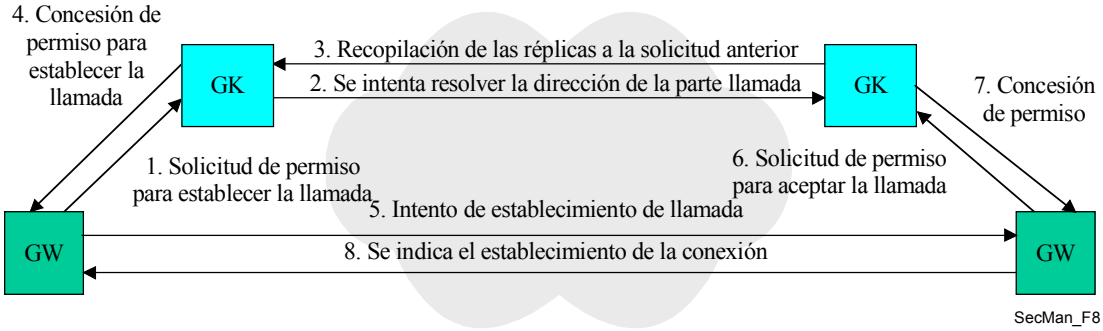
A pesar de haber sido diseñado desde un principio como protocolo multimedios, el protocolo H.323 se utiliza principalmente hoy en día en el mercado de la voz por IP. Las redes de este tipo que funcionan actualmente transportan miles de millones de minutos de tráfico de voz y vídeo cada mes (considerando solamente las redes públicas); hasta el punto de que la mayor parte del tráfico VoIP se transporta en la actualidad por sistemas H.323. Según estudios recientes, se considera que el tráfico de VoIP corresponde a más del 10% de todo el tráfico de larga distancia internacional. Asimismo, el tráfico de vídeo H.323 sigue aumentando constantemente. Esto se debe principalmente a que el protocolo y sus implementaciones han alcanzado la madurez, y a que la solución H.323 ha demostrado ser perfectamente escalable y satisfacer las necesidades tanto de los proveedores de servicios como de los clientes institucionales, utilizando productos H.323 que van desde las pilas de protocolos y los circuitos integrados hasta los teléfonos inalámbricos y los dispositivos necesarios para la conferencia de vídeo.



(a) Topología con RAS[1]



(b) Topología con el anexo G/H.225.0



(c) Flujo de llamada de alto nivel

BE: elemento de frontera; GK: controlador de acceso; GW: pasarela;
MCU: unidad de control multipunto; T: terminal

Figura 8
Comunicación entre dominios administrativos

Las funcionalidades con que cuentan los sistemas H.323 son:

- capacidad de conferencia de voz, vídeo y datos;
- comunicación entre diversos tipos de terminales, incluidos PC a teléfono, fax a fax, teléfono a teléfono y llamadas a través de la Internet;
- soporte de fax y módem por IP, conforme a la Rec. UIT-T T.38;
- diversos servicios suplementarios (reenvío de llamada, extracción de llamada, etc.);

- interoperabilidad robusta con otros sistemas de la serie H.32x, incluidos los de las Recomendaciones UIT-T H.320 (RDSI) y H.323M (servicios móviles inalámbricos 3GPP);
- especificación de la descomposición de la pasarela de medios (a través del protocolo de control de pasarelas H.248);
- soporte de seguridad de señalización y medios;
- movilidad de usuario, terminal y terminal de servicio;
- soporte de la señalización de los servicios de urgencia.

La norma H.323 es utilizada, por ejemplo, por los operadores para el tráfico al por mayor, en especial por las rutas troncales de VoIP (conmutadores de clase 4 para el tráfico vocal), y los servicios de llamada con tarjeta de crédito. En las empresas, se utiliza la norma H.323 para, por ejemplo, IP-PBX, IP-Centrex, VPN para tráfico de voz, sistemas integrados de voz y datos, teléfonos WiFi, implementación de centros de llamadas, y servicios de movilidad. En el caso de las comunicaciones profesionales, se utiliza ampliamente para las conferencias de voz (o audio) y vídeo, para la colaboración vocal/de datos/de vídeo y para la formación a distancia. En los hogares, su utilización incluye el acceso audiovisual de banda ancha, PC a teléfono, y para la prestación de servicios de noticias e información adaptados a cada persona.

6.1.1 Aspectos de seguridad relativos a multimedios y VoIP

Al estar geográficamente distribuidos y debido a la naturaleza abierta de las redes IP, todos los elementos de un sistema H.323 están expuestos a amenazas, como se muestra en la figura 9.

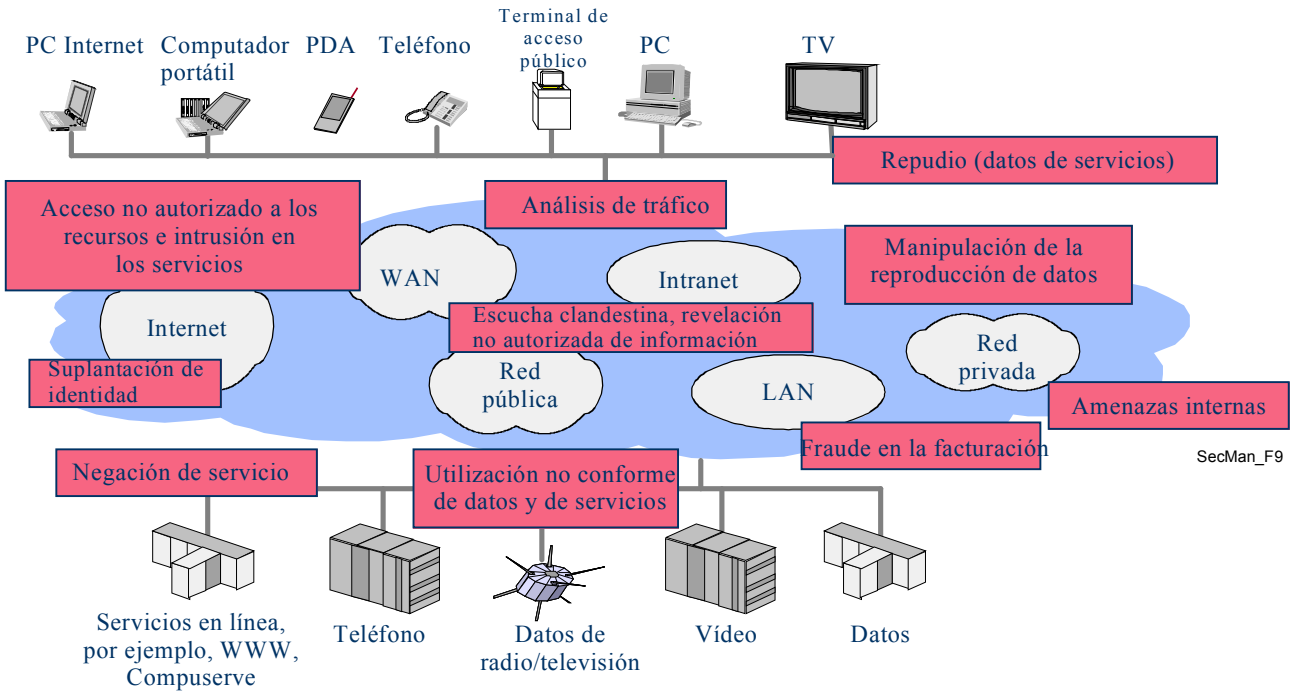


Figura 9
Amenazas contra la seguridad en las comunicaciones multimedios

Según [Euchner] los aspectos de seguridad más importantes en las comunicaciones multimedios y en la telefonía IP son en general:

- Autenticación de usuario y terminal: los proveedores de servicio VoIP necesitan saber quién los utiliza a fin de poder contabilizar correctamente la utilización y tal vez cobrar por ella. Antes de poder autenticar, se ha de identificar al usuario y/o terminal mediante algún tipo de identidad, tras lo cual éste debe probar que la identidad reclamada es la verdadera. En general, esto se hace mediante procesos robustos de autenticación criptográfica (por ejemplo, contraseña protegida o firma digital X.509). De igual manera, es probable que los usuarios deseen saber con quién se están comunicando.

- Autenticación de servidor: En general, los usuarios VoIP se comunican entre ellos a través de alguna infraestructura de VoIP que involucra servidores (controladores de acceso, unidades multidifusión, pasarelas) por lo que les interesa saber si se están comunicando con el servidor y/o el proveedor de servicio correctos. Ese aspecto incumbe tanto a usuarios fijos como móviles.

- Amenazas contra la seguridad de autenticación de usuario/terminal y servidor, tales como la usurpación de identidad, el intermediario, la simulación de dirección IP y el pirataje de la conexión.

- La autorización de llamada, que consiste en el proceso de toma de decisiones tendiente a establecer si se permite al usuario/terminal utilizar los recursos de servicio, tales como una característica de servicio (por ejemplo, una llamada en la RTPC) o los recursos de red (QoS, ancho de banda, códec, etc.). Suele ocurrir que las funciones de autenticación y autorización se utilicen conjuntamente para tomar una decisión de control de acceso. Gracias a la autenticación y a la autorización es posible contrarrestar ataques del tipo usurpación de identidad, mala utilización y fraude, manipulación y negación de servicio.

- La protección de la seguridad de señalización se refiere a evitar la manipulación, uso inadecuado, ataque a la confidencialidad y privacidad de los protocolos de señalización. En general, estos protocolos se protegen mediante métodos criptográficos, utilizando el criptado así como la protección de integridad y reproducción. Conviene prestar atención particular al cumplimiento de los requisitos críticos de calidad de funcionamiento de las comunicaciones en tiempo real utilizando pocos eventos de toma de contacto y atajos para evitar tiempos de establecimiento de llamada demasiado largos o que se degrade la calidad vocal debido a retrasos de paquetes o a fluctuación de fase causada por el procesamiento de seguridad.

- Se logra la confidencialidad en las transmisiones vocales mediante la criptación de los paquetes de voz; es decir, las cabidas útiles RTP y contrarrestando la intromisión de piratas en los datos vocales. En general, también se encriptan los paquetes de medios (por ejemplo vídeo) de las aplicaciones multimedios. Otros tipos de protección avanzada de los paquetes de medios incluyen la protección de autenticación e integridad de las cabidas útiles.

- La gestión de claves no solo incluye todas las tareas necesarias para distribuirlas con seguridad entre las diferentes partes hacia los usuarios y servidores, sino también otras como la actualización de claves que han expirado o de claves perdidas. Es probable que la gestión de claves sea independiente de la aplicación VoIP (configuración de la contraseña) o también puede ocurrir que se haga conjuntamente con la señalización cuando se negocian dinámicamente perfiles de seguridad con capacidades de seguridad y se distribuyen claves basadas en sesión conjuntamente.

- La seguridad entre dominios tiene que ver con el problema que suele presentarse cuando los sistemas de entorno heterogéneo han implementado características diferentes de seguridad, ya sea debido a requisitos, políticas de seguridad y capacidades de seguridad diferentes. Siendo así, se han de negociar dinámicamente los perfiles y capacidades de seguridad, tales como los algoritmos de criptografía y sus parámetros. Este aspecto es particularmente importante cuando se trata de pasar entre fronteras de dominios y se cuenta con diversos proveedores y redes. La capacidad de atravesar sin problemas los cortafuegos y acomodarse a las restricciones de los dispositivos de traducción de dirección de red (NAT) es un requisito muy importante de seguridad en las comunicaciones entre dominios.

Si bien esta lista no es extensiva, sí constituye el núcleo de la seguridad H.323. No obstante, en la práctica suele ocurrir que haya aspectos de seguridad fuera del alcance de H.323 (por ejemplo, política de seguridad, seguridad de gestión de red, suministro de la seguridad, seguridad de la implementación, seguridad operacional o seguridad en el manejo de incidentes).

6.1.2 Cómo se obtiene la seguridad en la VoIP

En un sistema multimedios H.323, la Rec. UIT-T H.235 define el marco de seguridad incluida la especificación de los mecanismos y protocolos de seguridad para H.323. La primera aplicación de la Rec. UIT-T H.235 se dio en 1998 para los sistemas de la versión 2 de H.323. Desde entonces, H.235 ha evolucionado hasta llegar a consolidar los mecanismos de seguridad ofrecidos, adicionando algoritmos de seguridad más sofisticados (por ejemplo, criptado AES de alta seguridad y alta velocidad) y desarrollando perfiles de seguridad más útiles y eficaces para determinados entornos y casos. Actualmente, la versión 3 de H.235 es la Recomendación UIT-T de seguridad para los sistemas basados en H.323, y gracias a ella se proporciona seguridad escalable que va desde pequeños grupos hasta empresas enteras y operadores de gran tamaño.

En resumen, H.235 suministra la protección criptográfica de los protocolos de control (RAS y señalización de llamada de H.225.0 y H.245), así como de los datos de trenes de medios de audio/vídeo. La Rec. UIT-T H.235 suministra maneras de negociar, a través de las diversas etapas de la señalización H.323, los servicios criptográficos deseados y requeridos, los algoritmos de criptografía y las capacidades de seguridad. Las funciones de gestión de claves necesarias para establecer claves de sesiones dinámicas se integran completamente en las tomas de contacto de señalización y, por ende, es posible reducir el tiempo de latencia del establecimiento de llamada. A la vez que la gestión de clave H.235 permite soportar la comunicación punto a punto (clásica), también lo hace con las configuraciones multipunto gracias a las unidades de multidifusión (MCU), siempre que se comuniquen varias terminales multimedios dentro de un grupo.

Las medidas de seguridad H.235 cubren una amplia gama que va desde entornos objetivos tan diferentes como aquéllos entre empresas y al interior de ellas y los de operadores de telecomunicaciones. Dependiendo del tipo de hipótesis, tales como la infraestructura de seguridad y capacidades de terminal y plataforma disponibles (puntos extremos simples o inteligentes), la Rec. UIT-T H.235 ofrece una importante variedad de perfiles de seguridad interoperables adaptados a cada caso. Estos perfiles de seguridad pueden ir desde los de simple secreto compartido, incluida la contraseña protegida (anexo D/H.235 para la autenticación e integridad de mensaje) hasta los más sofisticados que contienen firmas digitales y certificados PKI X.509 (anexos E y F/H.235). De esta manera, se permite que haya protección salto por salto utilizando técnicas más simples pero menos escalables o bien extremo a extremo utilizando técnicas PKI escalables. En el anexo I/H.235 se disminuye la dependencia estricta que hay en una arquitectura encaminada por controlador de acceso y centrada en el servidor y se proporcionan medidas de seguridad que facilitan asegurar un modelo entre pares.

La Rec. UIT-T H.235 utiliza técnicas especiales de seguridad optimizada como la criptografía de curva elíptica y el criptado más moderno de tipo AES, a fin de cumplir con los requisitos rigurosos de calidad de funcionamiento. De haber criptación vocal, ésta se efectúa en la capa de aplicación mediante el criptado de las cabidas útiles RTP, permitiendo así una implementación más benéfica que tiene menores huellas en los puntos extremos gracias a una interacción más intensa con el procesador de señal digital (DSP, *digital signal processor*) y los códecs de compresión vocal, además de no depender de una plataforma específica de sistema operativo. Siempre que los haya y sea recomendable, se pueden (re)utilizar en el contexto de H.235 las herramientas de seguridad existentes, como por ejemplo los paquetes y normas de seguridad de Internet disponibles (IPSec, SSL/TLS).

En la figura 10 se muestra el alcance de la Rec. UIT-T H.235, que va desde las disposiciones para el establecimiento de llamadas (bloques H.225.0 y H.245) y la comunicación bidireccional (criptado de cabidas útiles RTP que contienen audio y/o vídeo comprimido). Las funcionalidades incluyen mecanismos para autenticación, integridad, privacidad y no repudio. Los controladores de acceso se encargan de la autenticación mediante un control de admisión en los puntos extremo, y de suministrar mecanismos de no repudio. Aunque la seguridad de la capa de transporte y capas inferiores, basadas en el IP, está fuera del alcance de las Recomendaciones UIT-T H.323 y H.235, suele implementarse utilizando los protocolos de seguridad IP (IPSec) y de seguridad de capa de transporte (TLS) del IETF. En general, estos dos protocolos se pueden utilizar con fines de autenticación y, facultativamente, confidencialidad (es decir criptado) en la capa IP, de una manera transparente cualquier protocolo (aplicación) que esté funcionando por encima de ella. Para esto, no es necesario actualizar el protocolo de aplicación sino que basta con hacerlo en la política de seguridad de cada extremo.

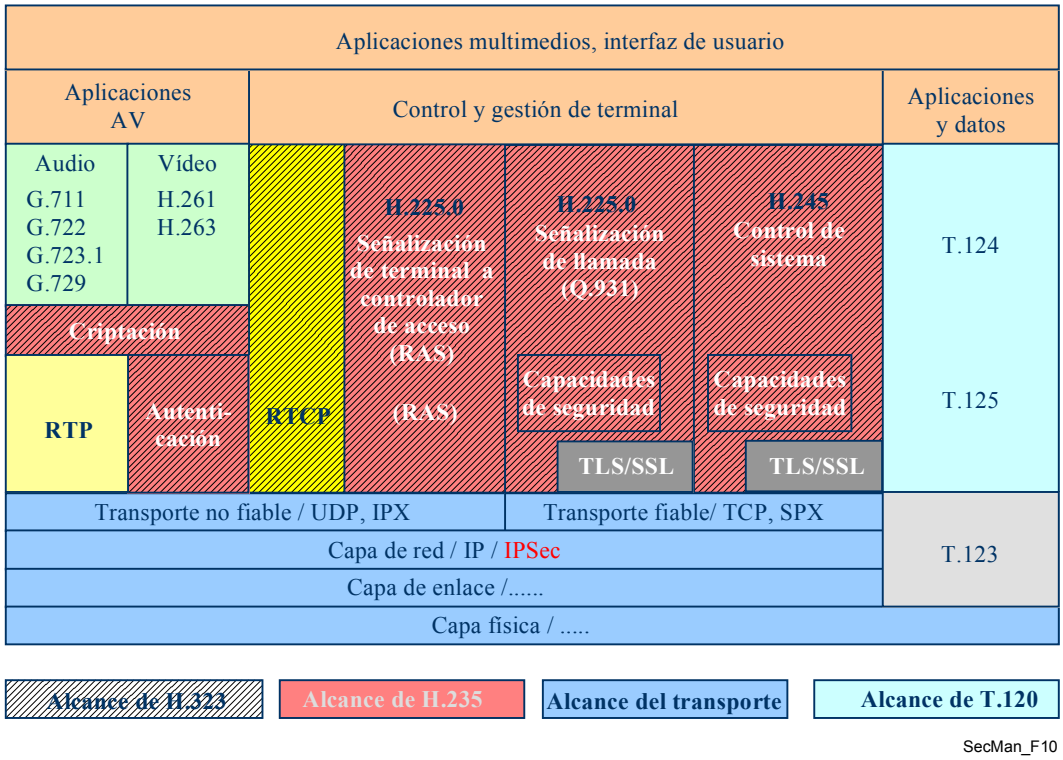


Figura 10
Seguridad en los sistemas H.323 proporcionada por H.235 [Euchner]

Si bien en la Rec. UIT-T H.235 se tratan en particular los entornos H.323 "estáticos" solamente con prestaciones limitadas de movilidad, se acepta que es necesario proveer movilidad segura de usuario y terminal en los entornos distribuidos H.323, más allá de la interconexión entre dominios y la movilidad de zona de controlador de acceso limitada. Estas necesidades de seguridad se tratan en la Rec. UIT-T H.530 mediante el estudio de aspectos de seguridad como por ejemplo:

- Autenticación y autorización de terminal/usuario móvil en los dominios visitados.
- Autenticación de dominio visitado.
- Gestión de clave segura.
- Protección de los datos de señalización entre un terminal móvil y un dominio visitado.

Además de las disposiciones consignadas en H.235, las Recomendaciones UIT-T H.350 y H.350.2 permiten la gestión escalable de clave utilizando LDAP y SSL3. En la serie de Recomendaciones UIT-T H.350.x se incluyen capacidades importantes que permiten a las empresas y los operadores gestionar con seguridad un gran número de usuarios de servicios de vídeo y voz por IP. En la Rec. UIT-T H.350 hay un método para conectar H.323, SIP, H.320 y servicios de mensajería genéricos en un servicio directorio, de tal manera que se puedan aplicar prácticas modernas de gestión de identidad a las comunicaciones multimedios. Más aún, gracias a esta arquitectura se cuenta con un lugar normalizado para almacenar las credenciales de seguridad de estos protocolos.

La Rec. UIT-T H.350 no modifica las arquitecturas de seguridad de ningún protocolo particular. No obstante, ofrece un lugar normalizado para almacenar las credenciales de autenticación (cuando proceda). Cabe observar que tanto H.323 como SIP soportan la autenticación de secreto compartido (anexo D/H.235 HTTP Digest, respectivamente). En estos enfoques es necesario que el servidor de llamada tenga acceso a las contraseñas, es decir, de haber una amenaza para el servidor de llamada o el directorio H.350 también la hay para las contraseñas. Esta debilidad se debe probablemente más a una debilidad en los sistemas (directorio H.350 o servidores de llamada) y a su operación más que a la propia H.350.

Se recomienda enfáticamente que los servidores de llamada y el directorio H.350 se autentiquen mutuamente antes de compartir cualquier información. Además, es muy conveniente que las comunicaciones entre los directorios H.350 y los servidores de llamada o puntos extremos se establezcan a través de canales de comunicación seguros, como por ejemplo, SSL o TLS.

Cabe observar que las listas de control de acceso en los servidores LDAP son un asunto de política y no forman parte de la norma. Se recomienda a los administradores de sistema utilizar el sentido común cuando fijen el control de acceso en los atributos H.350. Por ejemplo, es necesario que solamente un usuario autenticado pueda acceder a los atributos de contraseña, mientras que los de dirección pueden ser públicos.

6.2 Sistema IPCablecom

Este sistema permite a los operadores de televisión por cable prestar servicios basados en el IP en tiempo real (por ejemplo, comunicaciones vocales) por sus redes ampliadas para soportar módems de cable. En la Rec. UIT-T J.160 se define la arquitectura del sistema IPCablecom. A un muy alto nivel, esta arquitectura tiene en cuenta tres redes: la "red de acceso HFC J.112", la "red IP gestionada" y la RTPC. El nodo de acceso (AN) permite la conectividad entre la primera y la segunda de dichas redes. Tanto la pasarela de señalización (SG) como la de medios (MG) hacen posible la conectividad entre "la red IP gestionada" y la RTPC. En la figura 11 se muestra la arquitectura de referencia de IPCablecom.

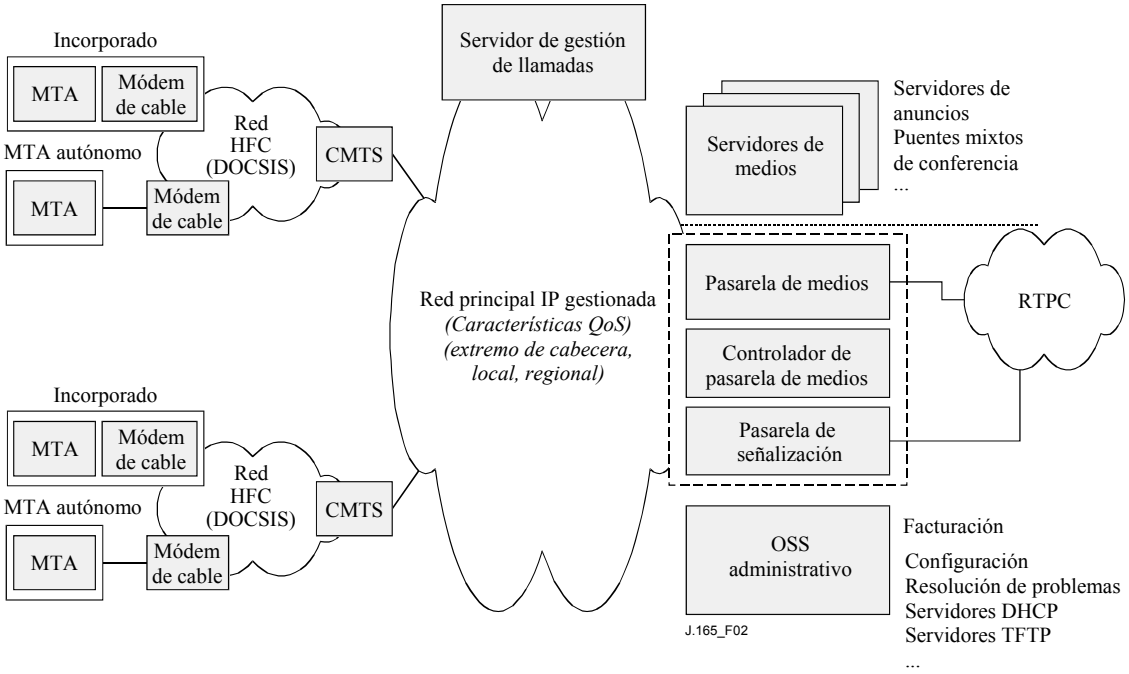


Figura 11
Arquitectura de referencia IPCablecom [J.165]

En la red de acceso que utiliza el sistema híbrido de fibra óptica/cable coaxial (HFC) que se especifica en J.112 se proporciona transporte de datos de alta velocidad, fiable y seguro entre los locales del cliente y el extremo de cabecera del cable. Esta red de acceso también puede suministrar todas las capacidades J.112, incluida la calidad de servicio, así como las interfaces con la capa física a través de un sistema de terminación de módem de cable (CMTS).

La red IP gestionada cumple con diversas funciones. En primer lugar, proporciona interconexión entre las componentes funcionales básicas de IPCablecom que se encargan del establecimiento de señalización, medios, prestación de servicio y calidad de éste. Además, permite la conectividad IP a grandes distancias entre otras redes IP gestionadas y HFC J.112. La red IP gestionada cuenta con las siguientes componentes funcionales: servidor de gestión de llamadas, servidor de anuncios, pasarela de señalización, pasarela de medios, controlador de pasarelas de medios, y varios servidores administrativos del sistema de soporte de operaciones (OSS).

El *servidor de gestión de llamadas* (CMS) proporciona el control de llamada y los servicios relativos a la señalización para el adaptador de terminal de medios (MTA), el nodo de acceso, y las pasarelas RTPC en la red IPCablecom. El CMS es un elemento de red de confianza que se encuentra en la porción IP gestionada de la red IPCablecom. Los *servidores de anuncios* son componentes lógicos de red que gestionan y reproducen tonos y mensajes de información como respuesta a eventos que ocurren en la red. La función *pasarela de señalización* envía y recibe señalización de red con conmutación de circuitos en la frontera de la red IPCablecom. Para estas últimas redes, dicha función sólo soporta señalización no asociada con la facilidad, en la forma de SS7 (señalización asociada con la facilidad, del tipo tonos de multifrecuencia que se soporta directamente mediante la función pasarela). El *controlador de pasarela de medios* (MGC) recibe y tramita la información de señalización de llamada entre la red IPCablecom y la RTPC. Mantiene y controla el estado general de todas las llamadas que requieran interconexión RTPC. La *pasarela de medios* (MG) suministra conectividad de portador entre la red RTPC y la red IPCablecom. Cada portador se representa aquí

como un punto extremo, y el MGC ordena a la MG establecer y controlar conexiones de medios hacia los otros puntos extremos en la red IPCablecom. Asimismo, el MGC ordena a la MG detectar y generar eventos y señales relativas al estado de llamada que él conoce. El *Sistema Administrativo OSS* tiene componentes de índole comercial, de servicios y de gestión de red que soportan todos los procesos comerciales principales. Las áreas funcionales más importantes del OSS son: gestión de fallos, gestión de calidad de funcionamiento, gestión de seguridad, gestión de contabilidad, y gestión de configuración. En IPCablecom se define un conjunto limitado de componentes funcionales e interfaces de OSS a fin de soportar la preparación de dispositivos MTA y la mensajería de eventos que transportan información de facturación.

6.2.1 Aspectos de seguridad IPCablecom

Toda interfaz de protocolo IPCablecom está sujeta a amenazas que comprometen la seguridad tanto del abonado como del proveedor de servicio. Por ejemplo, el trayecto del tren de medios puede pasar a través de un gran número de posibles servicios Internet y de enlaces de proveedores de servicio troncal desconocidos, provocando que pueda ser vulnerable a escuchas clandestinas malintencionadas que resulten en una pérdida de privacidad en la comunicación.

6.2.2 Mecanismos de seguridad de IPCablecom

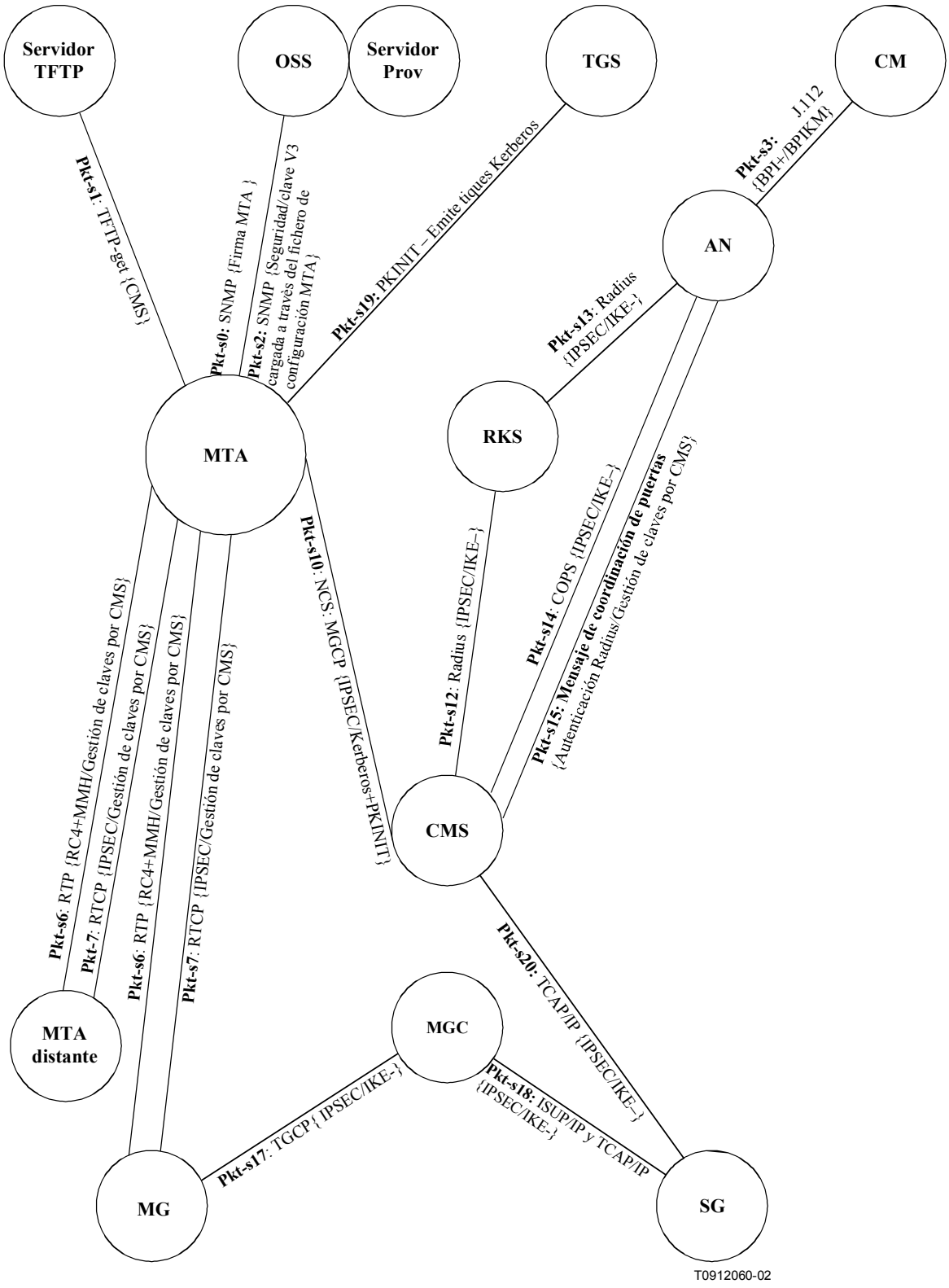
La seguridad de IPCablecom se implementa en los elementos de la pila de protocolos inferior y, por ende, utiliza especialmente mecanismos definidos por el IETF. En la arquitectura IPCablecom se consideran las amenazas especificando, para cada interfaz de protocolo definida, el mecanismo de seguridad subyacente (como por ejemplo IPsec) que proporciona la interfaz de protocolo con los servicios de seguridad requeridos. Con arreglo a la arquitectura X.805, los servicios de seguridad para la IPCablecom tienen en cuenta los nueve componentes resultantes de la matriz tres por tres de planos y capas de la figura 1. Por ejemplo, el IPSec soporta los servicios de los protocolos de señalización del plano de control, mientras que gracias a la utilización de SNMP v3 es posible lograr la seguridad de la infraestructura de gestión.

En la capa de servicio principal de IPCablecom se encuentran disponibles diversos servicios de seguridad, a saber autenticación, control de acceso, integridad, confidencialidad y no repudio. Una interfaz de protocolo IPCablecom puede utilizar o no estos servicios con el fin de suplir sus necesidades particulares de seguridad.

En IPCablecom se tratan los aspectos de seguridad de cada interfaz de protocolo constitutiva de la siguiente manera:

- identificando el modelo de amenaza específica a cada interfaz de protocolo constitutiva;
- identificando los servicios de seguridad (autenticación, autorización, confidencialidad, integridad y no repudio) necesarios para enfrentar las amenazas identificadas;
- especificando el mecanismo de seguridad particular que proporcionan los servicios de seguridad requeridos.

Los mecanismos de seguridad incluyen tanto el protocolo de seguridad (por ejemplo IPsec, seguridad de capa RTP y seguridad SNMPv3) como el protocolo de soporte de gestión de clave (por ejemplo IKE, PKINIT/Kerberos). Asimismo, el núcleo de seguridad IPCablecom contiene un mecanismo que permite la criptación extremo a extremo de los trenes de medios RTP, reduciendo así sustancialmente la posibilidad de una amenaza a la privacidad. En la figura 12 se muestra un resumen de todas las interfaces de seguridad IPCablecom. Cuando no se haya incluido el protocolo de gestión de clave, quiere decir que no se necesita para dicha interfaz. Se omiten las interfaces IPCablecom que no necesitan seguridad.



IKE –	IKE con claves compartidas
IKE+	El IKE requiere certificados de clave pública
Gestión de claves por CMS	El CMS genera y distribuye la claves aleatoriamente

Figure 12
Interfaces de seguridad IPCablecom (etiquetadas como <label>: <protocol> { <security protocol> / <key management protocol> })

La arquitectura de seguridad IPCablecom divide la configuración de equipos en tres actividades distintas: la inscripción de abonado, la configuración y la autorización de equipo. El proceso de *inscripción de abonado* permite establecer una cuenta de facturación permanente de usuario que identifica unívocamente el MTA ante el CMS a través del número de serie del MTA o la dirección MAC. La cuenta de facturación se utiliza también para identificar los servicios a los que se ha abonado el usuario para el MTA. Este proceso de inscripción puede darse en banda o fuera de banda. Su especificación precisa está fuera del alcance de IPCablecom y puede variar según cada proveedor de servicio. En el caso de la *configuración de equipo*, el MTA verifica la autenticidad del archivo de configuración que ha telecargado estableciendo en primer lugar la seguridad SNMPv3 (utilizando la autenticación basada en Kerberos y la gestión de clave) entre sí mismo y el servidor de configuración. Este último proporciona entonces al MTA la ubicación del fichero de configuración, y una versión de dicho fichero al que se le ha aplicado la función hash. El MTA recupera dicho fichero, le aplica la función hash, y compara el resultado con la función hash suministrada por el servidor de configuración. De coincidir ambas funciones se autentica el fichero de configuración. Es posible también, si se quiere, criptar dicho fichero a efectos de privacidad (se debe entonces habilitar la privacidad de SNMPv3 a fin de hacer pasar con seguridad la clave de criptación de archivo de configuración al MTA). La *autorización de equipo* ocurre cuando un equipo MTA configurado se autentica a sí mismo ante el servidor de gestión de llamada, y establece una asociación de seguridad con ese servidor antes de entrar completamente en funcionamiento. La autorización de equipo permite que se proteja la señalización de llamada subsiguiente a través de la asociación de seguridad establecida.

Es posible proteger tanto el tráfico de señalización como los trenes de medios. El primero de ellos, que incluye señalización QoS, señalización de llamada, y señalización con la interfaz de pasarela RTPC, se asegurará a través del IPsec. La gestión de asociación de seguridad IPsec se efectúa mediante la utilización de dos protocolos de gestión de clave, a saber Kerberos/PKINIT e IKE. El primero de éstos se utilizará para intercambiar claves entre los clientes MTA y su servidor CMS; mientras que el otro se emplea para gestionar el resto de señalización de las SA IPsec. En lo que respecta a los trenes de medios, cada paquete RTP de medios se cripta a fin de obtener privacidad y se autentica para verificar la integridad y su origen. Los MTA han de ser capaces de negociar el algoritmo de criptado particular, aunque en realidad el único requerido es el AES. Puede ocurrir que cada paquete RTP incluya un código opcional de autenticación de mensaje (MAC). Si bien es posible negociar el algoritmo MAC, el único del que se dispone actualmente es el MMH. El cálculo que utiliza el MAC se aplica desde el encabezamiento no criptado de los paquetes hasta la cabida útil criptada.

Las claves para la criptación y para el cálculo MAC se obtienen a partir del secreto extremo a extremo y del relleno facultativo, que son intercambiados entre los MTA de origen y destino como parte de la señalización de llamada, tras lo cual, los intercambios de clave para seguridad de trenes de medios se aseguran a sí mismos mediante la seguridad de señalización de llamada.

Hay también seguridad para el OSS y el sistema de facturación. Los agentes SNMP de los equipos IPCablecom implementan SNMPv3. El modelo de seguridad de usuario SNMPv3 [RFC 2274] proporciona servicios de autenticación y privacidad para el tráfico SNMP. Se puede utilizar el control de acceso basado en vistas SNMPv3 [RFC 2275] para efectuar el control de acceso a los objetos MIB.

El protocolo de gestión de clave IKE se utiliza para establecer claves de criptación y autenticación entre el servidor de mantenimiento de registros (RKS) y cada elemento de red IPCablecom que genera mensajes Evento. Una vez establecidas las asociaciones de seguridad IPsec de red, se tienen que crear las claves entre cada RKS (primario, secundario, etc.) y todo CMS y AN. Puede ocurrir que haya un intercambio de claves entre el MGC y el RKS, lo que se deja a la implementación particular de cada fabricante en la fase 1 IPCablecom. Los mensajes Evento se envían desde el CMS y el AN hacia el RKS utilizando el protocolo de transporte RADIUS, que a su vez obtiene la seguridad a través del IPsec.

6.3 Transmisión segura por fax

El facsímil es una aplicación muy popular, que se definió inicialmente para la transmisión por la RTPC (Rec. UIT-T T.4), luego para la RDSI (Rec. UIT-T T.6), y más recientemente se ha extendido para el transporte por las redes IP (incluida la red Internet) para la transmisión en tiempo no real (retransmisión de correo electrónico) utilizando la Rec. UIT-T T.37 y para el tiempo real (utilizando RTP) conforme a la T.38. La transmisión por fax debe, en general, hacer frente a dos aspectos básicos de seguridad, sin importar si se trata de RTPC, RDSI, o IP, como son la autenticación (y algunas veces el no repudio) de una conexión, y la confidencialidad de los datos transmitidos. En las Recomendaciones UIT-T T.37 y T.38 estos aspectos han adquirido aún más relevancia debido a la naturaleza distribuida de la red IP.

En la Rec. UIT-T T.36 se definen dos soluciones técnicas independientes que pueden ser utilizadas en el contexto de la transmisión segura de fax para la criptación de los documentos. Ambas se basan en los algoritmos HKM/HFX40 (anexo A/T.36) y RSA (anexo B/T.36). Aunque en ambos se limitan las claves de sesión a 40 bits (debido a reglamentos nacionales en el momento de aprobación de la Recomendación, 1997), se especifica un mecanismo útil para generar una clave de sesión redundante (a partir de una clave de sesión de 40 bits) para los algoritmos que requieran claves más largas. En el anexo C/T.36 se describe la utilización del sistema HKM para suministrar capacidades de gestión de clave segura en los terminales de facsímil mediante el registro unidireccional entre entidades X e Y, o para la transmisión segura de una clave secreta entre las entidades X e Y. En el anexo D/T.36 se tratan los procedimientos necesarios para la utilización del sistema de cifrado HFX40 a fin de lograr la confidencialidad de mensajes en terminales facsímil. Finalmente, en el anexo E se describe el algoritmo hashing HFX40-I, en términos de su utilización, los cálculos necesarios y la información que se ha de intercambiar entre los terminales facsímil para garantizar la integridad de un mensaje facsímil transmitido bien sea como alternativa escogida o preprogramada para la criptación de dicho mensaje.

En la Rec. UIT-T T.36 se definen también los siguientes servicios de seguridad:

- Autenticación mutua (obligatoria).
- Servicio de seguridad (facultativa), que incluye autenticación mutua, integridad de mensaje y confirmación de recepción de mensaje.
- Servicio de seguridad (facultativo), que incluye autenticación mutua, confidencialidad de mensaje (criptado), y establecimiento de clave de sesión.
- Servicio de seguridad (facultativo), que incluye autenticación mutua, integridad de mensaje, confirmación de recepción de mensaje, confidencialidad de mensaje (criptado), y establecimiento de clave de sesión.

Se definen cuatro perfiles de servicio basándose en los anteriores servicios de seguridad, tal como se muestra en el cuadro 2 a continuación.

Cuadro 2
Perfiles de seguridad del anexo H/T.30

Servicios de seguridad	Perfiles de servicio			
	1	2	3	4
Autenticación mutua	X	X	X	X
• Integridad del mensaje • Confirmación de recepción del mensaje		X		X
• Confidencialidad del mensaje (criptación) • Establecimiento de clave de sesión			X	X

6.3.1 Seguridad en transmisiones de facsímil con HKM y HFX

Al combinar los sistemas de *gestión de clave Hawthorne* (HKM) y *cifrado de facsímil Hawthorne* (HFX) se obtienen las siguientes capacidades para las comunicaciones seguras de documentos entre entidades (terminales u operadores de terminales):

- autenticación de entidades mutuas;
- establecimiento de clave de sesión secreta;
- confidencialidad de documento;
- confirmación de recibo;
- confirmación de negación de integridad de documento.

El sistema HKM definido en el anexo B/T.36 permite lograr la gestión de clave. Se definen dos procesos: el registro (o inscripción) y la transmisión segura de una clave secreta. El registro permite establecer claves secretas mutuas y efectuar las transmisiones subsiguientes con seguridad, pues el sistema HKM proporciona autenticación mutua, una clave secreta de sesión para confidencialidad e integridad de documento, confirmación de recepción y confirmación o negación de integridad de documento.

La confidencialidad de documento se obtiene a través del sistema de cifrado que se define en el anexo D/T.36. Este cifrado utiliza una clave digital de 12 cifras, que es aproximadamente igual a una clave de sesión de 40 bit.

La integridad de documento se obtiene mediante el sistema definido en el anexo E/T.36, en la que se define el algoritmo hashing (de troceo) incluidos los cálculos e intercambio de información correspondientes.

En el modo de registro, ambos terminales intercambian información permitiendo a las entidades identificarse entre ellas unívocamente. Todo esto se basa en una clave secreta de un solo uso entre los usuarios. Cada entidad almacena un número de 16 cifras que se asocia unívocamente con la entidad con la cual haya efectuado el registro.

De ser necesario enviar un documento con seguridad, la terminal que transmite envía el número secreto de 16 cifras asociado con la entidad receptora junto con un número aleatorio y una clave de sesión criptada, solicitando identificación a la entidad receptora. Esta última responde transmitiendo la clave de 16 cifras asociada con la entidad transmisora junto con un número aleatorio y una versión recriptada de la petición de identidad de esta última entidad. Al mismo tiempo, envía un número aleatorio y una clave de sesión criptada como petición de identidad a la entidad transmisora. Esta última responde con un número aleatorio y una versión recriptada de la petición de la entidad receptora. De esta manera, se permite a ambas entidades autenticarse mutuamente. Al mismo tiempo, el terminal transmisor envía un número aleatorio y la clave de sesión criptada que ha de utilizarse en la criptación y la función hashing.

Tras haber transmitido el documento, el terminal transmisor envía un número aleatorio y una clave de sesión criptada solicitando la identidad de la entidad receptora. Al mismo tiempo, transmite un número aleatorio y un valor hash criptado, lo que permite a la entidad receptora garantizar la integridad del documento recibido y, entonces, transmitir un número aleatorio y una versión recriptada de la petición de identificación proveniente de la entidad de transmisión, mientras envía un número aleatorio y un Documento de Integridad criptado que actúa como confirmación o negación de la integridad del documento recibido. El algoritmo hashing que se ha utilizado para la integridad de documento se transporta en el cuerpo de éste.

Existe también un modo anulación, en el que no se intercambia ninguna señal de seguridad entre los dos terminales. En él, los usuarios se ponen de acuerdo en una clave secreta de un solo uso que ha de producirse manualmente y que será utilizada por el terminal transmisor para criptar el documento y por el terminal receptor para decriptarlo.

6.3.2 Seguridad de facsímil con RSA

En el anexo H/T.30 se especifican los mecanismos necesarios para poder ofrecer características de seguridad basándose en el mecanismo criptográfico de *Rivest, Shamir & Adleman* (RSA). En la referencia [ApplCryp, pp.466-474] se pueden encontrar más detalles acerca de dicho algoritmo. El esquema de codificación del documento transmitido con características de seguridad puede ser cualesquiera de los definidos en las Recomendaciones UIT-T T.4 y T.30 (Huffman modificado, MR, MMR, Modo carácter como se define en el anexo D/T.4, BFT, o cualquier modo de transferencia de ficheros definido en el anexo C/T.4).

El algoritmo básico que se utiliza para la firma digital (servicios del tipo de autenticación e integridad) es el RSA que utiliza un par "clave pública"/"clave secreta".

Siempre que se ofrezca el servicio facultativo de confidencialidad, también se encripta el testigo que contiene la clave de sesión "Ks", utilizado para el cifrado del documento, mediante el algoritmo RSA. El par de claves que se utiliza a estos fines, llamado "clave pública de cifrado"/"clave secreta de cifrado", es diferente del que se usa para los servicios de tipos de autenticación e integridad. De esta manera se separan los dos tipos de utilización.

En la norma ISO/CEI 9796 (*Digital signature scheme giving message recovery*) se describe la implementación de RSA que se utiliza en el anexo H.

A fin de cifrar el testigo que contiene la clave de sesión, al procesar el algoritmo RSA se utilizan las mismas reglas de redundancia que las que aparecen especificadas en la norma ISO/CEI 9796. Cabe observar que algunas administraciones pueden solicitar que se implemente el mecanismo de *algoritmo de firma digital* (DSA) [ApplCryp, pp-483-502] además del RSA.

Aunque en principio no se utilicen por defecto las *autoridades de certificación* en el modelo del anexo H/T.30, puede ocurrir que se utilicen para validar la clave pública del remitente del mensaje facsímil, en cuyo caso se puede certificar la clave pública con arreglo a la Rec. UIT-T X.509. Si bien en el anexo H se describen los medios para transmitir el certificado de clave pública del remitente, el formato preciso de éste se deja para estudio ulterior y la transmisión real se negocia en el protocolo.

Se proporciona un *modo de registro*, que es una característica obligatoria. Este modo permite al emisor y al receptor registrar y almacenar confidencialmente las claves públicas de la contraparte antes de cualquier comunicación facsímil segura entre los dos. Gracias a este modo se puede evitar que el usuario tenga que introducir manualmente en el terminal las claves públicas de sus contrapartes (pues son bastante largas, del orden de 64 octetos o más).

Puesto que el modo de registro permite intercambiar las claves públicas y almacenarlas en los terminales, no es necesario transmitirlas durante las comunicaciones de facsímil.

Como se describe en dicho anexo, algunas firmas se aplican al resultado de una función "hash".

Se pueden utilizar dos tipos de funciones hash, a saber el algoritmo SHA-1, que proviene del NIST (*National Institute of Standards and Technology*) en Estados Unidos, o el MD-5 (RFC 1321). En el primero de ellos la longitud del resultado del proceso tiene 160 bits, mientras que en la segunda tiene 128. Un terminal conforme al anexo H/T.30 puede implementar cualquiera de los dos, o ambos. El uso de determinado algoritmo se negocia en el protocolo (véase más adelante).

El cifrado de los datos a fin de garantizar el servicio de confidencialidad es facultativo. En el alcance del anexo H/T.30 se describen cinco esquemas de cifrado facultativos: FEAL-32, SAFER K-64, RC5, IDEA y HFX40 (que se describe en la Rec. UIT-T T.36). Es posible que en algunos países su utilización esté sujeta a reglamentación nacional.

De igual manera, se pueden utilizar otros algoritmos facultativos, que se escogen con arreglo a la norma ISO/CEI 9979 (Procedimiento para el registro de algoritmos criptográficos).

En el protocolo se negocia la capacidad del terminal para utilizar uno de estos algoritmos y la utilización propiamente dicha de éste durante la comunicación. Se utiliza una clave de sesión para el cifrado, cuya longitud básica es 40 bits. Cuando se trate de algoritmos que utilizan esta longitud básica (por ejemplo HFX40), la clave de sesión "Ks" es en realidad la que se utiliza en el algoritmo de cifrado, mientras que para aquellos que requieren claves mayores que 40 bits (por ejemplo FEAL-32, IDEA, SAFER K-64 que requieren respectivamente 64, 128 y 64 bits), se ejecuta un mecanismo de redundancia a fin de obtener la longitud necesaria. La clave así obtenida se denomina "clave de sesión redundante", que es la realmente utilizada en el algoritmo de cifrado.

6.4 Aplicaciones de gestión de red

Tal como se menciona en la cláusula relativa a los requisitos para el marco de seguridad, es imperativo asegurar el tráfico de gestión que se utiliza para supervisar y controlar la red de telecomunicaciones. Dicho tráfico se puede catalogar en diferentes categorías conforme a la información necesaria para ejecutar las funciones de gestión de fallos, configuración, calidad de funcionamiento, contabilidad y seguridad. Por gestión de seguridad se entiende tanto el establecimiento de una red de gestión segura como la gestión de la seguridad de la información relacionada con los tres planos y capas de seguridad de la arquitectura correspondiente. En esta subcláusula se describe la segunda de ellas.

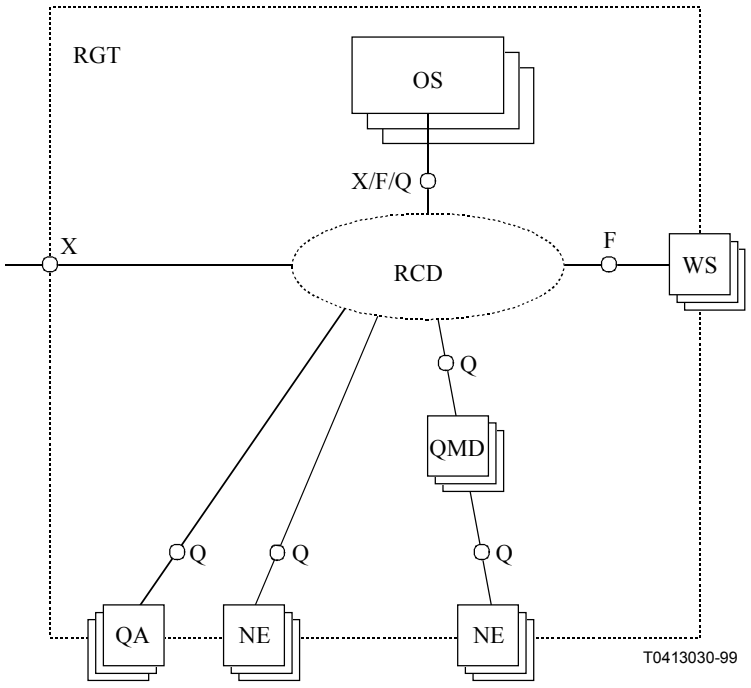
En las redes tradicionales de telecomunicaciones se suele transmitir el tráfico de gestión en una red separada que transporta solamente tráfico de gestión de red y no de usuario. Con frecuencia se conoce esta red como la red de gestión de telecomunicaciones (TMN), que se describe en la Rec. UIT-T M.3010. La TMN se separa y aísla de la infraestructura de red pública, de tal manera que no se contamine de problemas relativos a interrupciones debidas a amenazas contra la seguridad en el plano de usuario de la red pública. Siendo así, es relativamente fácil garantizar la seguridad del tráfico de red de gestión puesto que el acceso a este plano está restringido a los administradores de red autorizados, y el tráfico a actividades válidas de gestión. Tras la introducción de las redes de próxima generación, puede ocurrir que en algunos casos el tráfico para las aplicaciones de usuario extremo se combine con el de gestión. Si bien esta característica minimiza los costos al requerir de una sola infraestructura de red integrada, introduce muchos nuevos desafíos a la seguridad, puesto que las amenazas que se presenten en el plano de usuario lo son también ahora para los planos de control y gestión. El plano de gestión deviene ahora accesible a muchos usuarios extremos, y múltiples variedades de actividades maliciosas son ahora posibles.

Para lograr una solución completa extremo a extremo, conviene aplicar todas las medidas de seguridad (por ejemplo control de acceso, autenticación) a cada tipo de actividad de red (es decir, actividades del plano de gestión, del plano de control y del plano de usuario extremo) para la infraestructura, los servicios y las aplicaciones de red. Existen varias Recomendaciones UIT-T que se centran particularmente en el aspecto de seguridad del plano de gestión para elementos de red (NE) y sistemas de gestión (MS) que forman parte de la infraestructura de red.

Aunque existen muchas normas, como se describe a continuación, para garantizar la seguridad de la información de gestión que se requiere para el mantenimiento de la infraestructura de telecomunicaciones, también hay que considerar que dentro del término gestión de red se deben tener en cuenta los entornos en los que los diversos proveedores de servicios deben interactuar para poder ofrecer servicios de extremo a extremo como por ejemplo líneas arrendadas a los clientes que atraviesen fronteras geográficas, o a las instituciones gubernamentales o de regulación para soportar la recuperación en caso de desastre.

6.4.1 Arquitectura de gestión de red

La arquitectura necesaria para definir la gestión de red de una red de telecomunicaciones se define en la Rec. UIT-T M.3010, mientras que la arquitectura física se muestra en la figura 13. La red de gestión define interfaces que establecen los intercambios necesarios para realizar las funciones OAM&P a distintos niveles.



Interfaces

RCD Red de comunicación de datos
NE Elemento de red
OS Sistema de operaciones
WS Estación de trabajo

Figura 13
Ejemplo de arquitectura física conforme a la Rec. UIT-T M.3010

Desde el punto de vista de la seguridad, los requisitos que se imponen a las diferentes interfaces pueden variar. La interfaz Q funciona en un solo dominio administrativo, mientras que la X lo hace entre diferentes dominios que pueden pertenecer a diversos proveedores. Si bien ambas tienen necesidades de seguridad, es necesario aplicar medidas más robustas a la interfaz X para contrarrestar las amenazas. En la Rec. UIT-T M.3016 se examinan las amenazas contra la seguridad, las vulnerabilidades y las medidas de seguridad para dichas interfaces, mientras que en la Rec. UIT-T M.3320 se dan detalles más específicos relacionados con la seguridad de la interfaz X. En las Recomendaciones UIT-T Q.811 y Q.812 se especifican los aspectos de protocolo para las diferentes capas de comunicación.

Tratándose de la seguridad en el contexto de gestión, hay dos facetas diferentes. Una de ellas, tiene que ver con el plano de gestión para una actividad de extremo a extremo (por ejemplo, servicios VoIP). Se recomienda efectuar de una manera segura toda actividad de gestión en la que se requiera administrar usuarios. Esto es lo que se conoce como *seguridad de la información de gestión* que se intercambia en la red a fin de establecer una aplicación extremo a extremo. La segunda faceta es la gestión de la información de seguridad. Sin importar el tipo de aplicación, por ejemplo VoIP o actividad de informe de dificultades entre dos proveedores de servicios, conviene también gestionar las medidas de seguridad como por ejemplo la utilización de las claves de criptación. Esto es lo que se conoce como *gestión de la información de seguridad*. La PKI que se definió en la cláusula anterior es un ejemplo de esta última faceta. En la Recomendación UIT-T M.3400 se definen varias funciones relacionadas con ambas facetas.

Gracias a la utilización del marco de la Rec. UIT-T X.805, se dispone de varias Recomendaciones que tratan el tema de funciones de gestión para las tres componentes del plano de gestión. En las subcláusulas a continuación se describen algunas de estas Recomendaciones y se muestra cómo se trata en ellas el tema de las necesidades de seguridad. Además de las Recomendaciones para las tres capas del plano de gestión, hay otras que definen servicios genéricos o comunes como por ejemplo las alarmas de informes cuando hay una violación de seguridad, las funciones de auditoría, y los modelos de información que definen niveles de protección para diferentes objetivos (es decir, entidades de gestión).

6.4.2 Intersección entre plano de gestión y capa de infraestructura

Este elemento trata sobre cómo garantizar la seguridad de la actividad de gestión de los elementos de infraestructura de la red, es decir de los elementos de transmisión y conmutación y de los enlaces que los conectan, así como de los sistemas extremos (por ejemplo, los servidores). Como ejemplo, conviene que sea un usuario autorizado quien ejecute actividades del tipo configuración de elementos de red. La conectividad extremo a extremo puede considerarse en términos de la(s) red(es) de acceso y red(es) troncal(es) núcleo, en las que pueden utilizarse diversas tecnologías y para las que se han elaborado varias Recomendaciones. Una de las redes que se utiliza para el acceso es la red óptica pasiva de banda ancha (BPON, *broadband passive optical network*), cuya administración de privilegios de usuario se define utilizando la metodología de modelado unificado que aparece en la Rec. UIT-T Q.834.3, mientras que el intercambio de gestión se hace a través de CORBA (arquitectura de intermediario de petición de objeto común), especificada en Q.834.4. La interfaz que se describe en dichas Recomendaciones es la interfaz Q que se muestra en la figura 13 y que se aplica entre el sistema de gestión de elementos y los sistemas de gestión de red. Aquél se utiliza para gestionar los elementos de red particulares y, por tanto, tiene conocimiento de los detalles internos de las arquitecturas de hardware y software de los elementos que provienen de distintos fabricantes, mientras que los segundos ejecutan actividades al nivel de red extremo a extremo y cubren sistemas de gestión provenientes de muchos fabricantes. En la figura 14 se muestran los diferentes objetos que se utilizan en la creación, supresión, atribución y utilización de información de control de acceso para los usuarios del sistema de gestión de elementos. La lista de permisos de usuarios incluye para cada uno de ellos una enumeración de las actividades de gestión que le son permitidas. El gestor de control de acceso verifica el Id del utilizador y la contraseña del usuario de la actividad de gestión y concede el acceso a la funcionalidad permitida en la lista mencionada.

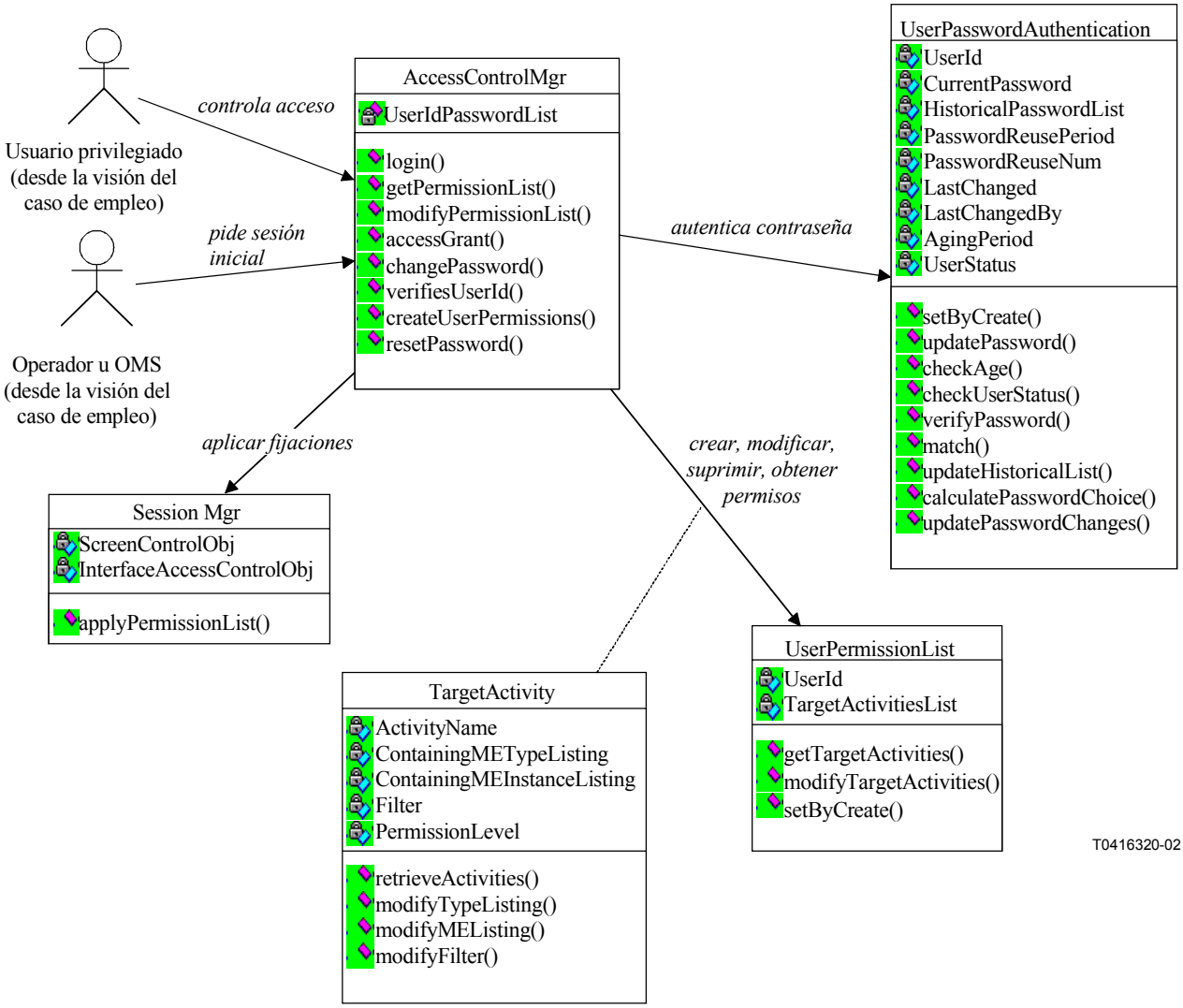


Figura 14
Administración de privilegios de usuarios conforme a la Rec. UIT-T Q.834.3

6.4.3 Intersección entre capa de servicios y plano de gestión

Tiene que ver con el tema de la seguridad de las actividades involucradas en la supervisión y control de los recursos de red suministrados para la prestación de servicios del proveedor. En las Recomendaciones UIT-T se tratan dos aspectos relacionados con esta intersección, a saber en primer lugar el poder garantizar que se disponga de las medidas de seguridad adecuadas para los servicios existentes en la red. Se puede, por ejemplo, garantizar que sólo se permita a los usuarios validados ejecutar operaciones asociadas con la prestación de un servicio. El segundo aspecto se refiere a la definición de cuáles intercambios administrativos y de gestión son válidos. De esta manera, se facilita la detección de violaciones de seguridad, que suelen ser gestionadas mediante sistemas de gestión específicos.

La Rec. UIT-T M.3208.2 sobre gestión de la conexión constituye un ejemplo de una en la que se trata el primer aspecto, la actividad de gestión de un servicio. El usuario a quien pertenecen enlaces preconfigurados lo utiliza para establecer una conexión de circuito arrendado extremo a extremo. Dicho servicio de gestión de conexión le permite crear/activar, modificar y suprimir los circuitos arrendados dentro de los límites impuestos por los recursos preconfigurados. Al tratarse de una conectividad de extremo a extremo establecida por el usuario, es necesario garantizar que se permita solamente a usuarios autorizados efectuar dichas operaciones. Las dimensiones de seguridad definidas para la actividad de gestión asociada con dicho servicio conforman un subconjunto de las ocho discutidas en la cláusula 2.5 y son: autenticación de entidad par, control de integridad de datos (a fin de evitar la modificación no autorizada de los datos mientras transitan), y control de acceso (para garantizar que un abonado no pueda acceder malintencionada o accidentalmente a la información de otro).

La Rec. UIT-T M.3210.1 es un ejemplo de una en la que se definen las actividades administrativas asociadas con el plano de gestión para el caso de servicios inalámbricos, o lo que es lo mismo es un ejemplo del segundo aspecto mencionado.

En una red inalámbrica, los usuarios pueden desplazarse desde una red propia hasta una visitada, mientras atraviesan diferentes dominios administrativos. En la Rec. UIT-T M.3210.1 se describe cómo el dominio de gestión de fraude de la ubicación propia recolecta la información adecuada sobre un abonado, una vez que éste se registró en la red visitada. En la figura 15 se presentan los casos a) y b) relativos al inicio de la actividad de gestión de supervisión efectuado bien sea por la red propia o por la visitada.

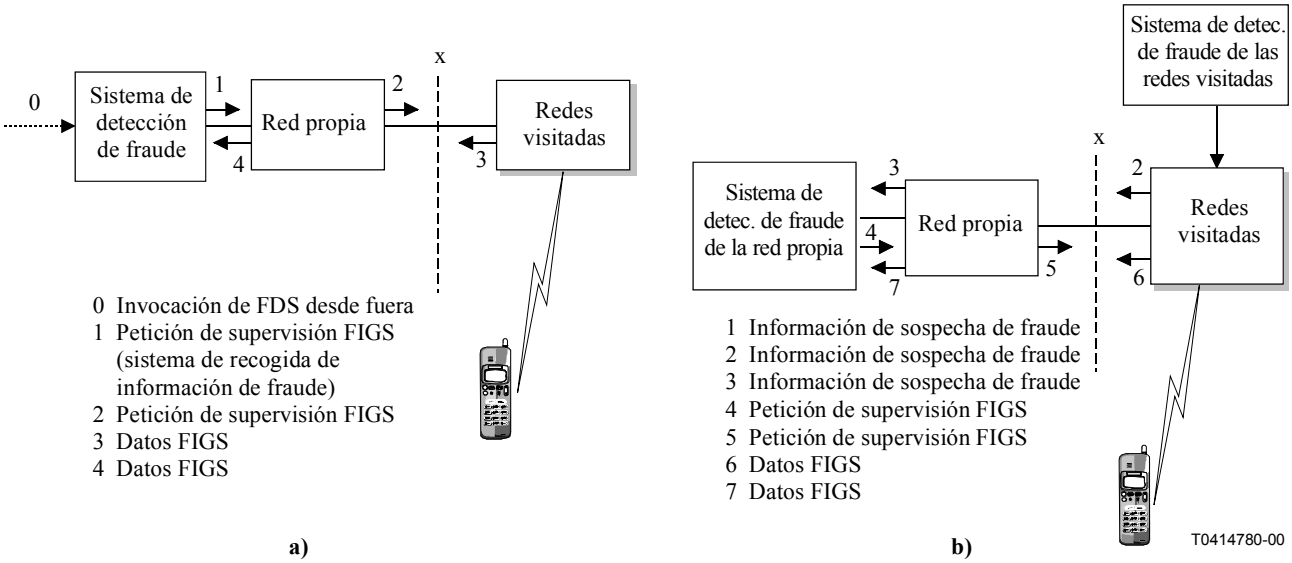


Figura 15
Servicio de gestión de fraudes para los servicios inalámbricos conforme a la Rec. UIT-T M.3210.1

6.4.4 Intersección del plano de gestión y la capa de aplicación

El tercer elemento tiene que ver con la seguridad de las aplicaciones basadas en red de usuario extremo. En las Recomendaciones UIT-T de las series X.400 y X.500 se han definido aplicaciones del tipo de mensajería y directorios, por ejemplo.

Otra clase de aplicaciones en las que se han de asegurar las actividades de gestión son las aplicaciones de gestión propiamente dichas. Aunque parezca redundante, es posible explicarlo mejor con algunos ejemplos: el usuario final de estas aplicaciones es el personal de (las operaciones de) gestión que forma parte de la administración del proveedor de servicio. Considérese el caso en que un proveedor de servicio utiliza los servicios de conexión de otro a fin de poder ofrecer un servicio de conectividad de extremo a extremo. Dependiendo del entorno reglamentario o de mercado, es posible que algunos proveedores de servicio ofrezcan servicios de acceso, mientras que otros, conocidos como operadores entre centrales, ofrezcan conectividad de larga distancia. Estos operadores arriendan servicios de acceso de los proveedores locales con miras a obtener una conectividad de extremo a extremo entre ubicaciones geográficamente distribuidas. De haber una pérdida de servicio, se utiliza una aplicación de gestión llamada informe de dificultades, a fin de informar de todo el problema entre sistemas de gestión. Tanto el usuario de dichos sistemas como la aplicación propiamente dicha requieren de autorización para poder dar estos informes en los servicios. Se recomienda también que los sistemas y usuarios autorizados desempeñen sus actividades accediendo a la información contenida en esos informes. En la figura 16 se muestran las interacciones que pueden ser adelantadas de una manera segura. Tal como se hace con la administración de las casillas de correo en las aplicaciones de correo electrónico, los privilegios de acceso se administran a fin de evitar el acceso no autorizado a los informes de dificultades. Sólo se permite a un proveedor de servicio emitirlos sobre los servicios que arrienda y no sobre aquéllos arrendados por otros proveedores.

En la Rec. UIT-T X.790 se define esta aplicación de gestión y se utilizan mecanismos como por ejemplo la lista de control de acceso, la autenticación bidireccional para garantizar la seguridad de las actividades. Gracias a estas Recomendaciones se han podido implementar y llevar a cabo esta aplicación y los mecanismos de seguridad necesarios para la autenticación.

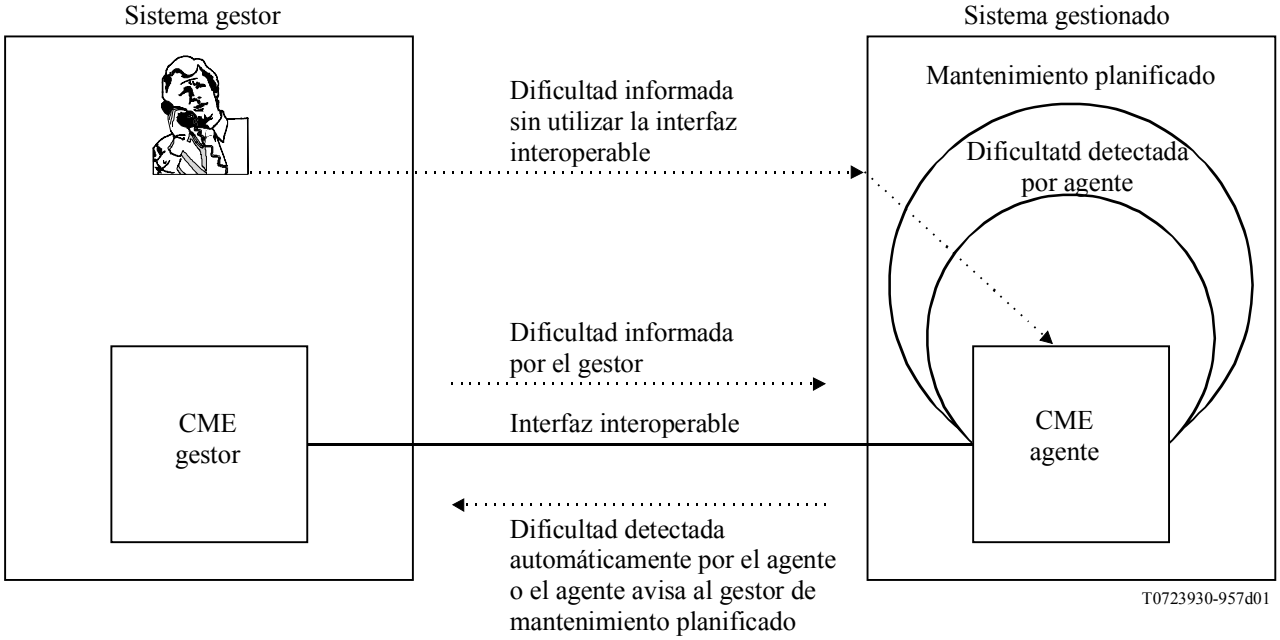


Figura 16
Creación de informe de gestión de dificultades conforme a la Rec. UIT-T X.790

6.4.5 Servicios comunes de gestión de seguridad

En las Recomendaciones UIT-T X.736, X.740 y X.741 se definen servicios comunes que se pueden aplicar a los tres elementos del plano de gestión siempre que se utilice en la interfaz el protocolo CMIP. En la Rec. UIT-T X.736 se definen incluso tipos de violación de seguridad física y se informa a los sistemas de gestión de las alarmas que resultan de ellos. Ésta constituye una actividad del plano de gestión que puede ser utilizada para informar sobre violación de seguridad cuando un usuario no autorizado obtenga acceso que le permita efectuar actividades de configuración en un elemento de red o pueda registrar usuarios para que disfruten de servicios o casillas de correo electrónico. La función de auditoria que se define en X.740, aplicable a las tres capas, describe cómo incluir en el fichero de registro cronológico los eventos relacionados con la violación de seguridad. En X.741 se define un modelo general y que se adapta a cualquier caso de utilización, para permitir la atribución de privilegios de control de acceso a las actividades gestionadas independientemente de los objetivos. Este modelo es rico en características gracias a que se define la capacidad de atribuir privilegios a un nivel de atributos muy concretos de objetivos.

La Rec. UIT-T Q.816 también adoptó los servicios de seguridad genéricos que se definieron en el foro del grupo de gestión de objetos (OMG, *object management group*) para las actividades de gestión realizadas a través del paradigma CORBA.

6.5 Ciberrecetas médicas por Internet (E-prescriptions)

Los servicios de salud requieren y generan una amplia variedad de datos e información, que ha de recolectarse, procesarse, distribuirse y a la cual se ha de poder acceder para utilizarla de una manera segura y que respete reglas legales y éticas estrictas. Si bien esto es particularmente esencial para la información clínica y de gestión, también es importante para otros tipos de información como: epidemiológica, bibliográfica y de bases de datos de conocimientos.

Las fuentes de todos estos tipos de datos e información pueden estar dentro y fuera de la infraestructura de los servicios de salud y ubicadas a diferentes distancias desde sus respectivos usuarios. En la práctica, los usuarios necesitan y generan una variedad de estas informaciones en diferentes etapas de sus funciones respectivas, por ejemplo, puede ocurrir que un médico quiera consultar una base de datos de información especializada mientras examina un paciente y asentando la información en su registro, que pueda ser utilizada para fines de facturación.

Las reuniones y transacciones que tienen que ver con la prestación de servicios de salud tienen múltiples facetas. Se dan, por ejemplo, entre un médico y un paciente, dos médicos, un médico y un asesor experto, un paciente y una institución de prestación de servicios de salud como un laboratorio de prueba, una farmacia o un centro de rehabilitación. Pueden ocurrir en la propia comunidad de residencia de la persona, en cualquier otra parte del país o en el exterior, y para todos ellos se necesitan datos e información antes de empezar, así como durante la reunión o inmediatamente después. Dichos datos e información pueden variar en cuanto a volúmenes, horarios y formas, como por ejemplo voz, cifras, textos, gráficas o imágenes estáticas o dinámicas, aunque con frecuencia constituyen una mezcla acertada de todos ellos.

Puede ocurrir que las fuentes y lugares de almacenamiento de estos datos e información se encuentren distribuidos en distintos lugares y en distintos formatos, por ejemplo, información completa sobre los pacientes, recetas manuscritas, e informes escritos por un médico, un asesor o un laboratorio.

Hasta no hace mucho tiempo, todos estos encuentros ocurrían en persona y el modo principal de comunicación y archivo de la información médica era la palabra oral o escrita, mientras que su transporte se efectuaba a través de servicios públicos o privados como el transporte terrestre, por ferrocarril o aéreo. A medida que se popularizó la red telefónica se convirtió en la red de comunicación de los profesionales e instituciones de la salud, nacional e internacionalmente, hasta la llegada de las herramientas modernas relativas a la cibersalud.

La utilización de la tecnología en los aspectos clínico/médico de los servicios de salud ha venido creciendo constantemente e incluye instrumentación y equipos, en particular equipos de detección y medida, servicios de laboratorio, y formación de imágenes médicas estáticas y dinámicas. Ha sido entonces inevitable que con el uso cada vez más frecuente de estas tecnologías y con su variedad y sofisticación los servicios tecnológicos dependan cada vez más de instituciones diferentes de las de prestación de servicios de salud, separadas de estas últimas no sólo en distancia sino especialmente en aspectos relativos a la gestión. Por ende, la comunicación entre los servicios basados en la tecnología y los servicios principales de salud se ha convertido en algo fundamental a la hora de considerar la eficacia y rentabilidad de esos servicios.

La utilización común de las TIC en el sector de salud empezó hace apenas 25 años con simples mensajes electrónicos que contenían notas e informes puramente alfanuméricos. De la misma manera que la necesidad de la comunicación vocal impulsó la instalación de teléfonos en los consultorios médicos e instituciones de salud, el correo electrónico fue la razón originaria para la instalación de enlaces modernos de telecomunicaciones. Así las cosas, a medida que crecían los servicios de correo electrónico lo hizo la demanda sobre su calidad de funcionamiento y cobertura geográfica, es decir se iban necesitando cada vez más ubicaciones a mayor velocidad y con mayor ancho de banda como consecuencia del crecimiento incipiente del tamaño de los ficheros adjuntos a los mensajes de correo electrónico. Durante la última década se ha podido observar el crecimiento exponencial de la utilización del correo electrónico en el sector de la salud, dentro de los países y entre ellos, incluidos los más pobres, en particular por lo que se refiere a la utilización de la Internet. Por ejemplo, las transacciones electrónicas reemplazan cada vez más a aquellas que no requieren de reuniones personales, como por ejemplo para la preparación y envío de informes y recetas médicas, el establecimiento de citas y programación de servicios, la remisión de pacientes y, siempre que la calidad de los servicios de telecomunicaciones lo permita, la transmisión de imágenes médicas y sus correspondientes diagnósticos efectuados por expertos, bien sea escritos u orales.

La telemedicina, es decir la "prestación de servicios médicos mediante las comunicaciones de audio, imagen y datos", es otro nivel de sofisticación de la utilización de las TIC que incluye el diagnóstico real, el examen e incluso el tratamiento de un paciente que se encuentre en una ubicación distante. La telemedicina es un campo importantísimo que experimenta un gran crecimiento y que se espera que cambie muchas de las costumbres tradicionales en los servicios de salud; de hecho, constituye el inicio de un nuevo paradigma en la atención médica.

Aunque el acceso y utilización de los sistemas basados en conocimiento no sea algo relativamente muy reciente, se prevé que su utilización se expandirá con la diseminación del soporte telemático. Estos sistemas, también conocidos como sistemas expertos y de soporte de decisión, proporcionan consejo y ayuda experta sobre aspectos y procedimientos médico-científicos. Por ejemplo, teniendo en cuenta los síntomas que presenta un paciente y en dónde se encuentre, puede proporcionar soporte de diagnóstico, sugerir pruebas adicionales o proponer un tratamiento.

De igual manera, todos estos desarrollos están produciendo un efecto importante en los sistemas de información de gestión (MIS) pertinentes que necesita y utiliza el sector de salud, es decir los MIS hospitalarios. Éstos ya no son sólo sistemas útiles para la gestión administrativa de la atención hospitalaria a pacientes, que van desde la admisión hasta que son dados de alta o transferidos, sino que también incluyen una variedad de interfaces inteligentes y fáciles de utilizar para el personal médico como, por ejemplo, sistemas de soporte de decisiones clínicas, enlaces de telemedicina, portales Internet, etc.

Conviene tener en cuenta otros dos aspectos bastante reales que tienen que ver tanto con los pacientes como con el personal de salud: su movilidad y necesidad de tener las manos libres para poder entonces dedicarse a la atención médica propiamente dicha. Por movilidad se entiende poder llegar a la información médica necesaria, por ejemplo, la versión electrónica de la historia médica de un paciente, o a una herramienta o instrumento, desde cualquier ubicación distante y siempre que sea necesario sujeto a la verificación de identidad, dentro del mismo edificio o ciudad así como dentro de todo un país y entre países. La característica "manos libres" implica que se han de poder encontrar soluciones para las funciones de identificación y autorización sin que el personal médico tenga que utilizar sus manos, es decir sin que sea necesario abrir una puerta o escribir en un teclado de computador, por ejemplo.

Se puede decir entonces que el servicio de salud es un sector en el que se hace un gran énfasis en la información, cuya recolección, flujo, procesamiento, presentación y distribución son factores claves para la eficacia, eficiencia y rentabilidad de las operaciones y desarrollo de los servicios de salud dentro de un país y entre varios de ellos.

Es fundamental que dicho flujo de información ocurra de una manera segura y confidencial y dentro de un marco estricto de reglas y reglamentaciones éticas y jurídicas.

6.5.1 Aspectos relativos a la PKI y la PMI en aplicaciones de cibersalud

Gracias a su cadena de autoridades de certificación, la PKI reproduce una estructura jerárquica del mundo real, sin importar si es geopolítica (regiones-países-estados-ciudades), o temática (salud-medicina-cirugía-cirugía especializada-proveedores, etc.). Más aún, dada la ubicuidad, la jerarquía de largo alcance y la cada vez mayor interactividad a través de las fronteras del sector de salud, es evidente que se ha de definir una PKI/PMI normalizada para este sector.

Se debe garantizar el interfuncionamiento técnico de los sistemas relativos a la salud mediante el uso exhaustivo de normas tecnológicas. Los fabricantes de las soluciones más seguras ya han adoptado normas del tipo X.509. Puesto que la autenticación de usuario es una aplicación crítica que depende de información local, la libertad de seleccionar determinadas PKI y PMI no debería afectar la capacidad del usuario para interactuar con personas certificadas por otras PKI/PMI en el sector de salud (lo que, por supuesto, también vale para al menos un mínimo de normalización relativa al control de acceso y otras políticas relacionadas en el sector de salud). Para ello, se pueden implementar diversas estrategias que habrían de incluir el reconocimiento mutuo de las diversas infraestructuras o la utilización de una raíz común. Se podrá garantizar una eficacia completa y un entorno integrado para todas las transacciones de salud en el mundo mediante la adopción de normas tecnológicas, el interfuncionamiento técnico de las diversas infraestructuras y la normalización de ciertas políticas.

6.5.2 Sistema de ciberrecetas médicas de Salford

El sistema de ciberrecetas médicas descrito en [Policy] constituye un buen ejemplo de una PKI y una PMI aplicadas a la cibersalud. Dado el gran número de profesionales de la salud que participan en el programa de transmisión electrónica de recetas médicas (ETP, *electronic transmission of prescriptions*) en el Reino Unido (34 500 médicos generales, 10 000 enfermeras con autorización para recetar que pasarán a ser 120 000 en los próximos años, 44 000 farmacéuticos registrados y 22 000 dentistas), y las poquísimas autorizaciones que se requieren hoy en día (es decir, diversos niveles de autorización para recetar y entregar medicamentos, así como derechos para recetas médicas gratuitas), cabe suponer que el mecanismo ideal de autorización para la ETP es el control de acceso basado en las funciones (RBAC, *role-based access controls*). Si se tiene en cuenta también que en el

Reino Unido hay cerca de 60 millones de pacientes en potencia, y que el 85% de los medicamentos formulados corresponden a recetas gratuitas [FreePresc], sería conveniente también utilizar el RBAC para el control de acceso a éstas de ser posible. Al ser necesario autorizar/otorgar derechos a tanta gente, es fundamental que se distribuya la gestión de las funciones entre las autoridades competentes en lugar de hacerlo de una manera centralizada, en cuyo caso el sistema sería inmanejable.

Para cada profesión de la salud ha de existir un órgano superior que otorgue el derecho a ejercerla. En el Reino Unido, por ejemplo, el General Medical Council se encarga del registro de los doctores, y es responsable de sanciones en caso de falta profesional. Para los dentistas esta función la cumple el General Dental Council, para las enfermeras el Nursing and Midwifery Council, y para los farmaceutas el Royal College of Pharmacy. Puesto que estos organismos cumplen a cabalidad el objetivo de atribuir las funciones, en el sistema ETP también se les utiliza para ello.

Creado en junio de 2001, el Department for Work and Pensions (DWP) ha absorbido a los antiguos departamentos de Seguridad Social, Educación y Empleos, y se encarga de pagar los subsidios de desempleo y las pensiones, así como de determinar, junto con la Prescription Pricing Authority (PPA), los derechos a las recetas gratuitas. Muchas personas tienen ese derecho, a saber los mayores de 60 años, los menores de 16, los jóvenes entre 16 y 18 en formación de tiempo completo, las personas sujetas al pago de Income Support or Jobseeker's Allowance y sus cónyuges, aquellos mencionados en un Low Income Scheme Full Help Certificate (HC2) del Sistema nacional de salud (NHS), las mujeres embarazadas, las que han dado a luz en los últimos 12 meses, y los incapacitados por causas de guerra. En consecuencia, se distribuye la gestión de estos derechos entre diversas componentes del DWP y la PPA.

Los organismos que rigen cada profesión atribuyen certificados de atributos de función a cada profesional, que se almacenan en el directorio LDAP del órgano correspondiente. Siempre que el sistema ETP esté autorizado a acceder a dichos directorios podrá tomar decisiones de autorización acerca de las recetas y la entrega de los medicamentos. De igual manera, el sistema ETP podrá tomar decisiones acerca del derecho a la receta de medicinas gratuitas siempre y cuando pueda acceder el directorio LDAP en el que el DWP almacena los certificados de atributo de función que otorga a quienes tienen derecho, por las razones ya mencionadas, a las medicinas gratuitas, sin que sea necesario que el farmaceuta pregunte al paciente si tiene el derecho a ello. Esto último será necesario solamente cuando se trate de un paciente que acaba de recibir el derecho, por ejemplo cuando se diagnostica por primera vez un embarazo, y el DWP no ha tenido tiempo suficiente para crear el certificado oficial de atributo.

Posteriormente, un dispositivo de autorización (como por ejemplo PERMIS, véase www.permis.org) utiliza estas funciones para establecer si un médico está autorizado para recetar, un farmaceuta para entregar, y un paciente para recibir recetas de medicación gratuita, conforme a la política del ETP. Cada aplicación ETP (sistemas de elaboración de recetas, entrega de medicamentos, y PPA) lee la política ETP en el momento de la inicialización, para que cuando los profesionales propiamente dichos soliciten acciones, como por ejemplo, recetar o entregar medicamentos, el dispositivo de decisión de autorización recupere la función de las personas a partir del directorio LDAP adecuado, y tome una decisión con arreglo a la política. Los usuarios pueden, por tanto, obtener acceso a múltiples aplicaciones, con la sola condición de poseer un par de claves PKI. Puede ocurrir que la emisión de los certificados de atributo de función tenga lugar sin que intervenga directamente el usuario, y sin que éste deba preocuparse sobre cómo y dónde están almacenados y cómo los utiliza el sistema.

En la figura 17 se muestra un ejemplo de implementación del sistema de ciberrecetas en el Reino Unido que incluye varios de los aspectos de seguridad esenciales. En el núcleo del sistema se encuentra una infraestructura de seguridad que permite proporcionar no solamente autenticación robusta (es decir, una PKI que utilice certificados de clave pública), sino también autorización robusta (es decir, PMI) en el cual los derechos específicos que poseen los profesionales de la salud han sido otorgados conforme a las funciones almacenadas en los certificados de atributos. En los modelos tradicionales se utilizan listas de control de acceso escondidas en cada aplicación (por ejemplo historias médicas, bases de datos de recetas, seguros, etc.), que hacen que los usuarios (doctores, farmaceutas, pacientes, etc.) requieran tal vez obtener y administrar varios testigos diferentes de seguridad (por ejemplo nombre de usuario/contraseña, tarjetas, etc.). Puesto que el nuevo modelo dispone de PKI y PMI, el usuario necesita solamente un testigo (el certificado de clave pública del usuario), a fin de poder disfrutar de los diferentes servicios y recursos que están distribuidos geográfica y/o topológicamente. Es el sistema y no el usuario quien mantiene los certificados de atributos de este último, que son transferidos entre los componentes conforme resulte necesario de tal manera que se pueda otorgar el acceso. Al tratarse de certificados de atributo con la firma digital de sus emisores, no se pueden falsificar durante estas transferencias.

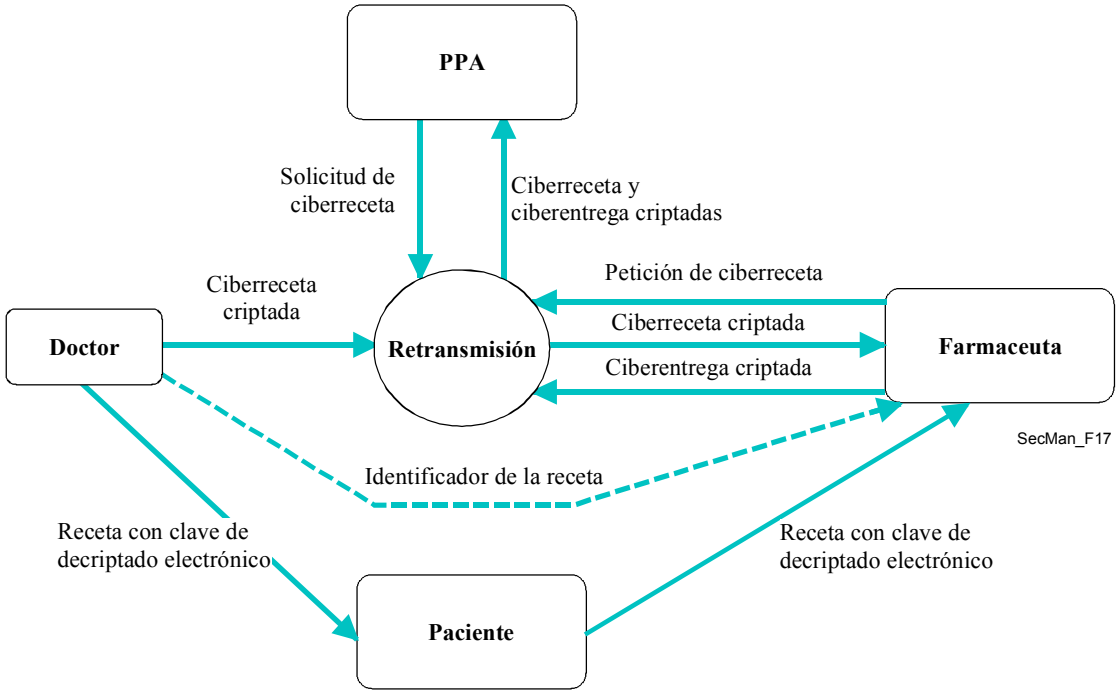


Figura 17
Sistema de ciberrecetas de Salford

En el ejemplo de la figura 17, el médico elabora la ciberreceta, tras lo cual se incluye una firma digital (a efectos de autenticación), se cripta simétricamente mediante una clave de sesión aleatoria (con fines de lograr la confidencialidad) y se envía a una ubicación central de almacenamiento. El paciente recibe una receta en papel que contiene un código de barras que presenta la clave de criptación simétrica, con lo cual puede ir a la farmacia de su elección, entregarlo al farmaceuta, quien la recupera utilizando el código de barras y la decripta. Si bien a la larga es el propio paciente quien controla a la persona autorizada a despacharle su fórmula, tal como ocurre en el sistema tradicional basado en recetas en papel, esto no es suficiente: ha de haber controles relativos a quién está autorizado para formular y entregar determinados tipos de medicamentos y quién tiene derecho a las recetas gratuitas.

Ahora bien, aun si todo lo anterior pareciera indicar un sistema altamente integrado, éste puede en realidad estar distribuido, de tal manera que el directorio de atributos de doctor sea diferente del sistema que autentica a los farmaceutas, o almacena los derechos y políticas de entrega de medicamentos, etc., que dependen de terceras partes de confianza para autenticar y autorizar a los diferentes participantes. Aún cuando sea posible aplicar soluciones PKI y PMI dependientes de fabricantes, es recomendable utilizar soluciones normalizadas como la X.509 a fin de lograr un acceso más generalizado y global a las ciberrecetas médicas.

7 Conclusiones

El UIT-T ha venido desarrollando desde hace mucho tiempo un conjunto de Recomendaciones fundamentales sobre el tema de la seguridad, a saber: la X.800 que es un documento de referencia sobre la arquitectura de seguridad para la interconexión de sistemas abiertos, y la serie X.810-X.816 donde se define un marco de seguridad para los sistemas abiertos, incluyendo aspectos generales, autenticación, control de acceso, no repudio, confidencialidad, integridad y seguridad y alarmas de auditoría, respectivamente. La Rec. UIT-T X.805, más reciente, ha sido desarrollada a fin de describir la arquitectura de seguridad para los sistemas que permiten comunicaciones extremo a extremo. En la revisión arquitectural incluida en esta última Recomendación se tiene en cuenta las crecientes amenazas y vulnerabilidades que resultan de los nuevos entornos de proveedor multired y multiservicios. La Rec. UIT-T X.509 que trata los marcos de claves públicas y atributos es, con seguridad, el texto más citado del UIT-T sobre aplicaciones de seguridad, bien sea directamente o a través de su referencia en otras normas que incorporen sus principios.

De otra parte, el UIT-T ha desarrollado disposiciones de seguridad para diversos sistemas y servicios que se definen en sus propias Recomendaciones. En la cláusula 6 de este Manual se describen algunas de ellas, como por ejemplo, VoIP que utiliza H.323 o IPCablecom, la transmisión segura de facsímil, y la gestión de red. Se presenta también un ejemplo de utilización de aplicaciones de clave pública e infraestructura de gestión de privilegios en cibersalud. *Caveat emptor*, hay muchas *más* áreas para que las Recomendaciones UIT-T traten necesidades de seguridad en las telecomunicaciones y las TI. En futuras versiones de este Manual se incluirán estos aspectos y otros como la prevención de fraude, el restablecimiento y recuperación en caso de desastre que están siendo desarrollados por varias Comisiones de Estudio. El trabajo del UIT-T en temas relativos a la seguridad se ve reforzado gracias a la organización de seminarios o talleres internacionales sobre seguridad, o la participación en ellos, el desarrollo de un proyecto de seguridad y a la creación de una comisión de estudio rectora para estos trabajos en el Sector.

Referencias

Además de las Recomendaciones del UIT-T (que puede encontrarse en http://www.itu.int/ITU-T/publications/recs.html) mencionadas en este Manual, también se utilizó el siguiente material.

[ApplCryp] B. Schneier, "Applied Cryptography – Protocols, Algorithms and Source Code in C" 2nd edition, Wiley, 1996; ISBN 0-471-12845-7

[Chadwick] D. W. Chadwick; "The Use of X.509 in E-Healthcare", Workshop on Standardization in E-health; Geneva, 23-25 de mayo de 2003; PowerPoint at www.itu.int/itudoc/itu-t/workshop/e-health/s5-02.html and audio presentation at www.itu.int/ibs/ITU-T/e-health/Links/B-20030524-1100.ram

[Euchner] M. Euchner, P-A. Probst; "Multimedia Security within Study Group 16: Past, Presence and Future", ITU-T Security Workshop; 13-14 de mayo de 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s2p3r1.html

[FreePresc] Free prescriptions statistics in the UK; www.doh.gov.uk/public/sb0119.htm

[Packetizer] "A Primer on the H.323 Series Standard" www.packetizer.com/iptel/h323/papers/primer/

[Policy] D. W. Chadwick, D. Mundy; "Policy Based Electronic Transmission of Prescriptions"; IEEE POLICY 2003, 4-6 de junio, Lake Como, Italy. sec.isi.salford.ac.uk/download/PolicyBasedETP.pdf

[SG17] ITU-T Study Group 17; "Lead Study Group on Communication System Security" www.itu.int/ITU-T/studygroups/com17/cssecurity.html (*Section 2* on the Catalogue of ITU-T Recommendations related to Communications System Security; *Section 3* on Compendium of Security Definitions in ITU-T Recommendations)

[Shannon] G. Shannon; "Security Vulnerabilities in Protocols"; ITU-T Security Workshop; 13-14 de mayo de 2002, Seoul, Korea; www.itu.int/itudoc/itu-t/workshop/security/present/s1p2.html

[Wisekey] S. Mandil, J. Darbellay; "Public Key Infrastructures in e-health"; written contribution to Workshop on Standardization in E-health; Geneva, 23-25 de mayo de 2003; www.itu.int/itudoc/itu-t/workshop/e-health/wcon/s5con002_ww9.doc

Anexo A: Terminología relativa a la seguridad

La relación de acrónimos y terminología que se presenta a continuación, se obtuvo de diversas Recomendaciones del UIT-T pertinentes así como de otras fuentes externas, como se indica cuando procede. Además, es recomendable referirse al anexo A.3 donde podrán encontrarse recursos complementarios

A.1 Acrónimos relacionados con la seguridad que se utilizan frecuentemente

Acrónimo	Definición
3DES	[H.235] DES triple.
A	[M.3010] Agente.
A/M	[M.3010] Agente/gestor.
AA	[X.509] Autoridad de atributo.
AAA	[X.805] Autenticación, autorización y contabilidad (*authentication, authorization and accounting*).
AARL	[X.509] Lista de revocación de autoridades de atributo (*attribute authority revocation list*).
ACI	[X.810] Información de control de acceso (*access control information*).
ACRL	[X.509] Lista de revocación de certificados de atributo (*attribute certificate revocation list*).
AE	[M.3010] Entidad de aplicación (*application entity*).
AES	[H.235] [J.170] Algoritmo de criptación avanzado (*advanced encryption standard algorithm*)
AH	[J.170] La cabecera de autenticación es un protocolo de seguridad de IPSec que ofrece integridad de los mensajes para paquetes IP completos, incluida la cabecera IP.
ASCII	[T.36] Código de la norma americana para intercambio de información (*american standard code for information interchange*).
ASD	[J.170] Datos específicos de aplicación (*application-specific data*). Campo específico de aplicación que aparece en el encabezamiento IPSec y que junto con la dirección IP de destino proporciona un número único para cada SA.
ASN.1	[H.680] Notación de sintaxis abstracta N.º 1 (*abstract syntax notation no.1*).
ASP	[X.805] Proveedor de servicio de aplicación (*application service provider*).
ATM	[X.805] Modo de transferencia asíncrono (*asynchronous transfer mode*).
ATM	[M.3010] Modo de transferencia asíncrono (*asynchronous transfer mode*).
AuF	[H.530] Función de autenticación (*authentication function*), véase la Rec. UIT-T H.510 [6].
B(n)	[T.36] Valor básico (n) (*base value (n)*).
BE	[H.530] Elemento de frontera (*border element*), véase el anexo G/UIT-T H.225.0 [2].
BES	[H.235] Servidor fuera del terminal (*backend server*).
BML	[M.3010] Capa de gestión empresarial (*business management layer*).
B-OSF	[M.3010] Función de sistema de operaciones – Capa de gestión empresarial (*business management layer – operations systems function*).
BPI+	[J.170] Interfaz de privacidad de referencia plus (*baseline privacy interface plus*) es la parte de seguridad de la Rec. UIT-T J.112 que funciona en la capa MAC.
CA	[H.234] [H.235] [J.170] [X.509] Autoridad de certificación (*certification authority*). Organización de confianza que acepta aplicaciones de certificados de las entidades, autentica las aplicaciones, emite certificados y mantiene información del estado de los certificados. [J.170] Agente de llamada (*call agent*). Parte de la CMS que mantiene el estado de la comunicación, y controla el lado de la línea de ésta.
CARL	[X.509] Lista de revocación de autoridades de certificación (*certification authority revocation list*).
CBC	[H.235] [J.170] Concatenación de bloques cifrados (*cipher block chiang*).
CCA	[H.234] Autoridad de certificación de país (*country certification authority*).

Acrónimo	Definición
CFB	[H.235] Modo de retroalimentación cifrado (*cipher feedback mode*).
CH_n	[H.530] Desafío número n (*challenge number n*).
CM	[J.170] Módem de cable (*cable modem*).
CME	[X.790] Entidad de gestión conforme (*conformant management entity*).
CMIP	[M.3010] Protocolo común de información de gestión (*common management information protocol*).
CMIS	[X.790] Servicio común de información de gestión (*common management information service*).
CMISE	[X.790] Elemento de servicio común de información de gestión (*common management information service element*).
CMS	[J.170] Sintaxis de mensaje criptográfico (*cryptographic message syntax*). [J.170] Servidor de gestión de llamadas *(call management server),* que controla las conexiones de audio. También conocido como Agente de llamada (*call agent*) en la terminología MGCP/SGCP (este es un ejemplo de servidor de aplicación).
CMTS	[J.112] Sistema de terminación de módem de cable (*cable modem termination system*).
CNM	[X.790] Gestión de red de cliente (*customer network management*).
CORBA	[SANCHO] Arquitectura de intermediario de petición de objeto común (*common object request broker architecture*).
CRL	[H.235] [X.509] Lista de revocación de certificados (*certificate revocation list*).
DCF	[M.3010] Función de comunicación de datos (*data communication function*).
dCRL	[X.509] Lista de revocación de certificados-delta (*delta certificate revocation list*).
DES	[H.235] [J.170] Norma de criptación de datos (*data encryption standard*).
DH	[H.235] [H.350] Diffie-Hellman.
DHCP	[J.170] [X.805] Protocolo dinámico de configuración de anfitrión *(dynamic host configuration protocol*).
DIB	[X.509] Base de información de directorio (*directory information base*).
DIT	[X.509] Árbol de información de directorio (*directory information tree*).
DN	[X.790] Nombre distinguido (*distinguished name*).
DNS	[H.235] [J.170] [X.805] Servidor de nombres de dominio (*domain name server*).
DOCSIS	[J.170] Especificación de la interfaz del servicio de datos por cable (*data-over-cable service interface specification*).
DoS	[X.805] Denegación de servicio (*denial of service*).
DQoS	[J.170] Calidad de servicio dinámica (*dynamic quality of service*).
DS-3	[X.805] Señal digital de nivel 3 (*digital signal level 3*).
DSA	[X.509] Agente de sistema de directorio (*directory system agent*).
DSCP	[J.170] Punto de código de servicios diferenciados (*diffserv code point*). Campo en cada paquete IP que identifica el comportamiento por saltos en los nodos DiffServ. En el IPv4, se redefine el byte TOS para que sea el DSCP. En el Ipv6, se utiliza el octeto Clase de tráfico como DSCP. Véase el anexo C.
DSS	[H.235] Norma sobre firmas digitales (*digital signature standard*).
DTMF	[H.235] [J.170] Multifrecuencia bitono (*dual-tone multi frequency (tones)).*
DUA	[X.509] Agente de usuario de directorio (*directory user agent*).
EARL	[X.509] Lista de revocación de certificados de atributo de entidad final (*end-entity attribute certificate revocation list*).
ECB	[H.235] Libro de código electrónico (*electronic code book mode*).

Acrónimo	Definición
ECC, EC	[H.235] Criptosistema de curva elíptica (*elliptic curve cryptosystem*) (Véase la cláusula 8.7 de la Versión 1.1 de la ATM Forum Security Specification). Sistema de criptación de clave pública.
EC-GDSA	[H.235] Firma digital de curva elíptica con apéndice análogo al algoritmo de firma digital NIST (DSA) (*Elliptic curve digital signature with appendix analog of the NIST digital signature algorithm (DSA*)) (Véase también el capítulo 5 de [ISO/CEI 15946-2]).
ECKAS-DH	[H.235] Esquema de convenio de claves de curva elíptica – Diffie-Hellman (*elliptic curve key agreement scheme – Diffie-Hellman*). Modelo de acuerdo de claves Diffie-Hellman que utiliza criptografía de curva elíptica.
EML	[M.3010] Capa de gestión de elemento (*element management layer*).
EOFB	[H.235] Modo OFB mejorado (*enhanced OFB mode*).
E-OSF	[M.3010] Función de sistema de operaciones – Capa de gestión de elemento (*element management layer – operations systems function*).
EP	[H.235] Punto extremo (*endpoint*).
EP_{ID}	[H.530] Identificador de punto extremo de MT (*MT endpoint identifier*), véase la Rec. UIT-T H.225.0 [1].
EPRL	[X.509] Lista de revocación de certificados de clave pública de entidad final (*end-entity public-key certificate revocation list*).
ESH	[T.36] Troceo (o función *hash*) simple encriptado y aleatorizado (*encrypted and scrambled plain hash)* (24 cifras decimales).
ESIM	[T.36] Mensaje de integridad criptado y aleatorizado (*encrypted scrambled integrity message).* Número con 12 cifras decimales.
ESP	[J.170] Seguridad de encapsulación Ipsec (*IPSec encapsulating security*).
ESSK	[T.36] Clave secreta encriptada y aleatorizada (*encrypted scrambled secret key*). Número con 12 cifras decimales.
FDS	[M.3210.1] Sistema de detección de fraude (*fraud detection system*).
FEAL	[T.36] Familia de algoritmos rápidos de criptado de datos (*fast data encipherment algorithm*) que hace corresponder bloques de 64 bits de texto sin cifrar con bloques cifrados de 64-bits, mediante una clave secreta con la misma longitud. Aunque es similar a la DES, tiene una función f (*f-function)* mucho más simple. Su diseño responde a la necesidad de velocidad y simplicidad, lo que la hace más adecuada para microprocesadores de baja complejidad (smartcards, por ejemplo). (A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
FIGS	[M.3210.1] Sistema de recogida de información de fraude (*fraud information gathering system*).
FQDN	[J.170] Nombre de dominio totalmente cualificado (*fully qualified domain name*). Véase la norma RFC 821 del IETF.
FTP	[X.805] Protocolo de transferencia de ficheros (*file transfer protocol*).
FU	[X.790] Unidad funcional (*functional unit*).
GCA	[H.234] Autoridad de certificación general (*general certification authority*).
GDMI	[M.3210.1] Directrices para la definición de la interfaz de gestión de la RGT (*guidelines for the definition of TMN management interface*).
GDMO	[M.3010] Directrices para la definición de objetos gestionados (*guidelines for the definition of managed objects*).
GK	[H.235] [H.510] [H.530] Controlador de acceso (*gatekeeper*).
GK_{ID}	[H.530] Identificador de controlador de acceso visitado (*visited gatekeeper identifier*), véase la Rec. UIT-T H.225.0 [1].
GNM	[X.790] Modelo de red general (*general network model*).
GRJ	[H.530] Rechazo de controlador de acceso (*gatekeeper reject*).
GRQ	[H.530] Petición de controlador de acceso (*gatekeeper request*).
GW	[H.235] Pasarela (*gateway*).

Acrónimo	Definición
h[*]	[H.234] Resultado de aplicar la función "h" a *.
H-BE	[H.530] Elemento de frontera de base (o propio) (*home BE*).
HFC	[J.165] Híbrido fibra/coaxial [cable] (*hybrid fibre/coaxial (cable)*).
HFX	[T.30] [T.36] Cifrado de facsímil Hawthorne (*hawthorne facsimile cipher*).
H-GK	[H.530] Controlador de acceso de base (o propio) (*home GK*).
HKM	[T.30] [T.36] Algoritmo de gestión de claves de Hawthorne (*hawthorne key management algorithm*).
HKMD1	[T.36] Criptación doble que utiliza el algoritmo HKM (*double encryption using the HKM algorithm*).
HLF	[H.530] Función ubicación de base (o propia) (*home location function*).
HMAC	[J.170] Código de autenticación de mensaje troceado (o generado mediante la función *hash*) (*hashed message authentication code*). Algoritmo de autenticación de mensaje, basado en las funciones *hash* SHA-1 o MD5 y definido en RFC 2104.
HMAC-SHA1-96	[H.530] Código de autenticación de mensaje troceado (o generado) con algoritmo hash securizado 1 (*hashed message authentication code with secure hash algorithm 1*).
HMAC$_Z$	[H.530] Código de autenticación de mensaje troceado (o generado mediante la función *hash*) para clave/respuesta con secreto compartido Z (*key hashed message authentication code/response with shared secret Z*); si no se indica Z se aplica el secreto del salto siguiente.
iCRL	[X.509] Lista de revocación de certificados indirecta (*indirect certificate revocation list*).
ICV	[H.235] Valor de comprobación de integridad (*integrity check value*).
ID	[H.235] Identificador (*identifier*).
IDEA	[T.36] El Algoritmo internacional de criptado de datos (*international data encryption algorithm*) fue creado por Xuejia Lai y James Massey en 1992, utiliza cifrado por bloques con una clave de 128-bits (bloques de 64 bits con clave de 128 bits), y suele considerarse muy seguro y uno de los mejores entre los más conocidos por el público. Desde su aparición, no se conocen ensayos de ataques contra él. (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html)
Idx	[T.36] Últimas seis cifras de la identificación del facsímil (número de teléfono del facsimil) de X.
Idy	[T.36] Últimas seis cifras de la identificación del facsímil (número de teléfono del facsimil) de Y.
IKE	[J.170] Intercambio de claves Internet (*internet key exchange*) es un mecanismo de gestión de claves que se utiliza para negociar y calcular claves para las SA en IPSec.
IKE–	[J.170] Se utiliza cuando se refiere a la utilización del IKE con claves precompartidas a efectos de autenticación.
IM	[T.36] Mensaje de integridad (*integrity message*), que se utiliza para confirmar o denegar la integridad de un mensaje recibido (12 cifras decimales).
IMT-2000	[M.3210.1] Telecomunicaciones móviles internacionales-2000 (*international mobile telecommunications 2000*).
Imy	[T.36] Mensaje de integridad generado por Y para confirmar o denegar la integridad del mensaje recibido (*integrity message generated by Y to confirm or deny integrity of the received message*). Número de 12 cifras decimales.
IP	[X.805] Protocolo Internet (*Internet protocol*).
IPSec	[H.235] [H.530] [J.170] [X.805] Seguridad del protocolo Internet (*Internet protocol security*).
ISAKMP	[H.235] Protocolo de gestión de clave con asociación de seguridad en Internet (*Internet security association key management protocol*).
ISTP	[J.170] Protocolo de transporte de señalización Internet (*Internet signalling transport protocol*).
IV	[H.235] Vector de inicialización (*initialization vector*).
IVR	[J.170] Sistema de respuesta vocal interactiva (*interactive voice response system*).
K	[H.530] Clave de sesión/enlace dinámico (*dynamic session/link key*).
KDC	[J.170] Centro de distribución de claves (*key distribution center*).

Acrónimo	Definición
LAN	[M.3010] Red de área local (*local area network*).
LDAP	[H.235] Protocolo ligero de acceso al directorio (*lightweight directory access protocol*).
LLA	[M.3010] Arquitectura lógica por capas (*logical layered architecture*).
MAC	[H.235] [J.170] Código de autenticación de mensaje (*message authentication code*). Cadena de datos de longitud fija que se envía junto con el mensaje para garantizar su integridad; también se le denomina MIC. [J.170], Control de acceso a medios (*media access control*), y es una subcapa de la capa de enlace de datos que suele funcionar directamente sobre la capa física.
MAF	[M.3010] Función de aplicación de gestión (*management application function*).
MAN	[M.3010] Red de área metropolitana (*metropolitan area network*).
MAPDU	[X.790] Unidad de datos de protocolo de aplicación de gestión (*management application protocol data unit*).
MCU	[H.235] Unidad multidifusión (*multicast unit*) [H.323]. Unidad de control multipunto (*multipoint control unit*).
MD5	[H.235] [J.170] Resumen de mensaje N.º 5 (*message digest No. 5*).
MG	[J.170] Pasarela de medios (*media gateway*).
MGC	[J.170] Controlador de pasarela de medios (*media gateway controller*).
MGCP	[J.170] Protocolo de control de pasarela de medios (*media gateway control protocol*).
MIB	[J.170] [M.3010] Base de información de gestión (*management information base*).
MIS	[M.3010] Servicio de información de gestión (*management information service*).
MO	[M.3010] Objetos gestionados (*managed objects*).
mod n	[T.36] Módulo aritmético que utiliza base n (*module arithmetic using base n*).
MPS	[H.235] Tren de cabida útil múltiple (*multiple payload stream*).
MPx	[T.36] Primitiva mutua de X (*mutual primitive of X*). Número de 16 cifras que solo puede ser generado por X utilizando el algoritmo HKM con primitivas formadas a partir de UINx, UCNx, Idx e Idy.
Mpy	[T.36] Primitiva mutua de Y (*mutual primitive of Y*).
MRP	[H.530] Apoderado de encaminamiento (en un entorno) de movilidad (*mobility routing proxy*).
MS	[M.3210.1] Servicios de gestión (*management services*).
MSB	[J.170] Bit más significativo (*most significant bit*)
MT	[H.530] Terminal móvil (*mobile terminal*), véase la Rec. UIT-T H.510 [6].
MTA	[J.170] Adaptador de terminal de medios (*media terminal adapter*).
NAT	[H.235] Traducción de dirección de red (*network address translation*).
NCS	[J.170] Señalización de llamada de red (*network call signalling*).
NE	[M.3010] [X.790] Elemento de red (*network element*).
NEF	[M.3010] Función de elemento de red (*network element function*).
NEF-MAF	[M.3010] Función de elemento de red – Función de aplicación de gestión *(network element function – management application function*).
NML	[M.3010] [M.3210.1] Capa de gestión de red (*network management layer*).
NOC	[X.790] Centro de explotación de la red (*network operations centre*).
N-OSF	[M.3010] Función de sistema de operaciones – Capa de gestión de red (*network management layer – operations systems function*).
NTP	[H.530] Protocolo de señales horarias de red (*network time protocol*).
O	[M.3010] Facultativo (*optional*).
OA&M	[M.3010] Operación, administración y mantenimiento (*operations, administration and maintenance*).
OAM&P	[SANCHO] Operaciones, administración, mantenimiento y aprovisionamiento (*operations, administration, maintenance & provisioning*).
OCSP	[H.235] Protocolo en línea del estado del certificado (*online certificate status protocol*).

Acrónimo	Definición
ODP	[X.810] Procesamiento distribuido abierto (*open distributed processing*).
OFB	[H.235] Modo realimentación de salida (*output feedback mode*).
OID	[H.235] [H.530] [J.170] [M.3010] Identificador de objeto (*object identifier*).
OS	[M.3010] [X.790] Sistema de operaciones (*operations system*).
OSF	[M.3010] Función de sistema de operaciones (*operations systems function*).
OSF-MAF	[M.3010] Función de sistema de operaciones – Función de aplicación de gestión (*operations systems function – management application function*).
OSI	[M.3010] [X.790] [X.805] [X.810] Interconexión de sistemas abiertos (*open systems interconnection*).
OSS	[J.170] Sistema de soporte de operaciones (*operations systems support*). Software administrativo utilizado para la gestión de configuración, calidad de funcionamiento, fallos, contabilidad, y seguridad.
OT	[T.36] Clave de un solo uso (*one-time key*). Un número que tiene entre 6 y 64 cifras decimales y es fijado de común acuerdo por ambos usuarios.
Otx	[T.36] Clave de un solo uso empleada por primera vez por X en el registro de X' con Y
Oty	[T.36] Clave de un solo uso empleada por primera vez por Y, cuando Y inicia el registro de Y' con X, a fin de completar el registro mutuo, ya sea o no idéntica a Otx.
P(n)	[T.36] Valor de fase (n) (*phase value (n)*).
PBX	[M.3010] Centralita de abonados; centralita privada (*private branch exchange*).
PDU	[H.235] Unidad de datos de protocolo (*protocol data unit*).
PH	[T.36] Troceo (o generación mediante la función *hash*) simple de mensaje (*plain hash of the message)* (24 cifras decimales).
PKCROSS	[J.170] Utiliza PKINIT para establecer las claves "entre ámbitos" y las políticas correspondientes que han de aplicarse para la emisión de tiquetes de servicio a través de ámbitos entre ámbitos y dominios, como soporte de la señalización CMS-a-CMS (CMSS) dentro de un dominio y entre dominios.
PKCS	[H.235] [J.170] [X.509] Normas de criptografía de clave pública (*public key cryptography standards*).
PKI	[H.235] [H.530] [X.509] [J.170] Infraestructura de claves públicas (*public key infrastructure*). Proceso de emisión de certificados de clave pública, que incluye normas, Autoridades de certificación, comunicación entre autoridades y protocolos para los procesos de gestión de la certificación.
PMI	[X.509] Infraestructura de gestión de privilegios (*privilege management infrastructure*).
PRF	[H.235] Función seudoaleatoria (*pseudo-random function*).
Primitive	[T.36] Número compuesto que tiene 64 cifras y que se forma a partir del UIN y del UCN.
procREGxy	[T.36] Procedimiento de registro entre X e Y.
procSTKxy	[T.36] Procedimiento para la transmisión segura de una clave secreta de X a Y.
PRS	[T.36] Secuencia seudoaleatoria (*pseudorandom sequence*).
PTO	[M.3010] Operador público de telecomunicaciones (*public telecommunication operator*).
PTR	[X.790] Informe de dificultades de proveedor (*provider trouble report*).
PVC	[X.805] Circuito virtual permanente (*permanent virtual circuit*).
PW	[H.530] Contraseña de usuario móvil (*mobile user password*).
QA	[M.3010] Adaptador Q (*Q adapter*).
QoS	[SANCHO] Calidad de servicio (*quality of service*).
R	[M.3010] Recurso.
R_1	[H.530] Número aleatorio (*random number*).
RADIUS	[J.170] Servicio de usuario de marcación de autenticación a distancia (*remote authentication dial-in user service*).

Acrónimo	Definición
RBAC	[X.509] Control de acceso basado en las funciones (*role-based access control*).
RC4	[J.170] Cifra de longitud de clave variable ofrecida en el conjunto de cifrado, que se utiliza para criptar el tráfico de medios en IPCablecom.
RCD (o DCN)	[M.3010] Red de comunicación de datos (*data communication network*).
RCN	[T.36] Número criptado registrado (*registered crypt number*). Número de 16 cifras decimales.
RDN	[X.790] Nombre distinguido relativo (*relative distinguished name*).
RDSI (o ISDN)	[M.3010] Red digital de servicios integrados (*integrated services digital network*)
RGT (o TMN)	[M.3010] [M.3210.1] [X.790] Red de gestión de las telecomunicaciones (*telecommunications management network*).
RI (o IN)	[M.3010] Red Inteligente (*intelligent network*).
RIP	[H.530] Petición en curso (*request in progress.*)
RKS	[J.170] Servidor de mantenimiento de registros (*record keeping server*). Dispositivo que colecta y correlaciona los diversos mensajes de evento.
RNCn	[T.36] Número aleatorio no secreto asociado con una SCn (*non-secret random number associated with an SCn*). Número de 4 cifras decimales.
RNIM	[T.36] Número aleatorio no secreto asociado con un IM (*non-secret random number associated with an IM*). Número de 4 cifras decimales.
RNK	[T.36] Número aleatorio no secreto utilizado para proporcionar variaciones de las primitivas generadas a partir de MPx cuando se encripta una SK. Número de 4 cifras decimales.
RNSRn	[T.36] Número aleatorio no secreto asociado con una SRn (*non-secret random number associated with an SRn*). Número de 4 cifras decimales.
RNSSn	[T.36] Número aleatorio no secreto asociado con una SSn. (*non-secret random number associated with an SSn*). Número de 4 cifras decimales.
RPTC (o PSTN)	[SANCHO] Red pública telefónica conmutada (*public switched telephone network*).
RRJ	[H.530] Rechazo de registro (*registration reject*).
RRQ	[H.530] Petición de registro (*registration request*).
RSA	[H.235] [T.30] [T.36] Rivest, Shamir y Adleman (Algoritmo de clave pública).
RSVP	[J.170] Protocolo de reserva de recursos (*resource reservation protocol*).
RTCP	[H.235] [J.170] Protocolo de control de transporte en tiempo real (*realtime transport control protocol*).
RTO	[J.170] Temporizador de retransmission (*retransmission timeout*).
RTP	[H.225.0] [H.235] [J.170] Protocolo en tiempo real (*real time protocol*).
SA	[J.170] Asociación de seguridad (*security association*).
SAFER K-64	[T.36] Rutina segura de criptación rápida (*secure and fast encryption routine*) cuyo algoritmo de clave de 64 bits fue introducido por J. L. Massey en 1993, y que consiste en un cifrado de bloques con iteración, en el que se tienen bloques de 64 bits de texto sin cifrar y cifrado (A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
SCn	[T.36] Clave secreta de petición de identificación, número n (*secret challenge key, number n).* Número de 12 cifras decimales.
SDH	[M.3010] Jerarquía digital síncrona (*synchronous digital hierarchy*).
SDP	[J.170] Protocolo de descripción de sesión (*session description protocol*).
SDU	[H.235] Unidad de datos de servicio (*service data unit*).

Acrónimo	Definición
SG	[J.170] Pasarela de señalización (*signalling gateway*). Agente de señalización que recibe y envía señalización nativa SCN en el borde de la red IP. En particular, la función SG SS7 traduce variantes de la PU-RDSI y el TCAP en una pasarela SS7-Internet en una versión común de PU-RDSI y TCAP.
SH	[T.36] Troceo (o generación mediante función *hash*) simple aleatorizado (*scrambled plain hash*) (24 cifras decimales).
SHA1	[H.235] Algoritmo de generación numérica seguro Nº 1 *(secure hash algorithm No.1*).
SI	[X.810] Información de seguridad (*security information*).
SIP	[J.170] [X.805] Protocolo de inicio de sesión (*session initiation protocol*). Protocolo (de señalización) de control de la capa de aplicación utilizado para crear, modificar, y terminar sesiones con uno o varios participantes.
SIP+	[J.170] Protocolo de inicio de sesión plus (*session initiation protocol plus*). Una extension del SIP.
SK	[T.36] Clave secreta (*secret key*) que puede ser SCn, SRn, SSn, etc. Número de 12 cifras decimales.
SMAPM	[X.790] Máquina de protocolo de aplicación de gestión de sistemas (*system management application protocol machine*).
SMK	[M.3010] Conocimiento de gestión compartido (*shared management knowledge*).
SML	[M.3010] [M.3210.1] Capa de gestión de servicio (*service management layer*).
SMO	[X.790] Visión general de la gestión de sistemas (*systems management overview*).
SMTP	[X.805] Protocolo de transferencia de correo simple (*simple mail transfer protocol*).
SNMP	[J.170] [X.805] Protocolo simple de gestión de red (*simple network management protocol*).
SNTP	[H.530] Protocolo de señales horarias de red simple (*simple network time protocol*).
SOA	[X.509] Fuente de autoridad (*source of authority*).
SONET	[X.805] Red óptica síncrona (*synchronous optical network*).
S-OSF	[M.3010] Función de sistema de operaciones – Capa de gestión de servicios (*service management layer – operations systems function*).
SRn	[T.36] Clave secreta de respuesta, número n (*secret response key, number n*). Número de 12 cifras decimales.
SRTP	[H.225.0] [H.235] Protocolo de transporte en tiempo real seguro (*secure real time protocol*).
SS	[T.36] Clave de sesión secreta (*secret session key*) utilizada con el algoritmo de integridad HFX40-I (12 cifras decimales).
SS7	[J.170] [X.805] Sistema de señalización número 7. Arquitectura y conjunto de protocolos para la señalización de llamada fuera de banda en una red telefónica.
SSK	[T.36] Clave secreta aleatorizada (*scrambled secret key*). Número de 12 cifras decimales.
SSL	[H.235] [X.805] Capa de zocálo segura (*secure socket layer*).
SSn	[T.36] Clave de sesión secreta, número n (*secret session key, number n*), debe utilizarse con el método cifrado y/o la función del operador. Número de 12 cifras decimales.
SSx	[T.36] Clave de sesión secreta generada por X (*secret session key generated by X*) utilizada con el algoritmo de cifrado HFX40 (12 cifras decimales).
TCAP	[J.170] Protocolo de aplicación de capacidad de transacción (*transaction capabilities application protocol).* Protocolo que forma parte de la pila SS7 y que se utiliza en transacciones de bases de datos distantes con un punto de control de señalización.
TD	[J.170] Temporización para desconexión (*timeout for disconnect*).
TF	[M.3010] (Función de transformación (*transformation function*).
TF-MAF	[M.3010] Función de transformación – Función de aplicación de gestión (*transformation function – management application function*).
TFTP	[J.170] Protocolo de transferencia de ficheros trivial (*trivial file transfer protocol*).

Acrónimo	Definición
TGS	[J.170] Servidor que concede tiquete (*ticket granting server*). Subsistema del KDC utilizado para conceder tiquetes Kerberos.
TKx	[T.36] Clave de transferencia (*transfer key*). Criptado de MPx generado por X. Número de 16 cifras decimales.
TLS	[H.235] Seguridad de capa de transporte (*transport level security*).
T_n	[H.530] Indicación de tiempo número n (*timestamp number n*).
TSAP	[H.235] Punto de acceso al servicio de transporte (*transport service access point*).
TSP	[X.790] Prioridad de servicio y de telecomunicaciones (*telecommunication service priority*).
TTP	[X.810] Tercera parte confiable (*trusted third party*).
TTR	[X.790] Informe de dificultades de telecomunicaciones (*telecommunications trouble report*).
UCN	[T.36] Número criptado único (*unique crypt number*), por ejemplo, UCNx, UCNy. Número de 16 cifras decimales conocido sólo por el sistema.
UDP	[J.170] Protocolo de datagrama de usuario (*user datagram protocol*).
UIN	[T.36] Número de identidad único (*unique identity number*), p.ej. UINx, UINy, número de 48 cifras decimales conocido sólo por el sistema.
V-BE	[H.530] BE visitado.
V-GK	[H.530] GK visitado.
VLF	[H.530] Función ubicación del visitante (*visitor location function*).
VoIP	[X.805] Voz por IP (*voice over IP*).
VPN	[X.805] Red privada virtual (*virtual private network*).
W	[H.530] Valor compuesto mediante una combinación aritmética de semiclaves Diffie-Hellman.
WSF	[M.3010] Función de estación de trabajo (*workstation function*).
WSSF	[M.3010] Función de soporte de estación de trabajo (*workstation support function*).
WT	[H.530] ClearToken de movilidad (*mobility cleartoken*).
X	[T.36] Nombre de una entidad.
x	[T.36] Sufijo que implica que algo pertenece o ha sido generado por X.
X<<Y>>	[H.234] Certificado de Y generado por X.
XOR'd	[T.36] [H.235] Operación O (OR) exclusiva.
Xp	[H.234] Clave RSA pública de la entidad X.
Xp[*]	[H.234] Criptado o decriptado de [*] con Xp. En el caso del RSA, se usa exponenciación
Xs	[H.234] Clave RSA secreta de la entidad X.
Xs[*]	[H.234] Criptado o decriptado de [*] con Xs. En el caso del RSA, se usa exponenciación.
XT	[H.530] CryptoToken para autenticación del MT.
Y	[T.36] Nombre de una segunda entidad.
y	[T.36] Sufijo que implica que algo pertenece o ha sido generado por Y.
ZZ	[H.530] Secreto/contraseña compartido del usuario móvil, que se comparte con la AuF correspondiente .
ZZMT	[H.530] Secreto compartido del terminal móvil MT, que se comparte con la AuF correspondiente.
ZZ_n	[H.530] Secreto compartido número n.

A.2 Definiciones relativas a la seguridad que se usan con frecuencia

Término	Definición
Control de acceso	[H.235] [X.800] Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada (X.800). [J.170] Limitación del flujo de información de los recursos de un sistema de una red solamente a personas, programas, procesos u otros recursos de sistema autorizados. [X.805] La dimensión de seguridad control de acceso protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Además, el control de acceso basado en las funciones (RBAC, *role-based access control*) establece varios niveles para restringir el acceso a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones, a las personas y los dispositivos autorizados.
Lista de control de acceso	[X.800] Lista de entidades, con sus derechos de acceso, que están autorizadas a tener acceso a un recurso.
Nodo de acceso	[J.170] Según se utiliza en este documento, un nodo de acceso (AN, *access node*) es un dispositivo de terminación de capa 2 que termina el extremo de red de la conexión del módem de cable. Es específico de la tecnología. En el anexo A/J.112 se denomina adaptador de red interactivo (INA, *interactive network adaptor*) mientras que en el anexo B es el sistema de terminación de módem de cable (CMTS, *cable modem termination system*).
Imputabilidad	[X.800] Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.
Amenaza activa	[X.800] Amenaza de un cambio deliberado y no autorizado del estado del sistema. (Nota – Como ejemplos de amenazas activas relativas a la seguridad cabe citar: la modificación de mensajes, la reproducción de mensajes, la inserción de mensajes espurios, la usurpación de identidad (o impostura) de una entidad autorizada y la negación (o denegación) de servicio).
Agente	[X.790] Como se define en la Rec. UIT-T X.701, la visión general de la gestión de sistemas, pero con la restricción siguiente. Con respecto a un determinado servicio (o recurso) de telecomunicaciones, será posible gestionar el servicio con un sistema que desempeña el cometido de gestor y el otro que desempeña el cometido de agente.
Alias	[X.790] Otro nombre, además del identificador de objeto, por el cual un informe de dificultades puede ser conocido, referenciado o identificado (usualmente por el cliente).
Asociación de aplicación	[X.790] Una relación cooperativa entre dos entidades de aplicación, formada por su intercambio de información de control de protocolo de aplicación mediante su utilización de servicios de presentación.
Contexto de aplicación	[X.790] Un conjunto explícitamente identificado de elementos de servicio de aplicación, opciones conexas y cualquier otra información necesaria para el interfuncionamiento de entidades de aplicación en una asociación de aplicación.
Entidad de aplicación	[X.790] Los aspectos de un proceso de aplicación pertinente a la interconexión de sistemas abiertos.

Término	Definición
Alarmas asociadas	[X.790] Alarmas directamente relacionadas con una dificultad identificada dada.
Algoritmo criptográfico asimétrico	[X.810] Algoritmo para ejecutar el criptado o el decriptado correspondiente, cuyas claves para el criptado y el decriptado son diferentes. (Nota – Con algunos algoritmos criptográficos asimétricos, el decriptado del texto criptado o la generación de una firma digital requiere la utilización de más de una clave privada.)
Ataque	[H.235] Actividades realizadas para obviar los mecanismos de seguridad de un sistema o aprovechar sus deficiencias. Los ataques directos a un sistema aprovechan las deficiencias en los algoritmos, principios o propiedades subyacentes de un mecanismo de seguridad. Los ataques indirectos obvian el mecanismo, o hacen que el sistema utilice el mecanismo incorrectamente.
Atributo	[X.790] Información relativa a un objeto gestionado utilizada para describir (parcial o totalmente) el objeto gestionado. Esta información consiste en un tipo de atributo y su valor (un solo valor) o valores (múltiples valores) de atributo correspondientes.
Autoridad de atributo (AA)	[X.509] Autoridad que asigna privilegios expidiendo certificados de atributo.
Lista de revocación de autoridad de atributo	[X.509] Lista de revocación que contiene una lista de referencias para certificados de atributo expedidos por las AA, que la autoridad expedidora ya no considera válidos.
Certificado de atributo	[X.509] Estructura de datos, firmada digitalmente por una autoridad de atributo, que vincula algunos valores de atributo con información de identificación de su titular.
Lista de revocación de certificado de atributo	[X.509] Lista de revocación que contiene una lista de referencias para certificados de atributo que la autoridad expedidora ya no considera válidos.
Tipo de atributo	[X.790] El componente de un atributo que indica la clase de información dada por ese atributo.
Valor de atributo	[X.790] Un caso particular de la clase de información indicada por un tipo de atributo.
Servidor de audio	[J.170] El servidor de audio reproduce anuncios de información en la red IPCablecom. Los anuncios de los medios son necesarios para las comunicaciones que no se completan y para proporcionar al usuario servicios de información mejorados. Las partes componentes de los servicios de servidor de audio son los reproductores de medios y los controladores de reproductores de medios.
Auditoría	[X.800] Véase "auditoría de seguridad".
Registro de auditoría	[X.800] Véase "registro de auditoría de seguridad".

Término	Definición
Autenticación	[H.235] [X.800] [X.811] Confirmación de que la fuente de los datos recibidos es la alegada. Véanse "autenticación de origen de los datos" y "autenticación de entidad par". Nota – En la presente Recomendación, el término "autenticación" no se utiliza en relación con la integridad de los datos; en su lugar se utiliza el término "integridad de los datos". [J.170] Proceso de verificación de la identidad alegada de una entidad ante otra entidad. [X.805] La dimensión de seguridad autenticación se utiliza para confirmar la identidad de las entidades comunicantes. La autenticación garantiza la validez de la identidad que se atribuyen las entidades de una comunicación (por ejemplo, personas, dispositivos, servicios o aplicaciones) y que una entidad no interviene usurpando una identidad o reproduciendo una comunicación anterior sin autorización.
Intercambio de autenticación	[X.800] Mecanismo destinado a garantizar la identidad de una entidad mediante intercambio de información.
Función de autenticación	[H.530] Entidad funcional de seguridad en el dominio de base que mantiene una relación de seguridad con los usuarios móviles abonados y con los terminales móviles abonados.
Información de autenticación	[X.800] Información utilizada para establecer la validez de una identidad alegada.
Testigo de autenticación; (testigo)	[X.509] Información transportada durante un intercambio de autenticación robusta, que se puede utilizar para autenticar a quien la envió.
Autenticidad	[J.170] Se garantiza que determinada información no ha sido modificada o falsificada, y además que proviene de la entidad que clama su autoría.
Autoridad	[X.509] Entidad responsable de la expedición de certificados. En esta Especificación se definen dos tipos; la autoridad de certificación que expide certificados de clave pública y la autoridad de atributo que expide certificados de atributo.
Certificado de autoridad	[X.509] Certificado expedido a una autoridad (por ejemplo, puede ser a una autoridad de certificación o a una autoridad de atributo).
Autorización	[H.235] Concesión de permisos sobre la base de identificación autenticada. [J.170] Acto de conceder acceso a un servicio o dispositivo cuando se tiene el permiso para utilizarlo. [X.800] Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.
Disponibilidad	[X.800] Propiedad de ser accesible y utilizable a petición por una entidad autorizada.
Disponibilidad	[X.805] La dimensión de seguridad de disponibilidad garantiza que las circunstancias de la red no impiden el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de catástrofe.
CRL básica	[X.509] CRL que se utiliza como base en la generación de una dCRL.
Capa de gestión empresarial	[M.3010] Capa de gestión que tiene la responsabilidad de la totalidad de la empresa y no está sujeta a normalización.
Certificado de CA	[X.509] Certificado para una CA expedido por otra CA.

Término	Definición
Cancelado	[X.790] Un gestor puede pedir al agente que "cancele" un informe de dificultades. El gestor desea abortar este informe de dificultades (porque se presentó erróneamente o porque ya no existe la condición de dificultad). En determinadas condiciones (por ejemplo, la dificultad no ha sido comunicada o probada) el agente "cancelará" el informe de dificultades actualizando su situación a "cerrado a petición del cliente". La "cancelación" de un informe de dificultades puede tener también ramificaciones comerciales fuera del alcance de esta Recomendación (por ejemplo, si el cliente debe pagar por el informe de dificultades).
Capacidad	[X.800] Testigo utilizado como identificador de un recurso de modo que la posesión del testigo confiera derechos de acceso a ese recurso.
Certificado	[H.235] Conjunto de datos relativos a la seguridad emitidos por una autoridad de seguridad o tercero de confianza, junto con información de seguridad que se utiliza para proporcionar los servicios de integridad y autenticación de origen de los datos (Rec. UIT-T X.810). En la presente Recomendación el término se relaciona con certificados de "clave pública" que son valores que representan una clave pública patentada (y otra información facultativa) verificada y firmada por una autoridad de confianza en un formato infalsificable.
Política de certificado	[X.509] Conjunto denominado de reglas que indica la aplicabilidad de un certificado a una determinada comunidad y/o clase de aplicación con requisitos de seguridad comunes. Por ejemplo, una determinada política de certificado pudiera indicar la aplicabilidad de un tipo de certificado a la autenticación de transacciones de intercambio electrónico de datos para el comercio de bienes dentro de una gama de precios dada.
Lista de revocación de certificados	[X.509] Lista firmada que indica un conjunto de certificados que el expedidor de certificados ya no considera válidos. Además del término genérico CRL, se definen algunos tipos de CRL específicos que tratan ámbitos particulares.
Número de serie de certificado	[X.509] Valor entero, único dentro de la autoridad de certificación expedidora, que está asociado inequívocamente con un certificado expedido por dicha autoridad de certificación.
Usuario de certificado	[X.509] Entidad que necesita conocer, con certidumbre, la clave pública de otra entidad.
Validación de certificado	[X.509] Proceso para asegurar que un certificado era válido en un momento determinado, con posible inclusión de la construcción y el procesamiento de un trayecto de certificación, y que asegura que todos los certificados en dicho trayecto eran válidos (es decir, no habían caducado ni estaban revocados) en un determinado momento.
Sistema que utiliza el certificado	[X.509] Implementación de las funciones definidas en esta Especificación de directorio que son utilizadas por un usuario de certificado.
Autoridad de certificación	[X.509] Autoridad a la cual uno o más usuarios han confiado la creación y asignación de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios. [X.810] Una autoridad que es confiable (en el contexto de una política de seguridad) para crear certificados de seguridad que contienen una o más clases de datos pertinentes a la seguridad.
Lista de revocación de autoridad de certificación	[X.509] Lista de revocación que incluye una lista de certificados de claves públicas expedidos a autoridades de certificación, a las que el expedidor del certificado ya no considera válidos.

Término	Definición
Trayecto de certificación	[X.509] Secuencia ordenada de certificados de objetos en el árbol de información de directorio que, junto con la clave pública del objeto inicial en el trayecto, puede ser procesada para obtener la del objeto final en el trayecto.
Canal	[X.800] Trayecto de transferencia de la información.
Cifrado	[H.235] Algoritmo criptográfico, una transformación matemática. [J.170] Algoritmo que transforma los datos entre el texto no criptado y el texto criptado.
Criptoserie o serie criptográfica (Ciphersuite)	[J.170] Un conjunto que debe contener el algoritmo criptado criptográfico y un algoritmo de autenticación de mensaje (por ejemplo, un MAC o un HMAC). En general, puede contener también un algoritmo de gestión de claves, que no se aplica en el contexto de IPCablecom.
Criptograma (o texto criptado)	[X.800] Datos producidos mediante criptado. El contenido semántico de los datos resultantes no está disponible. (Nota – Un criptograma puede ser criptado, de nuevo, para obtener un criptograma supercriptado.)
Solución de informes de dificultades	[X.790] Una afirmación por un agente de que las acciones identificadas en el informe de dificultades u objetos de actividad de reparación han sido ejecutadas satisfactoriamente para resolver la dificultad, o que dichas acciones ya no son necesarias, de modo que en cualquiera de los dos casos el informe de dificultades debe cerrarse.
Texto no criptado (Cleartext)	[X.800] Datos inteligibles, cuyo contenido semántico está disponible.
Cliente	[X.790] Usuario de un servicio proporcionado por un sistema o red.
Liquidación	[X.790] Un informe de dificultades se considera "liquidado" cuando el agente determina que la dificultad informada ha sido resuelta o ya no existe, y el agente actualiza la situación del informe de dificultades para indicar que el informe de dificultades está "liquidado". Solamente un agente puede cambiar la situación de un informe de dificultad a "liquidado". La situación de un informe de dificultades pudiera cambiar a "liquidado a petición del cliente" como resultado de una petición del gestor de cancelar el informe de dificultades.
Cierre de informe de dificultades	[X.790] Una afirmación por un agente de que la dificultad se ha resuelto de modo que el informe de dificultades solucionado sólo puede ser procesado ulteriormente para generar un registro de historial de dificultades y/o para suprimirlo.
Comunicación	[X.805] La dimensión de seguridad de la comunicación garantiza que la información sólo circula entre los puntos extremo autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremo).
Entidad condicionalmente confiable	[X.810] Una entidad que es confiable en el contexto de una política de seguridad, pero que no puede infringir la política de seguridad sin ser detectada.
Confidencialidad	[H.235] Propiedad que impide la revelación de información a individuos, entidades o procesos no autorizados [J.170] Una manera de asegurar que la información sólo es revelada a las partes destinadas y a nadie más. La información esta criptada para proporcionar la confidencialidad. Se denomina también privacidad. [X.800] Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

Término	Definición
Entidad de gestión conforme	[X.790] Un sistema abierto real que sustenta la interfaz interoperable definida en esta Recomendación.
Contacto	[X.790] Persona que puede proporcionar información adicional sobre la dificultad en nombre del gestor o del agente.
Credencial	[H.530] En esta Recomendación, por una credencial [por ejemplo, $HMACZZ(GK_{ID})$ o HMACZZ(W)] ha de entenderse un dato al cual la AuF ha aplicado criptográficamente su secreto compartido *ZZ*, que comparte con el usuario móvil. La credencial se transfiere para probar la autorización y oportunidad en la comprobación de autorización.
Credenciales	[X.800] Datos que se transfieren para establecer la identidad alegada de una entidad.
Punto de distribución de lista de revocación de certificados	[X.509] Asiento de directorio u otra fuente de distribución para las CRL; una CRL distribuida a través de un punto de distribución de CRL puede contener asientos de revocación sólo para un subconjunto del conjunto total de certificados expedidos por una autoridad de certificación o puede contener asientos de revocación para múltiples autoridades de certificación.
Criptoanálisis (o análisis criptográfico)	[J.170] Proceso de recuperar el texto sin criptar de un mensaje o la clave criptográfica sin acceso a la clave. [X.800] Análisis de un sistema criptográfico y/o sus entradas y salidas para deducir variables confidenciales y/o datos sensibles, incluido texto sin criptar.
Algoritmo criptográfico	[H.235] Función matemática que calcula un resultado a partir de uno o varios valores de entrada.
Encadenamiento criptográfico	[X.810] Modo de utilización de un algoritmo criptográfico en el cual la transformación realizada por el algoritmo depende de los valores de las entradas o salidas previas.
Valor de comprobación criptográfico	[X.800] Información que se obtiene realizando una transformación criptográfica (véase criptografía) sobre una unidad de datos. (Nota – El valor de comprobación puede obtenerse en uno o más pasos y es el resultado de una función matemática de la clave y una unidad de datos. Suele utilizarse para verificar la integridad de una unidad de datos.)
Sistema criptográfico, criptosistema	[X.509] Colección de transformaciones de texto sin criptar en texto criptado y viceversa, en la que la transformación o transformaciones que se han de utilizar son seleccionadas por claves. Las transformaciones son definidas normalmente por un algoritmo matemático.
Criptografía	[X.800] Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado. (Nota – La criptografía determina los métodos utilizados en el criptado y decriptado. Un ataque a los principios, medios y métodos criptográficos es criptoanálisis.)

Término	Definición
Cliente	[X.790] Usuario de servicios de telecomunicaciones suministrados por un proveedor de servicios. Particularmente en el contexto de la presente Recomendación, el cliente es cualquiera que elige utilizar la interfaz de interconexión de sistemas abiertos de un sistema de operaciones a otro sistema de operaciones para efectuar la gestión de red a través de jurisdicciones con miras a lograr el control de servicios (o recursos) de telecomunicaciones proporcionados por un proveedor de servicios. El cliente (o el representante del cliente) actúa con el cometido de gestor. No existe un requisito de que la interfaz se limite a casos en los que hay una relación cliente de servicio de telecomunicación tradicional/proveedor de servicio entre las partes. Es posible que dos empresas de telecomunicaciones pudieran utilizar esta interfaz para intercambiar informes de dificultades relativos a la prestación de servicio a un usuario extremo. En ese caso, el cometido de cliente puede cambiar ocasionalmente. Sin embargo, esta relación se puede descomponer en dos relaciones intercambiables gestor-agente.
Red de comunicación de datos	[M.3010] Red de comunicación dentro de una RGT o entre RGT que soportan la función comunicación de datos (DCF).
Confidencialidad de los datos	[X.509] Este servicio se puede utilizar para obtener la protección de los datos frente a buscadores no autorizados. El servicio de confidencialidad de datos está soportado por un marco de autenticación. Se puede utilizar para la protección contra la interceptación de datos. [X.805] La dimensión de seguridad confidencialidad de los datos impide que los datos sean divulgados sin autorización. La confidencialidad garantiza que las entidades no autorizadas no pueden entender el contenido de datos. Los métodos utilizados habitualmente son la criptación, las listas de control de acceso o las autorizaciones de archivos.
Integridad de los datos	[X.800] Confirmación de que los datos no han sido modificados o destruidos por personas no autorizadas. [X.805] La dimensión de seguridad integridad de los datos garantiza la exactitud y la veracidad de los datos. Protege los datos contra acciones no autorizadas de modificación, supresión, creación o duplicación, y señala estas acciones no autorizadas.
Autenticación del origen de los datos	[X.800] Confirmación de que la fuente de los datos recibidos es la alegada.
Descifrado	[X.800] Operación inversa de un criptado reversible correspondiente.
Decriptado	[X.800] Véase descifrado.
Aplazamiento	[X.790] Posponer, o dejar de lado, el trabajo relativo a un informe de dificultades hasta el momento en que se cumplan las condiciones apropiadas y se pueda hacerlo avanzar.
Delegación	[X.509] Envío de un privilegio desde una entidad que tiene dicho privilegio a otra entidad.
Trayecto de delegación	[X.509] Secuencia ordenada de certificados que, junto con la autenticación de una identidad de asertor de privilegios, puede ser procesada para verificar la autenticidad de un privilegio de asertor de privilegios.
Lista de revocación de certificados-delta	[X.509] Lista de revocación de certificados parcial que contiene únicamente asientos para certificados cuyo estado de revocación ha sido modificado después de la expedición de la lista de revocación de certificados básica referenciada.

Término	Definición
Negación (o denegación) de servicio	[X.800] Prevención de acceso autorizado a recursos o retardo deliberado de operaciones críticas desde el punto de vista del tiempo.
Huella dactilar digital	[X.810] Característica de un ítem de datos, por ejemplo un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo (hash) unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea las mismas características.
Firma digital	[X.800] Datos añadidos a una unidad de datos, o transformación criptográfica (véase criptografía) de esta última que permite al destinatario de la unidad de datos probar la fuente y la integridad de la unidad de datos y proteger contra la falsificación (por ejemplo, por el destinatario).
Identificador de distintivo	[X.810] Datos que identifican de manera única a una entidad.
Sentido descendente	[J.170] Sentido que va del extremo de cabecera hacia la ubicación del usuario.
Capa de gestión de elementos	[M.3010] Capa responsable de la gestión de los elementos de red sobre una base individual o de grupo.
Criptado	[H.235] Criptado es el proceso que hace que los datos sean ilegibles para entidades no autorizadas aplicando un algoritmo criptográfico (un algoritmo de criptación). El decriptado es la operación inversa por la cual el texto criptado se transforma en texto sin criptar. [X.800] Transformación criptográfica de datos (véase criptografía) para producir un criptograma o texto criptado. (Nota – El criptado puede ser irreversible, en cuyo caso no puede realizarse el proceso de decriptado correspondiente.)
Criptográfica, criptocifrado (Encryption)	[J.170] Método utilizado para traducir información en texto no criptado a texto criptado (criptograma). [X.800] Véase criptado.
Entidad final	[X.509] Sujeto del certificado que utiliza su clave privada para otros fines distintos que firmar certificados o entidad que es una parte confiante.
Lista de revocación de certificados de atributo de entidad final	[X.509] Lista de revocación que contiene una lista de certificados de atributo expedida a los titulares que no sean también autoridades de atributo, que el expedidor de certificados ya no considera válidos.
Lista de revocación de certificados de clave pública de entidad final	[X.509] Lista de revocación que contiene una lista de certificados de clave pública, expedidos a sujetos que no sean también autoridades de certificación, que el expedidor de certificados ya no considera válidos.
Punto extremo	[J.170] Un terminal, una pasarela o una MCU.
Criptado de extremo a extremo	[X.800] Criptado de datos en el interior o en el sistema extremo fuente, cuyo decriptado correspondiente se produce sólo en el interior o en el sistema extremo de destino (véase también "criptado enlace por enlace").
Variables ambientales (o de entorno)	[X.509] Aquellos aspectos de política necesarios para una decisión de autorización, que no estén contenidos en estructuras estáticas, pero de los que un verificador de privilegios disponga mediante algún medio local (por ejemplo, hora del día o balance de cuentas corrientes).
Escalada de un informe de dificultades	[X.790] Identificación de un informe de dificultades que ha de recibir atención de supervisión urgente e inmediata para resolver la dificultad.

Término	Definición
Evento	[X.790] Una ocurrencia instantánea que cambia la situación global de un objeto. Este cambio de situación puede ser persistente o temporal, teniendo así en cuenta la funcionalidad de vigilancia, supervisión y medición de la calidad de funcionamiento, etc. Los eventos pueden generar o no informes, pueden ser espontáneos o planificados, pueden activar otros eventos o pueden ser activados por otro u otros eventos.
Mensaje de evento	[J.170] Mensaje que recoge una sola porción de una conexión.
Interfaz F	[M.3010] Interfaz aplicada en los puntos de referencia f.
Punto de referencia f	[M.3010] Punto de referencia ubicado entre el bloque función de estación de trabajo (WSF) y el bloque función del sistema de operaciones (OSF).
Gestión de averías	[X.790] Consiste en un conjunto de funciones que permiten la detección, aislamiento y corrección del funcionamiento anormal de la red de telecomunicaciones y su entorno.
Lista de revocación de certificados completa	[X.509] Lista de revocación completa que contiene asientos para todos los certificados que han sido revocados en un ámbito determinado.
Bloque de función	[M.3010] La unidad (desplegable) más pequeña de la funcionalidad de gestión de la RGT que está sujeta a normalización.
Punto de referencia g	[M.3010] Punto de referencia situado fuera de la RGT entre los usuarios humanos y el bloque de función de estación de trabajo (WSF). No son considerados parte de la RGT, aun cuando transportan información de la RGT.
Pasarela	[J.170] Dispositivos que establecen un puente entre el mundo de la comunicación vocal de IPCablecom y la red telefónica pública conmutada (RTPC). Los ejemplos son la pasarela de medios, que proporciona las interfaces de circuitos portadores a la RTPC y transcodifica el tren de medios, y la pasarela de señalización, que envía y recibe señalización de la red con conmutación de circuitos al borde de la red IPCablecom.
Función Hash ("de troceo" o función de cálculo de clave)	[X.509] Función (matemática) que hace corresponder valores de un dominio grande (posiblemente muy grande) con una gama más pequeña. La función de troceo es "buena" cuando los resultados de la aplicación de la función a un (gran) conjunto de valores en el dominio se distribuyen uniformemente (y aparentemente al azar) en la gama. [X.810] Función (matemática) que hace corresponder los valores de un conjunto de valores grande (posiblemente muy grande) en una gama de valores más pequeña.
Encabezamiento	[J.170] Información de control de protocolo colocada al principio de una unidad de datos de protocolo.
Titular	[X.509] Entidad a la que se ha delegado algún privilegio ya sea directamente a partir de la fuente de autoridad o indirectamente a través de otra autoridad de atributo.
Elemento de frontera de base (o propio)	[H.530] Elemento de frontera (BE) situado dentro del dominio de base (o propio).
Política de seguridad basada en la identidad	[X.800] Política de seguridad basada en las identidades y/o atributos de los usuarios, de un grupo de usuarios o entidades que actúan en nombre de los usuarios y en los recursos/objetos a que se accede.
Lista de revocación de certificados indirecta	[X.509] Lista de revocación que contiene por lo menos información de revocación sobre certificados expedidos por autoridades distintas de la que expidió esta lista de revocación de certificados.

Término	Definición
Integridad	[H.235] Propiedad de que los datos no han sido alterados de una manera no autorizada. [J.170] Con ella se garantiza que nadie haya modificado la información, excepto por aquellas personas autorizadas. [X.800] Véase integridad de datos.
Interfaz	[M.3010] Concepto de arquitectura que proporciona interconexión entre bloques físicos y puntos de referencia.
Jurisdicción	[X.790] Se refiere a la separación funcional de redes de telecomunicaciones. Una jurisdicción es uno de los cuatro tipos siguientes: a) Red de operador de central local. b) Red de operador entre centrales. c) Red de usuario final. d) Alguna combinación de las anteriores.
Kerberos	[J.170] Un protocolo de autenticación de red de clave secreta que utiliza una opción de algoritmos criptográficos para la criptación y una base de datos de claves centralizada para la autenticación.
Clave	[J.170] Valor matemático introducido en el algoritmo criptográfico seleccionado. [X.800] Secuencia de símbolos que controla las operaciones de criptado y decriptado.
Acuerdo de clave	[X.509] Método para negociar un valor de clave en línea sin transferir la clave, incluso en forma criptada, por ejemplo, la técnica de Diffie-Hellman (para más información sobre los mecanismos de acuerdos de clave, véase ISO/CEI 11770-1).
Intercambio de claves	[J.170] Trueque de claves públicas entre entidades que serán utilizadas para criptar comunicaciones entre las entidades.
Gestión de claves	[H.235] [X.800] Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad.
Gestión de claves	[J.170] Proceso de distribución de claves simétricas compartidas necesarias para ejecutar un protocolo de seguridad.
Criptado enlace por enlace	[X.800] Aplicación individual del criptado a datos en cada enlace de un sistema de comunicación. (Véase también "criptado de extremo a extremo".) (Nota – El criptado enlace por enlace entraña que los datos estén en forma de texto no criptado en las entidades relevadoras.)
Arquitectura lógica por capas	[M.3010] Concepto arquitectural que organiza las funciones de gestión en un agrupamiento de capas de gestión y describe la relación entre las capas.
Punto de referencia m	[M.3010] Punto de referencia situado fuera de la RGT entre el bloque de función de adaptador Q (QAF) y entidades gestionadas no conformes a las Recomendaciones sobre la RGT.
Recurso gestionado	[M.3010] Abstracción de los aspectos de un recurso de telecomunicaciones (lógico o físico) requerido para la gestión de telecomunicaciones.
Función de aplicación de gestión	[M.3010] Función que representa una parte de la funcionalidad de uno o varios servicios de gestión.
Dominio de gestión	[M.3010] Conjunto de recursos gestionados sujetos a una política de gestión común.
Función de gestión	[M.3010] La parte más pequeña de un servicio de gestión percibido por el usuario del servicio.

Término	Definición
Conjunto de funciones de gestión	[M.3010] Agrupamiento de funciones de gestión de la RGT que pertenecen al mismo contexto, es decir, están relacionadas a una capacidad de gestión específica (por ejemplo, funciones señaladoras de alarma, control de la gestión del tráfico). El conjunto de funciones de gestión de la RGT es el elemento de especificación funcional reutilizable más pequeño. Debe ser considerado como un todo. Es similar a la parte requisitos de la función de gestión de sistema (SMF) de la interconexión de sistemas abiertos (OSI).
Servicio de gestión	[M.3010] Servicio que satisface las necesidades de gestión de telecomunicaciones específicas.
Capa de gestión	[M.3010] Concepto arquitectural que refleja aspectos particulares de la gestión e implica el agrupamiento de información de gestión relativa a ese aspecto.
Gestor	[X.790] Como se define en la Rec. UIT-T X.701, la visión general de la gestión de sistemas, pero con la siguiente restricción. Con respecto a un determinado servicio (o recurso) de telecomunicaciones, será posible gestionar el servicio con un sistema que desempeña el cometido de gestor y el otro que desempeña el cometido de agente.
Detección de manipulación	[X.800] Mecanismo que se utiliza para detectar si una unidad de datos ha sido modificada, sea accidental o intencionalmente.
Usurpación de identidad (o impostura)	[X.800] Cuando una entidad pretende pasar por una entidad diferente.
Tren de medios	[H.235] Un tren de medios puede ser del tipo audio, vídeo o datos, o una combinación de cualquiera de ellos. Los datos de trenes de medios transportan datos de usuario o de aplicación (cabida útil) pero no datos de control.
Apoderado de encaminamiento (en un entorno) de movilidad (MRP)	[H.530] Entidad funcional facultativa que actúa como una entidad funcional intermedia, terminando la asociación de seguridad de un enlace salto por salto.
Elemento de red	[M.3010] Concepto arquitectural que representa el equipo de telecomunicaciones (o grupos/partes del equipo de telecomunicaciones) y soporta el equipo o cualquier ítem o grupos de ítems que se considera que pertenecen al entorno de telecomunicaciones y que llevan a cabo funciones de elemento de red (NEF).
Función de elemento de red	[M.3010] Bloque de funciones que representa las funciones de telecomunicación y que se comunica con el bloque de función OSF de la RGT con el objeto de ser supervisado y/o controlado.
Capa de gestión de red	[M.3010] Capa que tiene la responsabilidad de la gestión, incluida la coordinación de actividad, desde el punto de vista de la red.

Término	Definición
No repudio	[H.235] Protección contra la negación de servicio por una de las entidades que participa en una comunicación o que ha participado en toda la comunicación o parte de ésta. [J.170] Capacidad de evitar que un remitente niegue más tarde haber enviado un mensaje o ejecutado una acción. [X.805] La dimensión de seguridad no repudio evita que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red (por ejemplo, de obligación, de intención o de compromiso; prueba de origen de los datos; prueba de propiedad; prueba de utilización del recurso). Garantiza la disponibilidad de pruebas que pueden presentarse a terceros y utilizarse para demostrar que un determinado evento o acción si ha tenido lugar.
Notarización	[X.800] Registro de datos por un tercero de confianza que permite la ulterior seguridad de la exactitud de sus características, tales como contenido, origen, fecha, entrega.
Método objeto	[X.509] Acción que puede ser invocada en un recurso (por ejemplo, un sistema de archivos puede haber leído, escrito, ejecutado métodos objeto).
Función unidireccional	[X.509] Función (matemática) f que es fácil de calcular, pero que para un valor y en la gama es difícil de calcular para hallar un valor x en el dominio de modo que f(x) = y. Puede haber unos pocos valores y para los cuales hallar x no sea difícil computacionalmente. [X.810] Función (matemática) cuyo cálculo es difícil pero que, cuando se conoce un resultado, no es factible, mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrados para obtenerlo.
Función hash (o de cálculo de clave) unidireccional	[X.810] Función (matemática) que es a la vez una función unidireccional y una función de cálculo de clave (hash).
Sistema de operaciones	[M.3010] Bloque físico que lleva a cabo funciones del sistema de operaciones (OSF).
Función del sistema de operaciones	[M.3010] Bloque de funciones que procesa la información relacionada con la gestión de las telecomunicaciones con el objeto de supervisar/coordinar y/o controlar las funciones de telecomunicación que incluyen funciones de gestión (es decir la misma RGT).
Interrupción	[X.790] Indisponibilidad de un servicio o recurso.
Amenaza pasiva	[X.800] Amenaza de revelación de la información no autorizada sin modificar el estado del sistema.
Contraseña	[H.530] [X.800] Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres.
Autenticación de entidad par	[X.800] Corroboración de que una entidad par en una asociación es la pretendida.
Gravedad percibida	[X.790] La gravedad del problema vista por la persona que informa de la dificultad.
Bloque físico	[M.3010] Concepto arquitectural que representa la realización de uno o más bloques de función.
Seguridad física	[X.800] Medidas adoptadas para proporcionar la protección física de los recursos contra amenazas deliberadas o accidentales.
Política	[X.800] Véase política de seguridad.

Término	Definición
Correspondencia de políticas	[X.509] Reconocimiento de que, cuando una autoridad de certificación en un dominio certifica a una autoridad de certificación en otro dominio, una determinada política de certificación en el segundo dominio puede ser considerada por la autoridad del primer dominio como equivalente (pero no necesariamente idéntica en todos los aspectos) a una determinada política de certificado en el primer dominio.
Prioridad	[X.790] El grado de urgencia que manifiesta el gestor para que se solucione el problema.
Privacidad	[H.235] Modo de comunicación en el cual sólo las partes habilitadas explícitamente pueden interpretar la comunicación. Esto se logra en general mediante criptación y claves compartidas para el criptado. [J.170] Una manera de asegurar que la información sólo es revelada a las partes destinadas y a nadie más. Normalmente la información es criptada para proporcionar la confidencialidad. Se denomina también confidencialidad. [X.800] Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada. (Nota – Como este término se relaciona con el derecho de las personas, no puede ser muy preciso y su uso debe evitarse, salvo como un motivo para exigir seguridad.) [X.805] La dimensión de seguridad privacidad protege la información que sería posible conocer observando las actividades de la red. Por ejemplo: los sitios web visitados por un usuario, la posición geográfica del usuario y las direcciones IP y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio.
Canal privado	[H.235] En la presente Recomendación, un canal privado es el resultante de negociación previa por un canal seguro. En este contexto, puede ser utilizado para manipular trenes de medios.
Clave privada	[J.170] Clave utilizada en la criptografía de claves públicas que pertenece a una entidad y se debe mantener secreta. [X.810] Clave que se utiliza con un algoritmo criptográfico asimétrico y cuya posesión está restringida (usualmente a una sola entidad).
Clave privada; clave secreta (término desaconsejado)	[X.509] (En un criptosistema de claves públicas) clave de un par de claves de usuario que sólo es conocida por ese usuario.
Privilegio	[X.509] Atributo o propiedad asignado a una entidad por una autoridad.
Asertor de privilegios	[X.509] Titular de un privilegio que utiliza su certificado de atributo o su certificado de clave pública para aseverar un privilegio.
Infraestructura de gestión de privilegios (PMI)	[X.509] Infraestructura capaz de soportar la gestión de privilegios como soporte de un servicio de autorización completo y en relación con una infraestructura de claves públicas.
Política de privilegios	[X.509] Política que destaca condiciones para los verificadores de privilegios con el fin de proporcionar o realizar servicios relacionados con asertores de privilegios cualificados. La política de privilegios relaciona atributos asociados con el servicio, así como atributos asociados con asertores de privilegios.
Verificador de privilegios	[X.509] Entidad que verifica certificados a partir de una política de privilegios.
Apoderado	[J.170] Facilidad que proporciona indirectamente algún servicio o que actúa como un representante para entregar información, evitando así que un anfitrión tenga que sustentar el servicio.

Término	Definición
Clave pública	[J.170] Clave utilizada en la criptografía de claves públicas que pertenece a una entidad particular y es distribuida públicamente. Otras entidades utilizan esta clave para criptar datos que han de ser enviados al propietario de la clave [X.810]. Clave que se utiliza con un algoritmo criptográfico asimétrico y que se puede poner a disposición del público.
Certificado de clave pública	[J.170] Vinculación entre la clave pública de una entidad y uno o más atributos relacionados con su identidad, se denomina también un certificado digital.
Criptografía de clave pública	[H.235] Sistema de criptación que utiliza claves asimétricas (para criptación/decriptación) en el cual las claves tienen una relación matemática entre sí, que no puede ser calculada razonablemente. [J.170] Procedimiento que utiliza un par de claves, una clave pública y una clave privada para criptación y decriptación, y que se denomina también algoritmo asimétrico. La clave pública de un usuario está disponible públicamente para que otros usuarios la utilicen con el fin de enviar un mensaje al propietario de la clave. La clave privada de un usuario se mantiene secreta y es la única clave que puede decriptar mensajes enviados criptados por la clave pública de los usuarios.
Infraestructura de claves públicas (PKI)	[X.509] Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio.
Operador público de telecomunicaciones (PTO)	[M.3010] Término que incluye a las administraciones de telecomunicación, empresas de explotación reconocidas, administraciones privadas (cliente y terceras partes) y otras organizaciones que operan o utilizan una red de gestión de las telecomunicaciones (RGT).
Clave pública	[X.509] (En un critposistema de claves públicas) clave de un par de claves de usuario que es conocida públicamente.
Certificado de clave pública	[X.509] Clave pública de un usuario, junto con alguna otra información, hecha infalsificable por criptado con la clave privada de la autoridad de certificación que la emitió.
Adaptador Q	[M.3010] Bloque físico que se caracteriza por un bloque de función de adaptador Q contenido y que conecta entidades físicas semejantes a NE y a OS que no proporcionan interfaces RGT compatibles (en los puntos de referencia m) a interfaces Q.
Interfaz Q	[M.3010] Interfaz aplicada en los puntos de referencia q.
Punto de referencia q	[M.3010] Punto de referencia ubicado entre NEF y OSF, entre QAF y OSF, y entre OSF y OSF.
Punto de referencia	[M.3010] Concepto arquitectural utilizado para delinear bloques de función de gestión y que definen una frontera de servicio entre dos bloques de función de gestión.
Parte confiante	[X.509] Usuario o agente que se fía de los datos de un certificado al tomar decisiones.
Repudio	[X.800] Negación de una de las entidades implicadas en una comunicación de haber participado en toda la comunicación o en parte de ella.
Certificado de revocación	[X.810] Certificado de seguridad expedido por una autoridad de seguridad para indicar que un determinado certificado de seguridad ha sido revocado.
Certificado de lista de revocaciones	[X.810] Certificado de seguridad que contiene una lista de certificados de seguridad que han sido revocados.
Certificado de asignación de cometido	[X.509] Certificado que contiene el atributo de cometido y asigna uno o más cometidos al sujeto/titular del certificado.

Término	Definición
Certificado de especificación de cometido	[X.509] Certificado que contiene la asignación de privilegios a un cometido.
Clave privada raíz	[J.170] La clave de signatura privada de la autoridad de certificación de nivel más alto. Se utiliza normalmente para firmar certificados de clave pública para autoridades de certificación de nivel más bajo u otras entidades.
Control de encaminamiento	[X.800] Aplicación de reglas durante el proceso de encaminamiento con el fin de elegir o evitar redes, enlaces o relevadores específicos.
Política de seguridad basada en reglas	[X.800] Política de seguridad basada en reglas globales impuestas a todos los usuarios. Estas reglas suelen depender de una comparación de la sensibilidad de los recursos a los que se accede y la posesión de los atributos correspondientes de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios.
Sello	[X.810] Valor de comprobación criptográfico que sustenta la integridad pero que no protege contra falsificaciones hechas por el destinatario (es decir, no proporciona servicios de no repudio). Cuando un sello está asociado con un elemento de datos, se dice que el elemento de datos está *sellado*. (Nota – Aunque un sello por sí mismo no proporciona el servicio de no repudio, algunos mecanismos de no repudio utilizan el servicio de integridad proporcionado por los sellos, por ejemplo, para proteger las comunicaciones con terceras partes confiables.)
Clave secreta	[X.810] Clave que se utiliza con un algoritmo criptográfico simétrico. La posesión de una clave secreta está restringida (usualmente a dos entidades).
Reglas de interacción de seguridad	[X.810] Reglas de política de seguridad que reglamentan las interacciones entre dominios de seguridad.
Administrador de seguridad	[X.810] Persona que es responsable de la definición o aplicación de una o más partes de una política de seguridad.
Auditoría de seguridad	[X.800] Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.
Registro de auditoría de seguridad	[X.800] Datos recogidos que posiblemente pueden usarse para efectuar una auditoría de seguridad.
Autoridad de seguridad	[X.810] Entidad que es responsable de la definición, aplicación o cumplimiento de la política de seguridad.
Certificado de seguridad	[X.810] Conjunto de datos pertinentes a la seguridad expedida por una autoridad de seguridad o tercera parte confiable, junto con información de seguridad que se utiliza para proporcionar servicios de integridad y autenticación de origen de los datos para los datos. (Nota – Se considera que todos los certificados son certificados de seguridad (véanse las definiciones pertinentes en ISO 7498-2.) Se adopta el término *certificado de seguridad* para evitar conflictos de terminología con la Rec. UIT-T X.509 | ISO/CEI 9594-8 (es decir, la norma de autenticación del directorio).

Término	Definición
Cadena de certificados de seguridad	[X.810] Secuencia ordenada de certificados de seguridad, en la cual el primer certificado de seguridad contiene información pertinente a la seguridad y cada certificado de seguridad subsiguiente contiene información de seguridad que se puede utilizar para verificar certificados de seguridad previos.
Dominio de seguridad	[X.810] Un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad, donde el conjunto de elementos está sujeto a la política de seguridad, para las actividades especificadas y la política de seguridad es administrada por la autoridad de seguridad para el dominio de seguridad.
Autoridad de dominio de seguridad	[X.810] Autoridad de seguridad que es responsable de la aplicación de una política de seguridad para un dominio de seguridad.
Información de seguridad	[X.810] Información necesaria para prestar los servicios de seguridad.
Etiqueta de seguridad	[X.800] Marca vinculada a un recurso (que puede ser una unidad de datos) que denomina o designa los atributos de seguridad de dicho recurso. (Nota – La marca y/o vinculación puede ser explícita o implícita.)
Política de seguridad	[X.509] Conjunto de reglas establecidas por la autoridad de seguridad que rigen la utilización y prestación de servicios y facilidades de seguridad. [X.800] Conjunto de criterios para la prestación de servicios de seguridad (véanse también "política de seguridad basada en la identidad" y "política de seguridad basada en reglas"). (Nota – Una política de seguridad completa tratará necesariamente muchos aspectos que están fuera del ámbito de OSI.)
Reglas de política de seguridad	[X.810] Una representación de una política de seguridad para un dominio de seguridad dentro de un sistema real.
Perfil de seguridad	[H.235] Conjunto (subconjunto) de características y procedimientos coherentes y con capacidad de interfuncionamiento entre sí que caen fuera del alcance de la Rec. UIT-T H.235 y que son útiles para proporcionar seguridad a las comunicaciones multimedios H.323 entre las entidades involucradas en un escenario específico.
Restablecimiento de seguridad	[X.810] Acciones que se ejecutan y procedimientos que se aplican cuando se detecta o se sospecha que se ha producido una infracción de la seguridad.
Servicio de seguridad	[X.800] Servicio proporcionado por una capa de sistemas abiertos de comunicación, que garantiza la seguridad adecuada de los sistemas y de la transferencia de datos.
Testigo de seguridad	[X.810] Conjunto de datos protegido por uno o más servicios de seguridad, junto con la información de seguridad utilizada para prestar esos servicios de seguridad, que se transfiere entre entidades comunicantes.
Protección selectiva de los campos	[X.800] Protección de ciertos campos específicos dentro de un mensaje que ha de transmitirse.
Sensibilidad	[X.509] Característica de un recurso que presupone su valor o importancia. [X.800] Característica de un recurso relativa a su valor o importancia y eventualmente a su vulnerabilidad.

Término	Definición
Servicio	[X.790] Este término representa capacidades de telecomunicaciones que el cliente compra o arrienda a un proveedor de servicio. El servicio es una abstracción del examen del elemento de red o del equipo. Servicios idénticos pueden ser proporcionados por diferentes elementos de red y servicios diferentes pueden ser proporcionados por los mismos elementos de red.
Capa de gestión de servicios	[M.3010] Capa de gestión que tiene que ver con los aspectos contractuales, incluidos el tratamiento de los pedidos de servicio, las quejas y la facturación, de los servicios que se suministran a los clientes o están disponibles para nuevos clientes potenciales, y es responsable de los mismos.
Proveedor de servicio	[X.790] Un sistema o una red que proporciona el servicio a un cliente. El proveedor de servicio es cualquiera que ofrece la interfaz de interconexión de sistema abiertos entre sistemas de operaciones (OS) para permitir a un usuario la gestión de red a través de jurisdicciones para controlar los servicios (o recursos) de telecomunicaciones que se proporcionan. El proveedor de servicio actúa con el cometido de agente. Véase *cliente*. No hay un requisito de que la interfaz esté limitada a los casos en que hay una relación cliente de servicio de telecomunicaciones tradicional/proveedor de servicio de telecomunicaciones entre las partes. Éste es ciertamente el caso cuando dos empresas de telecomunicaciones, cuyas redes interfuncionan a fin de prestar un servicio de telecomunicaciones, a un usuariuo extremo, pudieran utilizar esta interfaz. En ese caso, el cometido de cliente y proveedor de servicio puede cambiar ocasionalmente. Sin embargo, esta relación se puede descomponer en dos relaciones de gestor-agente.
Relación de servicio	[H.530] Asociación de seguridad establecida entre dos entidades funcionales en el supuesto de que está presente al menos una clave compartida.
Secreto compartido	[H.530] Clave de seguridad para los algoritmos cripotográficos; se puede derivar de una contraseña.
Firma	[X.800] Véase firma digital.
Autenticación simple	[X.509] Autenticación por medio de arreglos de contraseñas simples.
Fuente de autoridad	[X.509] Autoridad de atributo en la que confía un verificador de privilegios para un recurso determinado como la autoridad última para asignar un conjunto de privilegios.
Inundación (Spamming)	[H.235] Ataque de denegación de servicio que tiene lugar cuando se envían datos no autorizados en exceso a un sistema. Un caso especial es la inundación de medios que se produce cuando se envían paquetes RTP por puertos UDP. Normalmente el sistema es inundado con paquetes; su procesamiento consume recursos valiosos del sistema.
Situación de un informe de dificultades	[X.790] La etapa que ha sido alcanzada por un informe de dificultades desde su creación mientras la dificultad se está resolviendo.
Autenticación fuerte	[X.509] Autenticación por medio de credenciales derivadas criptográficamente.
Algoritmo criptográfico simétrico (basado en claves secretas)	[H.235] Un algoritmo para realizar el criptado o el algoritmo correspondiente para realizar el decriptado en el cual se requiere la misma clave para ambas operaciones (Rec. UIT-T X.810).

Término	Definición
Algoritmo criptográfico simétrico	[X.810] Algoritmo para realizar el criptado o el algoritmo correspondiente para realizar el decriptado en el cual se requiere la misma clave para el criptado y el decriptado.
Red de gestión de las telecomunicaciones	[M.3010] Arquitectura para la gestión, que incluye la planificación, prestación, instalación, mantenimiento, operación y administración de redes, equipos y servicios de telecomunicaciones.
Amenaza	[H.235] Violación potencial de la seguridad (X.800).
Sello de tiempo	[X.790] Un valor de tiempo utilizado para indicar cuándo se produjo una determinada actividad, acción, o evento.
Análisis del tráfico	[X.800] Inferencia de información a partir de la observación de flujos de tráfico (presencia, ausencia, cantidad, sentido y frecuencia).
Confidencialidad del flujo de tráfico	[X.800] Servicio de confidencialidad que ofrece protección contra el análisis de tráfico.
Relleno de tráfico	[X.800] Generación de instancias de comunicación espurias, de unidades de datos/o datos espurios en las unidades de datos.
Función de transformación	[M.3010] Bloque de función que traduce la información disponible entre un punto de referencia de la RGT y un punto de referencia no RGT (sea de dominio privado o normalizado). La parte no RGT de este bloque de función está fuera de la frontera de la RGT.
Dificultad	[X.790] Cualquier causa que puede conducir o contribuir a que un gestor perciba una degradación de la calidad de servicio de uno o más servicios de red o de uno o más recursos de red que son gestionados.
Administración de dificultades	[X.790] Conjunto de funciones que permite informar sobre las dificultades y seguir su evolución. Los servicios de administración de dificultades incluyen el formato de petición de informe de dificultades, la introducción del informe de dificultades, la adición de información de dificultades, la cancelación del informe de dificultades, la petición de la situación del informe de dificultades, el examen del historial de dificultades, la notificación de cambio de valor de atributo (por ejemplo, situación del informe de dificultades/tiempo de ejecución), la creación/supresión de objetos (informe de dificultades), la verificación de la conclusión de la reparación de la dificultad y la modificación de la información de administración de dificultades.
Anotación de historial de dificultades	[X.790] Una anotación de información seleccionada de un informe de dificultades que se mantiene con fines históricos después que se cierra el informe de dificultades.
Gestión de dificultades	[X.790] El informe y el seguimiento de la dificultad entre entidades de gestión conformes que interfuncionan cooperativamente para resolver un problema. (No se hace distinción entre interfaces entre jurisdicciones o dentro de jurisdicciones).
Informe de dificultades	[X.790] El acto de comunicar que se ha detectado una dificultad de modo que se pueda utilizar la gestión de dificultades para resolverla.
Solución de dificultades	[X.790] Es el proceso de diagnóstico y la acción de reparación requeridos para resolver un problema. Comprende el proceso de asignar elementos de trabajo específicos o responsabilidad general para solucionar y cerrar el informe de dificultades.
Seguimiento de dificultades	[X.790] La capacidad de seguir el curso de un informe de dificultades desde su creación hasta su cierre.
Tipo de dificultad	[X.790] La descripción o categoría de la dificultad detectada.

Término	Definición
Fiduciario (de confianza)	[X.509] En general, se puede decir que una entidad acepta como "fiduciaria" a una segunda entidad cuando aquella (la primera entidad) supone que la segunda entidad se comportará exactamente como ella lo espera. Esta relación de confianza se puede aplicar solamente para alguna función específica. El cometido principal de la confianza en el marco de la autenticación es describir la relación entre una entidad autenticadora y una entidad de certificación; una entidad autenticadora tendrá que estar segura de que puede confiar en que la autoridad de certificación crea solamente certificados válidos y fiables. [X.810] Se dice que la entidad X *confía* en la entidad Y para un conjunto de actividades solamente si la entidad X puede confiar en que la entidad Y se comporta de una manera particular con respecto a las actividades.
Entidad fiable	[X.810] Entidad que puede infringir una política de seguridad, ya sea porque ejecuta acciones indebidas o porque no ejecuta las acciones debidas.
Funcionalidad fiable	[X.800] Funcionalidad percibida como correcta con respecto a algunos criterios, por ejemplo, los establecidos por una política de seguridad.
Tercera parte fiable	[X.810] Autoridad de seguridad o su agente en el que se confía con respecto a algunas actividades pertinentes a la seguridad (en el contexto de una política de seguridad).
Entidad incondicionalmente fiable	[X.810] Entidad fiable que puede infringir una política de seguridad sin ser detectada.
Usuario	[M.3010] Persona o proceso que aplica servicios de gestión con el objeto de satisfacer operaciones de gestión.
Elemento de frontera visitado	[H.530] Elemento de frontera (BE) situado dentro del dominio visitado.
Estación de trabajo	[M.3010] Bloque físico que efectúa funciones de estación de trabajo (WSF).
Función de estación de trabajo	[M.3010] Bloque de función que interpreta la información de la RGT para el usuario humano, y viceversa.
Interfaz X	[M.3010] Interfaz aplicada en puntos de referencia x.
Punto de referencia x	[M.3010] Punto de referencia ubicado entre bloques de función OSF en diferentes RGT. (Nota – Las entidades ubicadas más allá del punto de referencia x pueden ser parte de una RGT efectiva (OSF) o parte de un entorno no RGT (semejante a OSF). Esta clasificación no es visible en el punto de referencia x.)
Certificado X.509	[J.170] Especificación de certificado de una clave pública elaborado como parte de las normas de directorio de la Rec. UIT-T X.500.

A.3 Otras fuentes terminológicas del UIT-T

En la base de datos en línea SANCHO (*Sector Abbreviations and defiNitions for a TeleCommunications tHesaurus Oriented*) se encuentran términos y definiciones, y abreviaturas y acrónimos, en inglés, francés y español, provenientes de las publicaciones del UIT-T. Se trata de un recurso gratuito al que se puede acceder a través de www.itu.int/sancho y también de una versión en CD-ROM que se actualiza regularmente. Todos los términos y definiciones citados en esta cláusula se pueden encontrar en SANCHO junto con la lista de Recomendaciones del UIT-T donde se los define.

La CE 17 del UIT-T desarrolló un Compendio de definiciones de seguridad utilizadas en las Recomendaciones del UIT-T. Este documento se encuentra en:
www.itu.int/ITU-T/studygroups/com17/cssecurity.html

Anexo B: Catálogo de Recomendaciones UIT-T relacionadas con la seguridad

B.1 Aspectos de seguridad que se tratan en este manual

F.400 *Visión de conjunto del sistema y del servicio de tratamiento de mensajes*

Esta Recomendación proporciona una visión de conjunto útil para definir globalmente el sistema y servicio de tratamiento de mensajes (MHS) y a su vez constituye una visión general del MHS. La presente visión de conjunto forma parte de un conjunto de Recomendaciones que describe el modelo del sistema de tratamiento de mensajes (MHS, *message handling system*) y sus elementos de servicio. En ella se pasa revista a las capacidades de un MHS que utilizan los proveedores de servicios para prestar servicios públicos de tratamiento de mensajes (MH, *message handling*) que permiten a los usuarios intercambiar mensajes con almacenamiento y retransmisión. El sistema de tratamiento de mensajes está diseñado de acuerdo con los principios del modelo de referencia de interconexión de sistemas abiertos (modelo de referencia OSI) para aplicaciones del UIT-T (Rec. UIT-T X.200) y utiliza los servicios de capa de presentación y servicios ofrecidos por otros elementos de servicio de aplicación más generales. Un MHS puede construirse utilizando cualquier red que se adapte al objeto de la OSI. El servicio de transferencia de mensajes proporcionado por el MTS es independiente de la aplicación. Un ejemplo de aplicación normalizada es el servicio IPM (F.420 + X.420), el servicio de mensajeria de intercambio electrónico de datos (EDI, *electronic data interchange*) (F.435 + X.435) y el servicio de mensajeria vocal (F.440 + X.440). Los sistemas finales pueden utilizar el servicio de transferencia de mensajes (MT, *message transfer*) para aplicaciones específicas que se definen en forma bilateral. Los servicios de tratamiento de mensajes proporcionados por los proveedores de servicios pertenecen al grupo de servicios telemáticos. Los servicios públicos disponibles en MHS, así como el acceso al MHS, y desde éste, para servicios públicos, se describen en la serie de Recomendaciones F.400. Los aspectos técnicos del MHS se definen en las Recomendaciones de la serie X.400. La arquitectura global del sistema de tratamiento de mensajes se define en la Rec. UIT-T X.402. Los elementos de servicio son las características de servicio prestadas a través de procesos de aplicación. Se considera que estos elementos de servicio son componentes de los servicios prestados a los usuarios, y son elementos de un servicio básico, o bien *facilidades de usuario facultativas*, clasificadas en *facilidades de usuario facultativas esenciales*, o *facilidades de usuario facultativas adicionales*. En la cláusula 15/F.400 se describen las capacidades de **seguridad** del MHS, incluyendo las **amenazas a la seguridad** MHS, el modelo de seguridad, los elementos de servicio que describen las características de seguridad (definidos en el anexo B), la **gestión de seguridad**, necesidades de seguridad MHS, seguridad IPM. Cuestión 11/17

F.440 *Servicios de tratamiento de mensajes: Servicio de mensajería vocal*

Esta Recomendación especifica los aspectos generales, operacionales y de calidad de servicio del servicio público internacional de mensajería vocal, un tipo de servicio de tratamiento de mensajes (MH) que es un servicio internacional de telecomunicación ofrecido por las Administraciones, y que permite a los abonados enviar mensajes a uno o más destinatarios y recibir mensajes por redes de telecomunicación, utilizando una combinación de técnicas de almacenamiento y retransmisión y de almacenamiento y extracción. El servicio de mensajería vocal (VM, *voice messaging*) permite a los abonados solicitar que se emplee una diversidad de características durante el tratamiento e intercambio de mensajes vocales codificados. Algunas características son inherentes al servicio VM básico. Otras características no básicas pueden ser seleccionadas por el abonado, mensaje por mensaje o durante un periodo de tiempo acordado por contrato, si son proporcionadas por las Administraciones. Con el servicio VM puede proporcionarse, opcionalmente, la intercomunicación con el de mensajería

interpersonal (IPM, *interpersonal messaging*). Las características básicas tienen que ser facilitadas internacionalmente por las Administraciones. Las no básicas, visibles para el abonado, se clasifican en esenciales o adicionales. Las características opcionales esenciales deben ser facilitadas internacionalmente por las Administraciones. Las características opcionales adicionales pueden ser facilitadas por algunas administraciones para uso nacional, e internacional por acuerdo bilateral. Las características no básicas se llaman facilidades facultativas de usuario. La prestación del servicio VM se efectúa utilizando cualquier red de comunicaciones. Este servicio puede ofrecerse por separado o en combinación con diversos servicios telemáticos o de comunicación de datos. Las especificaciones técnicas y los protocolos que han de utilizarse en el servicio VM se definen en las Recomendaciones de la serie X.400.

Anexo G – Elementos de servicio de **seguridad** de mensajería vocal

Anexo H – Visión de conjunto de la **seguridad** de mensajería vocal Cuestión 11/17

F.851 *Telecomunicación personal universal – Descripción del servicio (conjunto de servicios 1)*

Esta Recomendación proporciona una descripción del servicio y disposiciones operacionales para la telecomunicación personal universal (UPT, *universal personal telecommunication*). Se presenta una descripción general del servicio desde el punto de vista del abonado/usuario UPT. El usuario de servicios UPT tiene acceso, mediante abono, a un conjunto de servicios definidos por el mismo, en un perfil propio de servicios UPT. El riesgo de una violación de la privacidad o de facturación errónea debida a uso fraudulento es mínimo para el usuario UPT. En principio, se puede utilizar cualquier servicio básico de telecomunicaciones con el UTP. El tipo de servicios que recibe el usuario se ven limitados solamente por las redes y terminales utilizados. Entre las características del UTP esenciales para el usuario, cabe mencionar primero la "autenticación de identidad de usuario", y como característica opcional la autenticación de proveedor de servicio UTP. En la cláusula 4.4 se explican con detalle los requisitos de seguridad. Cuestión 3/2

H.233 *Sistema de confidencialidad para servicios audiovisuales*

Un sistema de privacidad consta de dos partes, el mecanismo de confidencialidad o proceso de criptación de los datos, y un subsistema de gestión de claves. Esta Recomendación describe la parte de confidencialidad de un sistema de privacidad adecuado para su utilización en los servicios audiovisuales de banda estrecha. Si bien este sistema de privacidad necesita un algoritmo de criptación, la especificación de dicho algoritmo no se incluye aquí: el sistema no se limita a un determinado algoritmo. El sistema de confidencialidad es aplicable a los enlaces punto a punto entre terminales o entre un terminal y una unidad de control multipunto (MCU, *multipoint control unit*); puede extenderse al funcionamiento multipunto, en el que no hay descriptación en la MCU. Cuestión G/16

H.234 *Sistema de auenticación y de gestión de las claves de criptación para los servicios audiovisuales*

Un sistema de privacidad consta de dos partes, el mecanismo de confidencialidad o proceso de criptación de los datos, y un subsistema de gestión de claves. En esta Recomendación se describen los métodos de autenticación y de gestión de claves para un sistema de privacidad adecuado para su utilización en servicios audiovisuales de banda estrecha. La privacidad se consigue utilizando *claves secretas*. Las claves se cargan en la parte confidencialidad del sistema de privacidad y controlan la manera según la cual se criptan y decriptan los datos transmitidos. Si un tercero consigue acceder a las claves que están siendo utilizadas, el sistema de privacidad deja de ser seguro. El mantenimiento de claves por los usuarios constituye, pues, parte importante del sistema de privacidad. En esta Recomendación se especifican tres métodos prácticos alternativos de gestión de claves.

Cuestión G/16

H.235 *Seguridad y criptado para terminales multimedios de la serie H (basados en H.323 y H.245)*

Las comunicaciones seguras en tiempo real a través de redes inseguras suelen involucrar *autenticación* y *privacidad* (criptado de datos). Esta Recomendación describe mejoras dentro del marco de las especificaciones de conferencias interactivas a fin de incorporar servicios de seguridad como autenticación de punto extremo y privacidad de medios, y describe la infraestructura de seguridad y las técnicas específicas de privacidad que han de emplearse. El esquema propuesto es aplicable a conferencias punto a punto y multipunto para cualquier tipo de terminales que utilicen como su protocolo de control el de H.245. Esta versión (11/00) incluye criptografía de curva elíptica, perfiles de seguridad (simple basado en contraseñas y perfeccionado basado en firmas digitales), las nuevas contramedidas de seguridad (antiinundación de medios), el soporte del algoritmo de criptación avanzado (AES), el soporte para el servicio fuera del terminal, los identificadores de objeto definidos (véase la guía del implementador de la Rec. UIT-T H.323). Cuestión G/16

H.235 Anexo F *Perfil de seguridad híbrido*

En este anexo se describe un perfil de seguridad híbrido basado en una infraestructura de clave pública (PKI, *public key infrastructure*), eficiente y escalable, que despliega firmas digitales del anexo E/H.235 y que despliega el perfil de seguridad básica del anexo D/H.235. El presente anexo se sugiere como una opción. Las entidades de seguridad H.323 (terminales, controladores de acceso, pasarelas, MCU, etc.) pueden implementar este perfil de seguridad híbrido para mejorar la seguridad o cuando sea necesario. La noción de "híbrido" en este texto significa que los procedimientos de seguridad del perfil de firmas en el anexo E se aplican realmente en un sentido ligero y las firmas digitales son aún conformes con los procedimientos RSA. Sin embargo, las firmas digitales se despliegan sólo cuando ello es absolutamente necesario; de lo contrario, se utilizan técnicas de seguridad simétrica sumamente eficientes del perfil de seguridad básico descrito en el anexo D. El perfil de seguridad híbrido es aplicable a la telefonía IP "mundial" escalable. Cuando se aplica estrictamente este perfil de seguridad supera las limitaciones del perfil de seguridad básico simple descrito en el anexo D, y además, resuelve ciertos inconvenientes del anexo E tales como la necesidad de mayor anchura de banda y de una mejor calidad para el procesamiento. Por ejemplo, el perfil de seguridad híbrido no depende de la administración (estática) de los secretos compartidos mutuos de los saltos en diferentes dominios. Así, los usuarios pueden elegir más fácilmente su proveedor VoIP. Por tanto, este perfil de seguridad soporta además cierto tipo de movilidad del usuario. Aplica criptografía asimétrica con firmas y certificados solamente cuando es necesario y en otro caso utiliza técnicas simétricas más simples y eficientes. Proporciona tunelización de los mensajes H.245 para la integridad de los mismos y también implementa algunas disposiciones para el no repudio de mensajes. El perfil de seguridad híbrido determina el modelo con encaminamiento por GK y se basa en las técnicas de tunelización H.245. Se encuentra en estudio el soporte para los modelos con encaminamiento no efectuado por GK. Cuestión G/16

H.323 *Sistemas de comunicación multimedios basados en paquetes (anexo J: Seguridad para tipos de punto extremo simples)*

La presente Recomendación describe terminales y otras entidades que proporcionan servicios de comunicaciones de audio, de video, de datos y multimedios en tiempo real por redes por paquetes (PBN) que tal vez no proporcionen una calidad de servicio garantizada. El soporte del audio es obligatorio, mientras que el de datos y vídeo es opcional, pero si se soportan es necesario poder utilizar un modo de funcionamiento común especificado, para que puedan interfuncionar todos los terminales que soporten ese tipo de medios. La red por paquetes puede incluir LAN, redes locales a una empresa, MAN, Intranets, Inter-Networks (incluyendo la Internet), conexiones punto a punto, un

segmento de red único o una interred que tenga múltiples sistemas con topologías complejas, por lo que pueden utilizarse en configuraciones punto a punto, multipunto o de difusión. Pueden interfuncionar con terminales por la RDSI-BA, por la RDSI-BE, redes LAN de calidad de servicio garantizada, por la RTGC y redes inalámbricas, y las entidades pueden estar integradas en computadores personales o implementadas en dispositivos autónomos como son los videoteléfonos. Cuestión G/16

H.530 *Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Rec. UIT-T H.510*

Esta Recomendación trata de los procedimientos de seguridad en entornos de movilidad H.323 como es el caso de la H.510 que describe el servicio de movilidad para servicios y sistemas multimedios de H.323. Proporciona detalles sobre los procedimientos de seguridad para la Rec. UIT-T H.510. Hasta el presente, las capacidades de señalización de la Rec. UIT-T H.235, versiones 1 y 2 están previstas para el tratamiento de la seguridad en entornos H.323, que suelen ser estáticos. Esos entornos y sistemas multimedios pueden lograr cierta movilidad limitada dentro de zonas de controladores de acceso; la Rec. UIT-T H.323 en general y la Rec. UIT-T H.235 en particular sólo proporcionan un soporte muy reducido para una itinerancia securizada de usuarios y terminales móviles a través de dominios diferentes en los que, por ejemplo, numerosas entidades participan en un entorno de movilidad, distribuido. Los escenarios de movilidad H.323 descritos en la Rec. UIT-T H.510 relativos a la movilidad del terminal plantean una nueva situación que refleja el carácter flexible y dinámico de esos escenarios, también desde el punto de vista de la seguridad. Los usuarios y terminales móviles H.323 en itinerancia tienen que ser autenticados por un dominio visitado, extranjero. Asimismo, interesa al usuario móvil tener la prueba de la verdadera identidad del dominio visitado. También puede ser conveniente tener la prueba de la identidad de los terminales que complementan la autenticación del usuario. Por tanto, se requiere la mutua autenticación del usuario y del dominio visitado y, facultativamente, también la autenticación de la identidad del terminal. Como generalmente el usuario móvil sólo se conoce en el dominio de base en el que está inscrito y donde se le ha asignado una contraseña, el dominio visitado inicialmente no conoce al usuario móvil. En consecuencia, el dominio visitado no comparte ninguna relación de seguridad establecida con el usuario y el terminal móviles. Para que el dominio visitado pueda obtener debidamente la autenticación y las condiciones de seguridad relativas al usuario móvil y al terminal móvil, el dominio visitado transferirá ciertas tareas de seguridad como las comprobaciones de autorización o la gestión de clave al dominio de base a través de entidades de red y de servicio intermedias. Esto exige también la securización de la comunicación y de la gestión de claves entre el dominio visitado y el dominio de base. Si bien, en principio, los entornos H.323 de movilidad son más abiertos que las redes H.323 cerradas, también es necesario, desde luego, securizar debidamente las tareas de gestión de clave. También es cierto que la comunicación dentro y a través de los dominios de movilidad merece protección contra las manipulaciones maliciosas. Cuestión G/16

J.93 *Requisitos del acceso condicional en la distribución secundaria de televisión digital por sistemas de televisión por cable*

En esta Recomendación se definen los requisitos de privacidad de datos y acceso para la protección de las señales de televisión digital MPEG transmitidas por redes de televisión por cable entre el extremo de cabecera principal de cable y el usuario final. Al depender de la industria o región de que se trate, no se incluyen aquí los algoritmos criptográficos exactos. CE 9

J.96 Enm. 1 *Procedimiento técnico para asegurar la privacidad en la transmisión internacional a larga distancia de señales de televisión MPEG-2 de conformidad con la Rec. UIT-T J.89*

Esta Recomendación constituye una norma común para un sistema de acceso condicional de transmisión internacional a larga distancia de televisión digital de acuerdo con el perfil profesional MPEG-2 (4:2:2). Se describe el sistema básico de aleatorización interoperable (BISS, *basic interoperable scrambling system*) basado en la especificación DVB-CSA que utiliza claves no criptadas fijas, denominadas palabras de sesión. En otro modo, que es compatible con versiones anteriores, se introduce un mecanismo adicional para insertar palabras de sesión criptadas sin perder interoperabilidad. Cuestión 6/9

J.170 *Especificación de la seguridad de Ipcablecom (J.sec)*

La presente Recomendación define la arquitectura, los protocolos, algoritmos, requisitos funcionales asociados y cualesquiera requisitos tecnológicos de seguridad que puedan proporcionar la seguridad del sistema para la red IPCablecom. Los servicios de seguridad de autenticación, control de acceso, integridad del contenido de los mensajes y del portador, confidencialidad y no repudio deben ser suministrados como se define en este documento para cada una de las interfaces de elementos de red. CE 9

M.3010 *Principios para una red de gestión de las telecomunicaciones*

En esta Recomendación se definen conceptos de las arquitecturas de la red de gestión de las telecomunicaciones (RGT) (arquitectura funcional de la RGT, arquitectura de información de la RGT y arquitectura física de la RGT) y sus elementos fundamentales. Se describe también la relación entre las tres arquitecturas y se proporciona un marco para derivar los requisitos de la especificación de arquitecturas físicas de la RGT desde el punto de vista de las arquitecturas funcional y de información de la RGT. Esta Recomendación trata los aspectos de seguridad solo en algunas de sus cláusulas. Asimismo, se presenta un modelo de referencia lógico para la partición de la funcionalidad de gestión denominado arquitectura lógica por capas (LLA). Se define también cómo demostrar conformidad y cumplimiento con la RGT a efectos de obtener interoperabilidad. Los requisitos de la RGT incluyen la aptitud para garantizar a los usuarios de información de gestión autorizados un acceso seguro a dicha información. La RGT contiene bloques funcionales para los que se alcanza la funcionalidad de seguridad mediante técnicas de seguridad en el entorno de la RGT y se debe asegurar la protección de la información intercambiada a través de las interfaces y que reside en la aplicación de gestión. Los principios y mecanismos de seguridad también están relacionados con el control de los derechos de acceso de los usuarios de la RGT a la información asociada con aplicaciones de la RGT.

Cuestión 7/4

M.3016 *Visión general de la seguridad en la red de gestión de las telecomunicaciones (M.3sec)*

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. Cuestión 7/4

M.3210.1 *Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000) – Requisitos*

Esta Recomendación pertenece a la serie de Recomendaciones UIT-T M.3200 relativas al servicio de gestión de la RGT que proporcionan la descripción de servicios de gestión, objetivos y contexto para los aspectos de gestión de las redes de telecomunicaciones móviles internacionales 2000 (IMT-2000). Basándose en los conjuntos de funciones identificados en la Rec. UIT-T M.3400, define nuevos conjuntos de funciones, así como nuevas funciones y parámetros, e introduce semánticas y restricciones adicionales. Se describe un subconjunto de servicios de gestión de seguridad a fin de satisfacer los requisitos y permitir el análisis de la gestión de seguridad, así como un perfil para la gestión del fraude en una red móvil IMT-2000. Se hace hincapié en la interfaz X entre dos proveedores de servicio y en los servicios de gestión que se necesitan entre los dos para detectar y prevenir el fraude mediante el sistema de recogida de información de fraude (FIGS, *fraud information gathering system*) entre proveedores de servicio como medio para supervisar un conjunto definido de actividades de abonado y limitar el riesgo financiero de cuentas no pagadas, que puede ocurrir mientras el abonado está itinerando. Cuestión 14/4

M.3320 *Requisitos para la interfaz X*

La presente Recomendación forma parte de una serie de Recomendaciones relativas a la transferencia de información para la gestión de las redes y servicios de telecomunicaciones, y solamente se tratan aspectos de seguridad en algunas partes de ella. El objetivo de esta Recomendación es definir un marco general relativo a los requisitos funcionales, de servicio y en la red para el intercambio de información sobre la RGT entre administraciones. La Recomendación presenta igualmente el marco general de utilización de la interfaz RGT-X para el intercambio de información entre administraciones, empresas de explotación reconocidas, otros operadores de redes, suministradores de servicios, clientes y otras entidades. Cuestión 9/4

M.3400 *Funciones de gestión de la RGT*

Esta Recomendación pertenece a la serie de Recomendaciones sobre la red de gestión de las telecomunicaciones (RGT), y proporciona especificaciones de las funciones de gestión de la RGT y de los conjuntos de funciones de gestión de la RGT. El material fue elaborado como apoyo de la base de información de tarea B (*cometidos, recursos y funciones*), asociada a la tarea 2 (*descripción del contexto de gestión de la RGT*) de la metodología de especificación de la interfaz de la red de gestión de las telecomunicaciones especificada en la Rec. UIT-T M.3020. Al proceder al análisis del contexto de gestión de la RGT, considérese la posibilidad de utilizar al máximo los conjuntos de funciones de gestión de la RGT que figuran en esta Recomendación. Cuestión 7/4

Q.293 *Periodos en los que conviene tomar medidas de seguridad*

Es un extracto del BlueBook y contiene solamente las cláusulas 8.5 (Periodos en los que conviene tomar medidas de seguridad) a 8.9 (Método de compartición de la carga) de Q.293 CE 4

Q.813 *Elemento de servicio de aplicación de transformaciones de seguridad para el elemento de servicio de operaciones a distancia (STASE-ROSE)*

La presente Recomendación proporciona las especificaciones para soportar transformaciones de seguridad, como criptación, troceado (función hash), sellado y firma, centrando la atención en las unidades de datos de protocolo (PDU) del elemento de servicio de operaciones a distancia (ROSE) en su totalidad. Las transformaciones de seguridad se utilizan para facilitar la prestación de diversos servicios de seguridad, por ejemplo los de autenticación, confidencialidad, integridad y no repudio. Esta Recomendación describe una manera de realizar las transformaciones de seguridad que se implementa en la capa de aplicación y no requiere ninguna funcionalidad específica de la seguridad en ninguna de las capas de la pila OSI subyacentes. Cuestión 18/4

Q.815 *Especificación de un módulo de seguridad para la protección del mensaje completo*

La presente Recomendación especifica un módulo de seguridad opcional utilizable con la Rec. UIT-T Q.814, Especificación de un agente interactivo de intercambio electrónico de datos, que proporciona servicios de seguridad a unidades de datos de protocolo (PDU) completas. En particular, el módulo de seguridad sustenta no repudio de origen y de recibo, así como integridad del mensaje completo. Cuestión 18/4

Q.817 *Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados*

En esta Recomendación se indica la forma en que pueden utilizarse los certificados digitales y las listas de revocación de certificados en la RGT y se proporcionan los requisitos necesarios para el uso de certificados y de extensiones de la lista de revocación de certificados. Esta Recomendación tiene por objeto promover el interfuncionamiento entre elementos de la red de gestión de las telecomunicaciones (RGT) que utilizan la infraestructura de claves públicas (PKI) como soporte de las funciones relacionadas con la seguridad. El objetivo de esta Recomendación es proporcionar un mecanismo interoperable y aplicable a escala variable de distribución y gestión de claves dentro de una RGT, a través de todas las interfaces, y de apoyo al servicio de no repudio a través de la interfaz X. Se aplica a todas las interfaces y realizaciones de la RGT. Es independiente de la pila de protocolos de comunicación o del protocolo de gestión de red que se emplee. Las posibilidades de utilización que ofrece la PKI se pueden aprovechar en una amplia gama de funciones de seguridad, tales como las de autenticación, integridad, no repudio e intercambio de claves (Rec. UIT-T M.3016). Sin embargo, la presente Recomendación no especifica si deben implementarse esas funciones, con o sin PKI. Cuestión 18/4

Q.1531 *Requisitos de seguridad en telecomunicaciones personales universales para el conjunto de servicios 1*

Esta Recomendación especifica los requisitos de seguridad UPT para las comunicaciones usuario a red y entre redes aplicables al conjunto de servicios 1 de UPT definido en la Rec. UIT-T F.851. Esta Recomendación cubre todos los aspectos de la seguridad para las UPT que utilizan acceso DTMF y accesos de usuario basados en DSS1 fuera de banda. CE 15

Q.1741.1 *Referencias de IMT-2000 a la publicación de 1999 del sistema global para comunicaciones móviles que ha evolucionado hacia la red medular del sistema de telecomunicaciones móviles universales con la red de acceso de la red terrenal de acceso radioeléctrico*

En esta Recomendación se incluyen referencias a las siguientes especificaciones de seguridad 3GPP:

TS 21.133: Amenazas y requisitos relativos a la seguridad

TS 22.100: Fase 1 del UMTS

TS 22.101: Principios de servicio UMTS

TS 33.102: Arquitectura de seguridad

TS 33.103: Directrices de integración de seguridad

TS 33.105: Requisitos de algoritmos criptográficos

TS 33.106: Requisitos de intercepción lícita

TS 33.107: Arquitectura y funciones de intercepción lícita

TS 33.120: Objetivos y principios de seguridad CCE

Q.1741.2 *Referencias de las IMT-2000 a la versión 4 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles con red terrenal de acceso radioeléctrico universal*

En esta Recomendación se incluyen referencias a las siguientes especificaciones de seguridad 3GPP:

TS 21.133: Seguridad en 3G; Amenazas y requisitos relativos a la seguridad

TS 22.048: Mecanismos de seguridad para el juego de herramientas de aplicaciones (U)SIM; Etapa 1

TS 22.101: Principios de servicio

TS 33.102: Seguridad en 3G; Arquitectura de seguridad

TS 33.103: Seguridad en 3G; Directrices de integración

TS 33.105: Requisitos de algoritmos criptográficos

TS 33.106: Requisitos de intercepción lícita

TS 33.107: Seguridad en 3G; Arquitectura y funciones de la intercepción lícita

TS 33.120: Objetivos y principios de seguridad

TS 33.200: Seguridad en el dominio de red; MAP

TS 35.205, .206, .207, y .208: Seguridad en 3G; Especificación del conjunto de algoritmos MILENAGE: Conjunto de ejemplos de algoritmos para las funciones de autenticación y de generación de las claves *f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 y *f*5* en 3GPP; (.205: Generalidades; .206: Especificación de algoritmo; .207: Datos de pruebas de implementador; .208: Datos de prueba de conformidad de diseño) CCE

Q.1741.3 *Referencias de las IMT-2000 a la versión 5 de la red medular del sistema de telecomunicaciones móviles universales derivada del sistema global para comunicaciones móviles con red terrenal de acceso radioeléctrico universal*

En esta Recomendación se incluyen referencias a las siguientes especificaciones de seguridad 3GPP:

TS 22.101: Aspectos de servicio; Principios de servicio

TS 33.102: Seguridad en 3G; Arquitectura de seguridad

TS 33.106: Requisitos de intercepción lícita

TS 33.107: Seguridad en 3G; Arquitectura y funciones de la intercepción lícita

TS 33.108: Seguridad en 3G; Interfaz de traspaso para la interceptación legal (LI)

TS 33.200: Seguridad en el dominio de red; MAP

TS 33.203: Seguridad en 3G; Seguridad de acceso para servicios basados en IP

TS 33.210: Seguridad en 3G; Seguridad del dominio de red (NDS); Seguridad de la capa de red IP

TS 35.205, .206, .207, .208 y .909: Seguridad en 3G; Especificación del conjunto de algoritmos MILENAGE: Conjunto de ejemplos de algoritmos para las funciones de autenticación y de generación de las claves *f*1, *f*1*, *f*2, *f*3, *f*4, *f*5 y *f*5* en 3GPP; (.205: Generalidades; .206: Especificación de algoritmo; .207: Datos de pruebas de implementador; .208: Datos de prueba de conformidad de diseño; .909: Resumen y resultados del diseño y evaluación) CEE

Q.1742.1 *Referencias en las IMT-2000 a la red medular desarrollada ANSI-41 con red de acceso cdma2000*

La presente Recomendación asocia las normas de la red medular publicadas por las organizaciones de desarrollo de normas (SDO, *standards development organizations*) con las especificaciones del 3GPP2 aprobadas el 17 de julio de 2001 para el miembro de la familia de las IMT-2000 "red medular desarrollada ANSI-41 con red de acceso cdma2000". Las especificaciones del 3GPP2 que fueron aprobadas en julio de 2002 estarán asociadas con las normas de la red medular publicadas en la futura Rec. UIT-T Q.1742.2. La interfaz radioeléctrica y la red de acceso y las normas de las SDO para este

miembro de la familia IMT-2000 están asociadas en la Recomendación UIT-R M.1457. Las asociaciones para otros miembros de la familia IMT-2000 se identifican en la serie de Recomendaciones UIT-T Q.174x. Esta Recomendación combina y asocia las normas pertinentes de red medular de varias organizaciones de desarrollo de normas para este miembro de la familia IMT-2000 en una Recomendación general. CEE

Q.1742.2 *Referencias en las IMT-2000 a la red medular desarrollada ANSI-41 con red de acceso cdma2000, (aprobadas el 11 de julio de 2002)*

La presente Recomendación asocia las normas de la red medular publicadas por las organizaciones regionales de normalización (SDO) con las especificaciones del 3GPP2 aprobadas el 11 de julio de 2002 para este miembro de la familia de las IMT-2000: "La red medular desarrollada ANSI-41 con red de acceso cdma2000". Las especificaciones del 3GPP2 que fueron aprobadas el 17 de julio de 2001 están asociadas con las normas de la red medular publicadas por las organizaciones regionales de normalización en la Recomendación UIT-T Q.1742.1. Las especificaciones del 3GPP2 que se aprueben en julio de 2003 estarán asociadas con las normas de la red medular publicadas en la futura Recomendación UIT-T Q.1742.3. La interfaz radioeléctrica y la red de acceso radioeléctrica y las normas de las SDO para este miembro de la familia IMT-2000 están asociadas en la Recomendación UIT-R M.1457. Las asociaciones para otros miembros de la familia IMT-2000 se identifican en la serie de Recomendaciones UIT-T Q.174x. La presente Recomendación combina y asocia las normas regionales de red medular para este miembro de la familia IMT-2000 en una Recomendación general. CEE

Q.1742.3 *Referencias IMT-2000 (aprobadas el 30 de junio de 2003) a la red medular evolucionada ANSI-41 con red de acceso cdma2000*

Especificaciones entre sistemas:

N.S0003-0 Versión 1.0 – Módulo de identidad de usuario (abril de 2001)

N.S0005-0 Versión 1.0 – Operaciones entre sistemas de radiocomunicaciones celulares (sin fecha)

N.S0009-0 Versión 1.0 – IMSI (sin fecha)

N.S0010-0 Versión 1.0 – Prestaciones avanzadas en sistemas de espectro ensanchado de banda ancha (sin fecha)

N.S0011-0 Versión 1.0 – OTASP y OTAPA (sin fecha)

N.S0014-0 Versión 1.0 – Mejoras de autenticación (sin fecha)

N.S0018 Versión 1.0.0 – TIA/EIA-41-D Tasación preabonada (14 de julio de 2000)

N.S0028 Versión 1.0.0 – Interfuncionamiento de red entre la MAP GSM y la MAP ANSI-41 Rev. B Revisión: 0 (abril de 2002)

Especificaciones relativas a redes de datos en paquetes:

P.S0001-A Versión 3.0.0 – Norma de red IP inalámbrica (16 de julio de 2001)

P.S0001-B Versión 1.0.0 – Norma de red IP inalámbrica (25 de octubre de 2002)

Especificaciones de aspectos de servicios y de sistemas:

S.R0005-B Versión 1.0 – Modelo de referencia de red para sistemas de espectro ensanchado cdma2000 Revisión: B (16 de abril de 2001)

S.R0006 Versión 1.0.0 – Revisión de la descripción de características inalámbricas Revisión: 0 (13 de diciembre de 1999)

S.R0009-0 Versión 1.0 – Módulo de identidad de usuario (Etapa 1) Revisión: 0 (13 de diciembre de 1999)

S.R0018 Versión 1.0.0 – Tasación preabonada (Etapa 1) Revisión: 0 (13 de diciembre de 1999)

S.R0019 Versión 1.0.0 – Sistema de servicios basados en la posición (LBSS) Descripción de la Etapa 1 (22 de septiembre de 2000)

S.R0032 Versión 1.0 – Autenticación de abonado mejorada (ESA) y privacidad de abonado mejorada (ESP) (6 de diciembre de 2000)

S.R0037-0 Versión 2.0 – Modelo de arquitectura de la red IP para los sistemas de espectro ensanchado cdma2000 (14 de mayo de 2002)

S.R0048 Versión 1.0 – Identificador de equipo móvil 3G (MEID) (10 de mayo de 2001)

S.S0053 Versión 1.0 – Algoritmos criptográficos comunes (21 de enero de 2002)

S.S0054 Versión 1.0 – Especificación de interfaz para algoritmos criptográficos comunes (21 de enero de 2002)

S.S0055 Versión 1.0 – Algoritmos criptográficos mejorados (21 de enero de 2002)

S.R0058 Versión 1.0 – Requisitos del sistema del dominio multimedios IP (17 de abril de 2003)

S.R0059 Versión 1.0 – Dominio MS anterior – Requisitos del sistema, Etapa 1 (16 de mayo de 2002)

S.R0066-0 Versión 1.0 – Requisitos de la Etapa 1 de los servicios IP basados en la posición (17 de abril de 2003)

S.R0071 Versión 1.0 – Requisitos de vigilancia de los datos en paquetes del sistema anterior – Requisitos de la Etapa 1 (18 de abril de 2002)

S.R0072 Versión 1.0 – Requisitos de vigilancia de datos en paquetes exclusivamente IP – Requisitos de la Etapa 1 (18 de abril de 2002)

S.R0073 Versión 1.0 – Gestión de la configuración de dispositivos durante la comunicación Internet (IOTA) – Etapa 1 (11 de julio de 2002)

S.S0078-0 Versión 1.0 – Algoritmos de seguridad común (12 de diciembre de 2002) CCE

T.30 *Procedimientos de transmisión de documentos por facsímil por la red telefónica general conmutada*

El anexo G describe el protocolo utilizado por los terminales facsímil grupo 3 para proporcionar comunicaciones seguras utilizando los sistemas HKM y HFX. El anexo H especifica los mecanismos que ofrecen características de seguridad para terminales facsímil grupo 3 basadas en el sistema criptográfico RSA. CE 16

T.36 *Capacidades de seguridad para su utilización con terminales facsímil del grupo 3*

Esta Recomendación define las dos soluciones técnicas independientes que pueden utilizarse en el contexto de una transmisión facsímil segura. Las dos soluciones técnicas se basan en los algoritmos HKM/HFX40 y en el algoritmo RSA. CE 16

T.123rev Anexo B *Conexiones de transporte ampliadas*

Este anexo a la versión revisada de T.123 define un protocolo de negociación de conexión (CNP, *connection negotiation protocol*) que ofrece negociación de capacidad de seguridad. El mecanismo de seguridad que se aplica incluye varios métodos para garantizar la seguridad de red y transporte, nodo por nodo, por ejemplo TLS/SSL, IPSEC y/o IKE, o gestión manual de claves, X.274/ ISO TLSP y GSS-API. Cuestión 1/16

T.503 *Perfil de aplicación de documento para el intercambio de documentos facsímil del Grupo 4*

Esta Recomendación define un perfil de aplicación de documento que puede ser utilizado por cualquier servicio telemático. Su finalidad es especificar un formato de intercambio adecuado para el intercambio de documentos facsímil del Grupo 4 que contienen solamente gráficos por puntos. Los documentos se intercambian en forma formateada, lo que permite al destinatario visualizar o imprimir el documento en la forma deseada por el originador. CE 16

T.563 *Características de terminal para aparatos facsímil del grupo 4*

La presente Recomendación define las características de terminal para aparatos facsímil del grupo 4 y la interfaz con la red física. CE 16

T.611 *Interfaz de programación de comunicación **APPLI/COM** para servicios facsímil grupo 3, facsímil grupo 4, teletex, télex, correo electrónico y transferencia de ficheros*

En esta Recomendación se define una interfaz de programación de comunicación denominada "**APPLI/COM**", que proporciona acceso unificado a diversos servicios de comunicaciones, como facsímil de Grupo 3 u otros servicios telemáticos. Describe la estructura y el contenido de estos mensajes, así como la manera de intercambiarlos (es decir, LA, aplicación local y CA, aplicación de comunicación). *Toda comunicación va precedida de un proceso de enganche (login process) y terminada por uno de desenganche(logout process), facilitando así la implementación de esquemas de seguridad, especialmente importantes cuando se trata de sistemas multiusuario. De igual manera, proporcionan medios para implementar un mecanismo de seguridad entre el LA y el CA.* Constituye también una interfaz de aplicación de programación (API, *application programming interface*) de alto nivel que oculta todas las peculiaridades de la telecomunicación, pero proporciona a los diseñadores de aplicaciones un gran poder de control y supervisión sobre la actividad de telecomunicación.
CE 8

X.217 *Tecnología de la información – Interconexión de sistemas abiertos – Definición de servicio para el elemento de servicio de control de asociación*

En esta Recomendación se proporciona la definición de servicio para el elemento de servicio de control de asociación **(ACSE)** que se utiliza para controlar asociaciones de aplicación OSI. ACSE ofrece dos modos de servicio de comunicación: con conexión y sin conexión. En el ACSE se definen tres unidades funcionales. La unidad funcional medular obligatoria se utiliza para establecer y liberar asociaciones de aplicación. El ACSE incluye dos unidades funcionales optativas. La unidad funcional optativa de autenticación soporta el intercambio de información para atender la autenticación durante el establecimiento de la asociación sin añadir servicios. Las facilidades ACSE de autenticación pueden utilizarse para soportar una clase limitada de métodos de autenticación.

Enmienda 1: Soporte del mecanismo de autenticación para el modo sin conexión. Cuestión 11/17

X.227 *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo con conexión para el elemento de servicio de control de asociación: Especificación de protocolo*

Esta Especificación de protocolo define los procedimientos que se aplican a situaciones de comunicación entre sistemas que desean interconectarse en un entorno de interconexión de sistemas abiertos en el modo con conexión, es decir un protocolo en modo orientado a conexión para el elemento-servicio-aplicación para el control de asociación-aplicación, el ACSE. La Especificación de protocolo incluye la unidad funcional medular que se utiliza para establecer y liberar asociaciones de aplicación. La unidad funcional autenticación proporciona medios adicionales para el intercambio de información a efectos de soportar la autenticación durante el establecimiento de la asociación sin añadir nuevos servicios. Las facilidades de autenticación ACSE pueden utilizarse para soportar una clase limitada de métodos de autenticación. La unidad funcional de negociación del contexto de aplicación proporciona una facilidad adicional para la selección del contexto de aplicación durante el establecimiento de la asociación. Contiene un anexo en el que se describe una máquina de protocolo

de control de asociación (ACPM, *association control protocol machine*), en términos de un cuadro de estado. Hay además un anexo que describe un mecanismo de autenticación sencillo que utiliza una contraseña con un título AE destinado a uso general, y constituye un ejemplo de una especificación de mecanismo de autenticación. A este mecanismo de autenticación se le asigna el siguiente nombre (del tipo de dato ASN.1 OBJECT IDENTIFIER):

{joint-iso-itu-t association-control(2) authentication-mechanism(3) password-1(1)}.

Para este mecanismo de autenticación, la contraseña es el valor de autenticación. El tipo de dato del valor de autenticación deberá ser "GraphicString" Cuestión 11/17

X.237 *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo en modo sin conexión para el elemento de servicio de control de asociación: Especificación de protocolo*

La enmienda 1 a esta Recomendación incluye el marcador de extensibilidad ASN.1 en el modulo que describe el protocolo. También amplía la especificación del protocolo ACSE sin conexión, a fin de soportar el transporte de los parámetros de autenticación en la APDU A-UNIT-DATA.
Cuestión 11/17

X.257 *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo en modo sin conexión para el elemento de servicio de control de asociación: Formulario de enunciado de conformidad de implementación de protocolo*

En esta Recomendación se presenta el formulario de enunciado de conformidad de implementación de protocolo (PICS, *protocol implementation conformance statement*) correspondiente al protocolo sin conexión de OSI para el elemento de servicio de control de asociación (ACSE, *association control service element*), que se especifica en la Rec. UIT-T X.237. El formulario PICS representa, en forma tabular, los elementos obligatorios y opcionales del protocolo ACSE sin conexión. El formulario PICS se utiliza para indicar las características y opciones de una determinada implementación del protocolo ACSE sin conexión. Cuestión 11/17

X.272 *Compresión de datos y privacidad en las redes con retransmisión de tramas*

En esta Recomendación se define el servicio de compresión y privacidad de datos por redes de retransmisión de tramas incluyendo negociación y encapsulación de compresión de datos, la compresión securizada de datos, autenticación y criptación por retransmisión de tramas. La presencia de un servicio de compresión de datos (DC) en una red se traducirá por un aumento de su caudal efectivo. La demanda de transmisión de datos sensibles a través de redes públicas requiere dispositivos que garanticen la privacidad de los datos. Para obtener relaciones de compresión óptimas es necesario comprimir los datos antes de criptarlos. En consecuencia, es conveniente que en el servicio de compresión de datos se especifiquen medios que permitan negociar también protocolos de criptación de datos. Como la tarea de comprimir datos y después criptarlos exige una intensa actividad de cálculo, se han propuesto algunos protocolos en los que las operaciones de compresión y de criptación de datos se refunden en una sola (compresión securizada de datos). Estos protocolos se basan en el protocolo de control del enlace (RFC 1661 del IETF), el protocolo de control de criptación (RFC 1968 del IETF y 1969). Esta Recomendación se aplica a tramas de información no numerada (UI, *unnumbered information*) encapsuladas por el procedimiento del anexo E/Q.933. Trata la compresión y privacidad de datos en conexiones virtuales permanentes (PVC, *permanent virtual connections*) y conexiones virtuales conmutadas (SVC, *switched virtual connections*). Cuestión 10/17

X.273 *Tecnología de la información – Interconexión de sistemas abiertos – Protocolo de seguridad de la capa de red*

En esta Recomendación se especifica el protocolo que sustenta todos los servicios de integridad, confidencialidad, autenticación y control de acceso que, según el modelo de seguridad OSI, son aplicables a los protocolos de capa de red en los modos con conexión y sin conexión. El protocolo sustenta estos servicios mediante el empleo de mecanismos criptográficos, etiquetas de seguridad y atributos de seguridad asignados, tales como claves criptográficas. Cuestión 11/17

X.274 *Tecnología de la información – Intercambio de telecomunicaciones e información entre sistemas – Protocolo de seguridad de la capa de transporte*

En esta Recomendación se especifica el protocolo que soporta todos los servicios de integridad, confidencialidad, autenticación y control de acceso que, según se identifica en el modelo de seguridad OSI, son aplicables a la capa de transporte. El protocolo soporta estos servicios mediante el empleo de mecanismos criptográficos, etiquetas de seguridad y atributos de seguridad asignados, tales como claves criptográficas. Cuestión 11/17

X.400/F.400 *Visión de conjunto del sistema y del servicio de tratamiento de mensajes*

Esta Recomendación define los elementos de servicio del sistema de tratamiento de mensajes (MHS) para los servicios de **seguridad**, pertinentes a la capa de aplicación, de confidencialidad, integridad, autenticación, no repudio y control de acceso en los casos agente de usuario(UA)-a-UA, agente de transferencia de mensaje(MTA, *Message Transfer Agent*)-a-MTA, UA-a-MTA, y UA-a-usuario de memoria de mensajes (MS, *message store*). (Véase F.400) Cuestión 11/17

X.402 *Tecnología de la información – Sistemas de tratamiento de mensajes: Arquitectura global*

En esta Recomendación se especifican procedimientos de seguridad e identificadores de objeto útiles en los protocolos MHS para garantizar los servicios de confidencialidad, integridad, autenticación, no repudio y control de acceso relevantes para la capa de aplicación. Cuestión 11/17

X.411 *Tecnología de la información – Sistemas de tratamiento de mensajes – Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos*

En esta Recomendación se especifican mecanismos y procedimientos para el soporte de los servicios de confidencialidad, integridad, autenticación y no repudio, en lo que concierne a la capa de aplicación. Esto se hace gracias a mecanismos criptográficos, etiquetado de seguridad y firmas digitales, tal como se define identifica en la Rec. UIT-T X.509. Si bien se especifica un protocolo que utiliza técnicas de criptografía asimétrica, también se soportan las simétricas. Cuestión 11/17

X.413 *Tecnología de la información – Sistemas de tratamiento de mensajes: Memoria de mensajes: Definición del servicio abstracto*

En esta Recomendación se especifican mecanismos, protocolos y procedimientos para el soporte de los servicios de integridad, autenticación, no repudio y control de acceso, en lo que concierne a la capa de aplicación. El protocolo soporta estos servicios en nombre del usuario directo de memoria de mensajes (MS, *message store*). Cuestión 11/17

X.419 *Tecnología de la información – Sistemas de tratamiento de mensajes: especificaciones de protocolo*

En esta Recomendación se especifican procedimientos y contextos de aplicación para identificar acceso seguro a las entidades MHS y usuarios distantes, mediante los servicios de autenticación y control de acceso, en lo que concierne a la capa de aplicación. Cuestión 11/17

X.420 *Technología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería interpersonal*

En esta Recomendación se especifican mecanismos, protocolos y procedimientos para el intercambio de objetos entre usuarios del servicio de mensajería interpersonal o agentes de usuarios en representación de su usuario directo identificado en lo que concierne a la capa de aplicación. Los servicios de seguridad que se soportan son confidencialidad, integridad, autenticación y control de acceso, en lo que concierne a la capa de aplicación. Cuestión 11/17

X.435 *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería con intercambio electrónico de datos*

En esta Recomendación se especifican mecanismos, protocolos y procedimientos para el intercambio de objetos entre agentes de usuario del intercambio electrónico de datos (EDI, *electronic data interchange*) en representación de su usuario directo. Los servicios de seguridad que se soportan son confidencialidad, integridad, autenticación y control de acceso, en lo que concierne a la capa de aplicación. Cuestión 11/17

X.440 *Tecnología de la información – Sistemas de tratamiento de mensajes: Sistema de mensajería vocal*

En esta Recomendación se especifican mecanismos, protocolos y procedimientos para el intercambio de objetos entre Agentes de usuario del agente de usuario del sistema de mensajería vocal en representación de su usuario directo. Los servicios de seguridad que se soportan son confidencialidad, integridad, autenticación y control de acceso, en lo que concierne a la capa de aplicación.
Cuestión 11/17

X.500 *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios*

En esta Recomendación se especifican el Directorio y sus características de seguridad.
Cuestión 9/17

X.501 *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*

En esta Recomendación se especifica la utilización de Directorio de sus marcos de certificado de atributo y clave pública conforme a la Rec. UIT-T X.509. Cuestión 9/17

X.509 *Tecnología de la información – Interconexión de sistemas abiertos – El directorio:*

- *---- Marco de autenticación (edición de 1993, segunda edición/versión)*
- *---- Marco de autenticación (edición de 1997, tercera edición/versión)*
- *---- Marcos de clave pública y certificados de atributo (edición de 2000, cuarta edición/versión)*

En esta Recomendación se define un marco para certificados de clave pública y para certificados de atributo, y un marco para la prestación de servicios de autenticación por el directorio a sus usuarios. Describe dos niveles de autenticación: autenticación simple que utiliza una contraseña como verificación de la identidad alegada, y autenticación fuerte con credenciales formadas utilizando técnicas criptográficas. Si bien la autenticación simple ofrece cierta protección limitada contra el

acceso no autorizado, sólo se debe utilizar la autenticación fuerte para proporcionar servicios seguros. Estos marcos se pueden utilizar para perfilar su aplicación a infraestructuras de clave pública **(PKI)** y a infraestructuras de gestión de privilegios **(PMI)**. Dicho marco incluye la especificación de objetos de datos utilizada para representar los propios certificados así como notificaciones de revocación para certificados expedidos en los que ya no se debe confiar. Si bien este marco de certificados de clave pública define algunos componentes críticos de la infraestructura de claves públicas **(PKI)**, no define una **PKI** en su totalidad. Sin embargo, esta Especificación proporciona las bases sobre las cuales se construirán las **PKI** y sus especificaciones. El marco de certificados de atributo incluye la especificación de objetos de datos utilizados para representar los propios certificados así como notificaciones de revocación para certificados expedidos en los que ya no se debe confiar. El marco de certificados de atributo definido en esta Especificación, aunque define algunos componentes críticos de la infraestructura de gestión de privilegios **(PMI)**, no define una **PMI** en su totalidad. Sin embargo, esta Especificación proporciona las bases sobre las cuales se construirán las **PMI** y sus especificaciones. También se definen *objetos de información* para alojar objetos de PKI y de PMI en el directorio y para comparar valores presentados con valores almacenados. Cuestión 9/17

X.519 *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Especificaciones de protocolo*

En esta Recomendación se especifican procedimientos y contextos de aplicación para identificar el acceso seguro durante la vinculación de entidades de directorio. Cuestión 9/17

X.733 *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas*

En esta Recomendación se define una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizado o descentralizado para interactuar a los efectos de la gestión de sistemas. También se define una función compuesta de definiciones genéricas, servicios y unidades funcionales. Esta función está ubicada en la capa de aplicación del modelo de referencia de OSI. Las notificaciones de alarma definidas por esta función proporcionan la información que un gestor puede necesitar en relación con la condición operativa y calidad de servicio de un sistema para ejecutar su cometido. Cuestión 17/4

X.735 *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función control de ficheros registro cronológico*

En esta Recomendación se define una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizado o descentralizado para interactuar a los efectos de sistemas. También se define la función control de fichero registro cronológico y está constituida por servicios y dos unidades funcionales. Esta función está situada en la capa de aplicación. Cuestión 17/4

X.736 *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad*

Se define en esta Recomendación | Norma Internacional la función señaladora de alarmas de seguridad. La función señaladora de alarmas de seguridad es una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizado o descentralizado para intercambiar información con fines de gestión de sistemas, según se define en la Recomendación CCITT X.700 | ISO/CEI 7498-4. Esta Recomendación | Norma Internacional está situada en la capa de aplicación de la Recomendación CCITT X.200 | ISO 7498, y está definida con arreglo al modelo proporcionado por ISO/CEI 9545. El cometido de las funciones de gestión de sistemas está descrito en la Recomendación CCITT X.701 | ISO/CEI 10040. Las notificaciones de alarma de seguridad definidas por esta función de gestión de sistemas proporcionan información sobre la condición operacional y la calidad de servicio, por lo que se refiere a la seguridad.

Cuestión 14/4

X.740 *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pista de auditoría de seguridad*

Esta Recomendación | Norma Internacional define la función de pista de auditoría de seguridad. La función de pista de auditoría de seguridad es una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizada o descentralizada para intercambiar información e instrucciones a efectos de gestión de sistemas, como se define en la Recomendación CCITT X.700 | ISO/CEI 7498-4. Esta Recomendación | Norma Internacional está posicionada en la capa de aplicación de la Recomendación CCITT X.200 | ISO 7498 y se define de acuerdo con el modelo proporcionado por ISO/CEI 9545. El rol de funciones de gestión de sistemas se describe en la Recomendación CCITT X.701 | ISO/CEI 10040. Cuestión 14/4

X.741 *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso*

En esta Recomendación | Norma Internacional se especifica un modelo de seguridad de control de acceso y la información de gestión necesaria para crear y administrar el control de acceso asociado con la gestión de sistemas de OSI. La política de seguridad adoptada para cualquier caso de utilización no se especifica y se deja como una opción de la realización. Esta Especificación es de aplicación genérica y se puede emplear para la gestión de seguridad de muchos tipos de aplicación.

Cuestión 14/4

X.800 *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del UIT-T*

Esta Recomendación define los elementos arquitecturales generales relacionados con la seguridad que pueden aplicarse adecuadamente en las circunstancias en que se requiere la protección de la comunicación entre sistemas abiertos. Establece, en el marco del modelo de referencia, directrices y restricciones para mejorar las Recomendaciones existentes o formular nuevas Recomendaciones en el contexto de OSI con el fin de permitir comunicaciones seguras y proporcionar así un enfoque coherente de la seguridad en OSI. También amplía el modelo de referencia para abarcar los aspectos de seguridad que son elementos arquitecturales generales de protocolos de comunicación, pero que no se examinan en el modelo de referencia. La presente Recomendación da una descripción general de los servicios de seguridad y mecanismos conexos, que pueden ser proporcionados por el modelo de referencia; y define las posiciones, dentro del modelo de referencia, en que pueden proporcionarse los servicios y mecanismos. Cuestión 10/17

X.802 *Tecnología de la información – Modelo de seguridad de capas más bajas*

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

Cuestión 10/17

X.803 *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*

En esta Recomendación se describe la selección, ubicación y utilización de los servicios y mecanismos de seguridad en las capas más altas del modelo de referencia de OSI (capas de aplicación, presentación y sesión). Cuestión 10/17

X.805 *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*

En esta Recomendación se definen los elementos de seguridad generales de la arquitectura, que, si son empleados correctamente, y tratándose de un entorno de productos de múltiples fabricantes, pueden garantizar la seguridad de la red contra ataques malintencionados o imprevistos, y garantizar condiciones de alta disponibilidad, tiempo de respuesta apropiado, integridad, y adaptación a otra escala, y también proporcionar información exacta para facturación. Cuestión 10/17

X.810 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*

En esta Recomendación se define el marco en el que se especifican los servicios de seguridad para los sistemas abiertos. Esta parte de los marcos de seguridad describe la organización del marco de seguridad, define los conceptos de seguridad que se requieren en más de una parte del marco de seguridad y describe la interrelación de los servicios y mecanismos identificados en otras partes del marco. En este marco se describen todos los aspectos relativos a la autenticación, ya que se aplican a los sistemas abiertos, la relación de autenticación con otras funciones de seguridad como el control de acceso y los requisitos de gestión necesarios para la autenticación. Cuestión 10/17

X.811 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*

En esta Recomendación se define un marco general a efectos de garantizar la autenticación. El objetivo primordial de la autenticación es proteger contra amenazas del tipo usurpación de identidad y reproducción no autorizada. Cuestión 10/17

X.812 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*

En esta Recomendación se define un marco general a efectos de garantizar el control de acceso. El objetivo primordial del control de acceso es proteger contra la amenaza de que se efectúen operaciones no autorizadas con un computador o sistema de comunicaciones; se suele clasificar estas amenazas en clases, a saber utilización no autorizada, divulgación, modificación, destrucción y negación de servicio. Cuestión 10/17

X.813 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo (no repudio)*

En esta Recomendación se define un marco general a efectos de garantizar los servicios de no repudio. El objetivo primordial del servicio de no repudio es recolectar, mantener, poner a disposición y validar evidencia irrefutable sobre la identidad de los remitentes y destinatarios de transferencias de datos. Cuestión 10/17

X.814 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de confidencialidad*

En esta Recomendación se define un marco general a efectos de garantizar los servicios de confidencialidad. Por confidencialidad se entiende la propiedad de que no se divulgue o haga disponible la información a personas, entidades o procesos no autorizados. Cuestión 10/17

X.815 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de integridad*

En esta Recomendación se define un marco general a efectos de garantizar los servicios de integridad, la propiedad que consiste en que los datos no hayan sido alterados o destruidos sin autorización. Cuestión 10/17

X.816 *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad*

En esta Recomendación se describe un modelo básico para tratar las alarmas de seguridad y para efectuar una auditoría de seguridad para sistemas abiertos. Una auditoría de seguridad es una revisión y un examen independientes de los registros y actividades del sistema. El servicio de auditoría de seguridad otorga a una autoridad de auditoría la capacidad de especificar, seleccionar y gestionar los eventos que tienen que ser registrados en un rastreo de auditoría de seguridad. Cuestión 10/17

X.830 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Sinopsis, modelo y notación*

Esta Recomendación forma parte de una serie de Recomendaciones que proporcionan diversas facilidades para la construcción de protocolos de capa superior de OSI que sustentan la prestación de servicios de seguridad. En esta Recomendación se definen: a) modelos generales de funciones de protocolo de intercambio de seguridad y transformaciones de seguridad; b) un conjunto de herramientas de notación para sustentar la especificación de requisitos de protección selectiva de los campos en una especificación de sintaxis abstracta y para sustentar la especificación de intercambios y transformaciones de seguridad; y c) un conjunto de directrices informativas sobre la aplicación de las facilidades de seguridad genérica de las capas superiores abarcadas por esta serie de Recomendaciones. Cuestión 10/17

X.831 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Definición de servicio del elemento de servicio de intercambio de seguridad*

Esta Recomendación forma parte de una serie de Recomendaciones que proporcionan diversas facilidades para la construcción de protocolos de capa superior de OSI que sustentan la prestación de servicios de seguridad. Se define el servicio proporcionado por el elemento de servicio de intercambio de seguridad (SESE), que es un elemento de servicio de aplicación (ASE) que facilita la comunicación de información de seguridad para soportar la prestación de servicios de seguridad en la capa de aplicación de OSI. Cuestión 10/17

X.832 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Especificación del protocolo de elemento de servicio de intercambio de seguridad*

Esta Recomendación forma parte de una serie de Recomendaciones que proporcionan diversas facilidades para la construcción de protocolos de capa superior de OSI que sustentan la prestación de servicios de seguridad. En ella se define el protocolo proporcionado por el elemento de servicio de intercambio de seguridad (SESE). El SESE es un elemento de servicio de aplicación (ASE) que facilita la comunicación de la información de seguridad para sustentar la prestación de servicios de seguridad dentro de la capa de aplicación de OSI. Cuestión 10/17

X.833 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Especificación de la sintaxis de transferencia de protección*

Esta Recomendación forma parte de una serie de Recomendaciones que proporcionan diversas facilidades para la construcción de protocolos de capa superior de OSI que sustentan la prestación de servicios de seguridad. En esta Recomendación | Norma Internacional se define la sintaxis de transferencia de protección, asociada con el soporte de la capa de presentación para servicios de seguridad en la capa de aplicación. Cuestión 10/17

X.834 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Formularios de declaración de conformidad de implementación del protocolo del elemento de servicio de intercambio de seguridad*

Esta Recomendación forma parte de una serie de Recomendaciones sobre seguridad genérica de las capas superiores (GULS, g*eneric upper layers security*). Se trata del formulario de declaración de conformidad de implementación de protocolo (PICS) para el protocolo del elemento de servicio de intercambio de seguridad especificado en la Rec. UIT-T X.832 y los intercambios de seguridad descritos en el anexo C/X.830. La presente Recomendación proporciona la descripción de capacidades y opciones normalizadas de una manera que permite evaluar la conformidad de una implementación determinada. Cuestión 10/17

X.835 *Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Formulario de declaración de conformidad de implementación de protocolo de la sintaxis de transferencia de protección*

Esta Recomendación forma parte de una serie de Recomendaciones sobre seguridad genérica de las capas superiores (GULS, *generic upper layers security*). Se trata del formulario de declaración de conformidad de implementación de protocolo (PICS) para la sintaxis de transferencia de protección especificada en la Rec. UIT-T X.833. Esta Recomendación proporciona la descripción de capacidades y opciones normalizadas de una manera que permite evaluar la conformidad de una implementación determinada. Cuestión 10/17

X.841 *Tecnología de la información – Técnicas de seguridad – Objetos de información de seguridad para control de acceso*

En esta Recomendación, que trata sobre objetos de información de seguridad (SIO) para el control de acceso, se proporcionan definiciones de objeto que, en muchas ocasiones, son necesarias en normas de seguridad para evitar la existencia de múltiples definiciones diferentes de la misma funcionalidad. Mediante el uso de la notación de sintaxis abstracta uno (ASN.1) se asegura la precisión de estas definiciones. Esta Recomendación trata solamente los aspectos estáticos de los SIO.

Cuestión 10/17

X.842 *Tecnología de la información – Técnicas de seguridad – Directrices sobre el uso y gestión de servicios de tercera parte confiable*

En esta Recomendación se proporcionan una orientación para el uso y gestión de los servicios de tercera parte confiable (TTP), una definición clara de las funciones y servicios básicos prestados, sus descripciones y finalidades, y los cometidos y responsabilidades de las TTP y las entidades que utilizan sus servicios. También se identifican diferentes categorías principales de servicios TTP que incluyen la identificación de tiempo, el no repudio, la gestión de claves, la gestión de certificados, y la notaría pública electrónica. Cuestión 10/17

X.843 *Tecnología de la información – Técnicas de seguridad – Especificación de servicios de tercera parte confiable para soportar la aplicación de firmas digitales*

En esta Recomendación se definen los servicios requeridos para soportar la aplicación de firmas digitales para el no repudio de la creación de un documento. Puesto que ello implica la integridad del documento y la autenticidad del creador, los servicios descritos pueden combinarse también para implementar los servicios de integridad y autenticidad. Cuestión 10/17

X.901 *Tecnología de la información – Procesamiento distribuido abierto – Modelo de Referencia: Visión de conjunto*

El rápido crecimiento del procesamiento distribuido ha creado la necesidad de un marco de coordinación para la normalización del procesamiento distribuido abierto (ODP*, open distributed processing*). Este modelo de referencia de ODP proporciona tal marco. Crea una arquitectura dentro de la cual se puede integrar un soporte de distribución, interfuncionamiento y portabilidad. Contiene una

visión de conjunto motivada del ODP, que da el alcance, la justificación y la explicación de conceptos esenciales, y una descripción de la arquitectura ODP. Contiene material explicativo sobre la interpretación y aplicación del modelo de referencia por los usuarios, entre los que puede haber escritores de normas y arquitectos de sistemas ODP. Contiene también una agrupación en categorías de las áreas de normalización requeridas, expresadas en términos de los puntos de referencia para conformidad identificados en la Rec. UIT-T X.903. Los sistemas ODP han de ser seguros, es decir se los debe construir y mantener de tal manera que se garantice la protección de las facilidades del sistema y de los datos contra acceso no autorizado, uso ilegal y cualesquiera otras amenazas o ataques. Debido al carácter distante de las interacciones y la movilidad de las partes del sistema y sus usuarios, es más difícil garantizar los requisitos de seguridad. Tratándose de la seguridad de sistemas abiertos se deben definir: reglas para la detección de amenazas de seguridad; reglas para la protección contra amenazas de seguridad; y reglas para limitar todo efecto perjudicial de una brecha en la seguridad.

Cuestión 26/17

X.902 *Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia: Fundamentos*

Esta Recomendación contiene la definición de los conceptos y el marco analítico para la descripción normalizada de sistemas de procesamiento distribuido (arbitrarios). Presenta los principios de conformidad con normas de procesamiento distribuido abierto (ODP) y la manera de aplicarlos, sólo a un nivel de detalle suficiente para sustentar la Rec. X.903 y establecer los requisitos para las nuevas técnicas de especificación. Cuestión 26/17

X.903 *Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia: Arquitectura*

Esta Recomendación contiene la especificación de las características requeridas que califican los sistemas de procesamiento distribuido como abiertos. Éstas son las constricciones que deben cumplir las normas de procesamiento distribuido abierto (ODP). Se emplean las técnicas descriptivas de la Rec. X.902. Cuestión 26/17

X.904 *Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia: Semántica arquitectural*

Esta Recomendación contiene una formalización de los conceptos de modelado del ODP definidos en las cláusulas 8 y 9 de la Rec. UIT-T X.902. La formalización se consigue interpretando cada concepto basándose en las construcciones de las diferentes técnicas de descripción formal normalizada.

Cuestión 26/17

B.2 Aspectos de seguridad que no se tratan en este Manual (Fiabilidad y protección física de la planta externa)

Desde el punto de vista de la fiabilidad y la disponibilidad de una red, el nivel de seguridad de transporte de información será mayor si la planta externa está protegida contra: corrosión, efectos ambientales, incendios, actividades humanas y otras posibles fuentes de daños en los cables de telecomunicaciones públicas y sus estructuras correspondientes. El cuidado que se tenga durante la construcción de cables y equipos, así como en su instalación y supervisión es fundamental a la hora de garantizar el buen funcionamiento de un enlace. Cuanta más información se transporte, más importante será la protección física de la planta. Las Recomendaciones de la serie L contienen técnicas que permiten incrementar el nivel de seguridad de una planta y, por ende, de la información que viaja de un extremo al otro del enlace.

L.3 *Armadura de los cables*

Al tratarse de cables que se tienden directamente por tierra, la armadura contribuye a la instalación segura y aumenta la fiabilidad de la operación gracias a que protege los cables contra cualquier daño mecánico que pueda ser causado por piedras, equipos de excavación o herramientas, roedores e insectos, corrosión química o electrolítica, efectos de rayos y de proximidad de líneas de alta tensión.
Cuestión 8/6

L.4 *Cubiertas de aluminio para cables*

Conviene generalizar la utilización del aluminio para las cubiertas de los cables por lo menos cuando el costo previsto del cable no sea superior al de un cable con cubierta de plomo y también cuando las cubiertas de aluminio satisfagan mejor las exigencias técnicas. La utilización de cables con cubiertas de aluminio ofrece especial interés en el caso de cables interurbanos. Cuestión 8/6

L.5 *Cubiertas de cable fabricadas con metales distintos del plomo y del aluminio*

Según el tipo de aplicación, se pueden utilizar otros tipos de armaduras, como por ejemplo aluminio ondulado (no liso) o cintas de cobre. Cuestión 8/6

L.7 *Aplicación de la protección catódica común*

Se entiende por protección catódica común de diferentes estructuras metálicas subterráneas, la protección de esas estructuras contra la corrosión por medio de dispositivos de protección comunes. Un sistema de protección común para varias estructuras metálicas subterráneas se compone de conexiones eléctricas entre las estructuras y los dispositivos de protección comunes que satisfacen los requisitos de protección catódica y drenaje eléctrico. Las técnicas comunes de protección mejoran la fiabilidad de las estructuras enterradas y la eficacia de los dispositivos de protección catódica, reduciendo al mismo tiempo los costos totales de inversión y mantenimiento del sistema de protección. Cuestión 7/6

L.16 *Material plástico conductor como revestimiento protector para cubiertas metálicas de cables*

Los principales beneficios que se obtienen al utilizar cables con revestimiento de material plástico conductor son: una mejor protección del conductor contra la corrosión, los relámpagos y los efectos de las líneas de alta tensión; una reducción de los costos de mantenimiento, en particular de puesta a tierra; y una simplificación de los proyectos de protección. Cuestión 8/6

L.20 *Creación de un código de seguridad contra incendios para instalaciones de telecomunicaciones*

En el caso de edificios, construidos o en proyecto, en los que se vayan a instalar equipos de telecomunicaciones, conviene que las administraciones establezcan un código de seguridad contra incendios, con arreglo al uso específico que se va a dar a cada inmueble y que contenga las directrices mínimas a seguir en lo que respecta a la seguridad y protección contra el fuego.
Cuestión 2/6

L.21 *Sistemas de detección y de alarma, detectores y sirenas de alarmas contra incendios*

A fin de proteger la propiedad, y en su caso la vida humana, pueden instalarse sistemas de detección y alarma contra incendios para iniciar cierto número de actividades diferentes, como la detección y localización de un incendio, la prestación de asistencia para contener y/o extinguir el fuego, los procedimientos de evacuación de emergencia, la convocación del personal antiincendios.
Cuestión 2/6

L.22 *Protección contra incendios*

Teniendo en cuenta los graves daños que pueden producirse cuando se declara un incendio y la importancia de la prevención de incendios para la seguridad, prestación de servicio y economía de los sistemas de comunicación, hay varios aspectos que deben considerarse, como son la reducción del coeficiente de carga de incendio, la división del edificio en compartimentos (sectores antiincendios) para reducir y retardar la propagación del fuego, y las estadísticas de incendios.

Cuestión 2/6

L.23 *Extinción de incendios – Clasificación y ubicación de las instalaciones de extinción de incendios y equipos situados en locales*

Los medios para combatir el fuego que se adopten en un edificio de telecomunicaciones pueden variar según la utilización y la ubicación de los locales, y dependen de si el edificio está ocupado. Estos son factores que determinan la magnitud de la asistencia del servicio de incendios inicialmente atribuida en caso de que se produzca un fuego. Cuestión 2/6

L.25 *Mantenimiento de redes de cables de fibra óptica*

Gracias a los sistemas y procedimiento de mantenimiento se puede verificar la calidad de una red de fibra óptica, sin importar qué tipo de equipo de transmisión se utilice. Cuestión 5/6

L.28 *Protección adicional externa para cables terrenales marinizados*

En los cables para aguas poco profundas, la probabilidad de avería es mayor que en las aplicaciones para aguas profundas, debido a los fenómenos ambientales (por ejemplo, desplazamiento de las olas marinas, terremotos y deslizamientos de tierra bajo el agua, etc.) y las actividades humanas que afectan al lecho marino (por ejemplo, pesca, tendido y mantenimiento de otros servicios y cables).

Además de las diversas armaduras con las que normalmente se construye el cable – por ejemplo, armadura para roca (RA, *rocky armour*), armadura de acero galvanizado como armadura doble (DA, *double armour*) y armadura simple (SA, *single armour*), en los casos necesarios se puede usar protecciones externas adicionales. Cuando se prevé que los factores externos o las características del fondo marino pueden dañar los cables, las protecciones se instalan en las proximidades de la costa en aguas superficiales, o en la playa, en el tramo entre la orilla del agua y la cámara de empalme en la playa, o en el recorrido del cable. Cuestión 10/6

L.32 *Dispositivos de protección para orificios pasacables entre sectores antiincendios*

Dado el gran número de orificios pasacables que hay en las fronteras entre sectores antiincendios de un edificio de telecomunicaciones, que disminuyen la eficacia del sistema de extinción, la adopción de medidas pasivas de control del humo y el fuego tales como el sellado de los orificios pasacables con materiales ignífugos o la utilización de sistemas de gestión (protección) de cables constituyen una estrategia adecuada. Cuestión 2/6

L.45 *Minimización de la repercusión sobre el medio ambiente de la planta exterior de las redes de telecomunicaciones*

En esta Recomendación se presenta la metodología adoptada para minimizar los efectos (por ejemplo, energía y CO_2) causados en el medio ambiente por el uso de la planta exterior. Se basa en el análisis del ciclo de vida, es decir en el periodo *de la cuna a la tumba* de los productos. Cuestión 1/6

L.46 *Protección de los cables y planta de telecomunicaciones contra las agresiones biológicas*

En esta Recomendación se describen los ataques biológicos y las contramedidas que deben aplicarse para proteger los cables de telecomunicaciones. Se refiere a los distintos tipos de ataques biológicos, a

los puntos débiles de los cables y a las características de los daños y considera métodos alternativos para proteger la planta, incluida la dependencia con la situación del cable. Cuestión 1/6

Las siguientes Recomendaciones versan sobre disponibilidad en lo que atañe a las redes SDH y OTN:

G.841 *Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona*

La presente Recomendación describe los distintos mecanismos de protección para las redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*), sus objetivos y sus aplicaciones.

Los esquemas de protección se clasifican como de protección de camino SDH (en la capa de sección o de trayecto) y de protección de conexión de subredes SDH (con supervisión intrínseca, supervisión no intrusiva y supervisión de subcapa). Cuestiones 15, 16, 17, 18/15

G.842 *Interfuncionamiento de las arquitecturas de protección para redes SDH*

Esta Recomendación proporcional las especificaciones para el interfuncionamiento de arquitecturas de protección de redes. Tiene un tratamiento especial la interconexión de nodo único y de nodo doble entre anillos de protección compartida de sección de multiplexión (MS) y anillos de protección de conexión de subred (SNCP) de tipos iguales o distintos. Cuestiones 15, 16, 17, 18/15

G.808.1 *Conmutación de protección genérica – Protección de camino lineal y de subred*

En este Recomendación se proporciona una visión global de la conmutación de protección lineal. Cubre los esquemas de protección basados en las redes OTN, SDH y ATM. En otras Recomendaciones se presentarán aspectos generales de los esquemas de interconexión de subredes (por ejemplo, en anillo) de nodo dual y protección de anillo. Cuestiones 15, 16, 17, 18/15

G.873.1 *Red óptica de transporte – Protección lineal*

En esta Recomendación se describe el protocolo de conmutación automática de protección (APS) y el funcionamiento de la conmutación de protección aplicable a los métodos de protección lineal de la red óptica de transporte en el nivel de la unidad de datos de canal óptico (ODUk). Se examinan los siguientes métodos de protección: protección de camino ODUk; protección de conexión de subred ODUk con supervisión inherente; protección de conexión de subred ODUk con supervisión no intrusiva; y protección de conexión de subred ODUk con supervisión de subcapa.

Cuestiones 15, 16, 17, 18/15

G.781 *Funciones de capas de sincronización*

Fiabilidad de fuente de temporización SDH y PDH. La presente Recomendación especifica una colección de bloques de construcción de distribución de sincronización básicos, a los que se denomina "funciones atómicas", y un conjunto de reglas que permiten combinarlos para describir la funcionalidad de sincronización de un equipo de transmisión digital.

Cuestiones 15, 16, 17, 18/15

G.911 *Parámetros y metodología de cálculo de la fiabilidad y la disponibilidad de los sistemas de fibra óptica*

La fiabilidad y la disponibilidad de los sistemas de fibra óptica: Esta Recomendación identifica un conjunto mínimo de parámetros necesarios para caracterizar la fiabilidad y la disponibilidad de los sistemas de fibra óptica. Se dan diferentes parámetros de fiabilidad y mantenimiento del sistema, de la fiabilidad de los dispositivos ópticos activos, de la fiabilidad de los dispositivos ópticos pasivos, y de la fiabilidad de las fibras y cables ópticos. La Recomendación también presenta directrices y métodos para calcular la fiabilidad predicha de los dispositivos, unidades y sistemas. Se incluyen ejemplos.

Cuestiones 15, 16, 17, 18/15

G.784 *Gestión de la jerarquía digital síncrona*

Gestión de SDH. Trata las funciones de Gestión de averías, configuración, contabilidad, funcionamiento y seguridad de los elementos de red SDH. Los aspectos de gestión de seguridad pertinentes a estas Recomendaciones se dejan para estudio ulterior. Cuestión Q.14/15

G.874 *Aspectos de la gestión de elementos de la red óptica de transporte*

Gestión OTN. Trata las funciones de Gestión de averías, configuración, contabilidad, funcionamiento y seguridad de los elementos de red OTN. Los aspectos de gestión de seguridad pertinentes a estas Recomendaciones se dejan para estudio ulterior. Cuestión Q.14/15

G.7712/Y.1703 *Arquitectura y especificación de la red de comunicación de datos*

En esta Recomendación se incluyen aspectos de seguridad de las redes de comunicación de gestión (RCG) y redes de comunicaciones de señalización (RCS). Las funciones de comunicación de datos que se proporcionan soportan servicios de red sin conexión. Es posible que en futuras versiones se añadan funciones que permitan también soportar servicios orientados a la conexión. Cuestión Q.14/15

NOTA – Es posible que las Recomendaciones UIT-T de las series G.650, 660-690, 950-970 contengan algunos elementos relacionados con la fiabilidad.

Anexo C: Lista de Comisiones de Estudio y Cuestiones relativas al tema de la seguridad

El trabajo de normalización del UIT-T se hace a través de Grupos Técnicos denominados Comisiones de Estudio (CE), en las que los representantes de los Miembros del Sector desarrollan Recomendaciones (normas) relativas a los diferentes campos de las telecomunicaciones internacionales. El trabajo de las CE se efectúa primordialmente gracias a la atribución de unas Cuestiones de estudio, que tratan cada una un aspecto determinado de la normalización de las telecomunicaciones. Cada CE tiene un Presidente y varios Vicepresidentes nombrados por la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT). A continuación se enumeran las Comisiones de Estudio del UIT-T para el periodo de estudios 2001-2004, sus títulos y mandatos, y se presenta una lista de las Cuestiones que tienen que ver con el tema de la seguridad.

CE 2	Aspectos de explotación de la prestación de servicios, redes y calidad de funcionamiento *Comisión de Estudio Rectora sobre definición de servicios, numeración encaminamiento y movilidad global*
Mandato: Se encarga de los estudios sobre los principios de la prestación de servicios, definición y requisitos de explotación de la emulación de servicios; requisitos de numeración, denominación, direccionamiento y asignación de recursos, incluidos los criterios y procedimientos para reservas y asignaciones; requisitos de encaminamiento e interfuncionamiento; factores humanos; aspectos de explotación de redes y requisitos conexos de calidad de funcionamiento, entre otros, gestión de tráfico de red, calidad de servicio (ingeniería de tráfico, calidad de funcionamiento operacional y mediciones del servicio); aspectos de explotación del interfuncionamiento entre redes tradicionales y en evolución de telecomunicaciones; evaluación de las experiencias comunicadas por operadores, fabricantes y usuarios sobre diversos aspectos de la explotación de redes.	
Cuestiones principales relacionadas con la seguridad: – C.5/2 – Calidad de servicio de las redes	

CE 3	Principios de tarificación y contabilidad, incluidos los temas relativos a economía y política de las telecomunicaciones
Mandato: Se encarga de los estudios referentes a los principios de tarificación y contabilidad para los servicios internacionales de telecomunicación y del estudio de los temas relativos a la economía y política de las telecomunicaciones. Con tal fin, la Comisión de Estudio 3 impulsará en particular la colaboración entre sus Miembros con vistas a establecer tasas lo más reducidas posible en consonancia con un servicio eficiente y teniendo en cuenta la necesidad de mantener una administración financiera independiente de las telecomunicaciones sobre bases idóneas.	
Cuestiones principales relacionadas con la seguridad: *Ninguna*	

CE 4	Gestión de las telecomunicaciones, incluida la red de gestión de las telecomunicaciones (RGT) *Comisión de Estudio Rectora sobre la RGT.*
Comisión de Estudio Rectora en aspectos de gestión. Su trabajo en temas de seguridad trata sobre: a) Consideraciones y requisitos de tipo arquitectural para las interfaces de gestión, b) Requisitos detallados para garantizar la seguridad de la red de gestión (también conocida como plano de gestión), en particular en un entorno cada vez más importante de convergencia de redes, c) Protocolos y modelos para la seguridad de la información de gestión y la gestión de los parámetros de seguridad.	

La gestión de la red de telecomunicaciones se define a varios niveles de abstracción, a saber desde la gestión misma de la información en un elemento de red hasta los servicios de gestión ofrecidos a los abonados. Los requisitos de seguridad para el intercambio de información entre sistemas de gestión, y entre ellos y elementos de red, depende de si las redes de gestión están dentro del dominio de una sola administración o entre varias de éstas. Basándose en los principios arquitecturales, se han venido definiendo, en varias Recomendaciones y en otras que están en desarrollo, los requisitos explícitos, y el soporte de mecanismos y protocolos.

Cuestiones principales relacionadas con la seguridad:
– C.16/4 – Soporte de la gestión RGT para las IMT-2000 y la RI

CE 5	Protección contra los efectos del entorno electromagnético

La CE 5 se encarga de los estudios relativos a la protección de redes y equipos de telecomunicaciones contra interferencias y descargas eléctricas, así como de los estudios relacionados con la compatibilidad electromagnética (EMC). En cumplimiento de su misión, la CE 5 ha trabajado en varias Cuestiones y desarrollado diversas Recomendaciones y Manuales sobre la seguridad de las redes contra las amenazas electromagnéticas. Entre estas últimas se cuentan aquellas que involucran fenómenos transitorios de alta potencia generados por actividades humanas malintencionadas, como los impulsos electromagnéticos a gran altitud (HEMP, *high-altitude electromagnetic pulse*) y las microondas de alta potencia (HPM, *high-power microwave*). La seguridad electromagnética también se encarga de posibles fugas de información en la red causadas por emisiones radioeléctricas inesperadas de los equipos.

La naturaleza de las amenazas y de las técnicas de mitigación correspondientes es similar a la de las perturbaciones electromagnéticas naturales o involuntarias. En otras palabras, las actividades tradicionales de la CE 5 sobre la protección contra rayos y el control de la interferencia electromagnética (EMI, *electromagnetic interference*) son útiles también cuando se trata de la seguridad de la red contra ataques maliciosos de origen humano. Actualmente, en la CE 6 hay seis Cuestiones relativas a la seguridad electromagnética de la red de telecomunicaciones.

Si bien hay mucha similitud entre los fenómenos electromagnéticos naturales o involuntarios mencionados y los ataques electromagnéticos de origen humano, también existen ciertas diferencias fundamentales entre ellos. En cumplimiento de su misión, la CE 5 ha trabajado en varias Cuestiones y desarrollado diversas Recomendaciones y Manuales sobre la seguridad de las redes contra las amenazas electromagnéticas.

La seguridad electromagnética se divide en dos partes principales:

- Resistencia e inmunidad de las redes y equipos de telecomunicaciones contra fenómenos transitorios de alta potencia de origen malicioso, como por ejemplo:
  - Campos electromagnéticos producidos por explosiones nucleares a gran altitud – impulsos electromagnéticos a gran altitud (HEMP, *high-altitude electromagnetic pulse*).
  - Generadores electromagnéticos de alta potencia (HPE, *high-power electromagnetic*), incluidos los de microondas de alta potencia (HPM) y las fuentes de ultra banda ancha (UWB, *ultra wideband*).
- Posibles fugas de información en la red causadas por emisiones radioeléctricas inesperadas de los equipos.

A medida que los medios de comunicación le dedican más espacio a estos fenómenos, hay cada vez más conciencia entre el público de su importancia.

La naturaleza de las amenazas y de las técnicas de mitigación correspondientes es similar a la de las perturbaciones electromagnéticas naturales o involuntarias. Por ejemplo, existen similitudes entre los HEMP y los impulsos electromagnéticos ocasionados por un rayo. Las técnicas de apantallamiento y filtrado que reducen las emisiones no deseadas de energía radioeléctrica en un equipo también ayudan a minimizar la posibilidad de fugas involuntarias de energía. En otras palabras, las actividades tradicionales de la CE 5 sobre la protección contra rayos y el control de la interferencia electromagnética (EMI, *electromagnetic interference*) son útiles también cuando se trata de la seguridad de la red contra ataques maliciosos de origen humano. En el cuadro a continuación se enumeran las Cuestiones atribuidas a la CE 5 para el periodo de estudio 2001-2004 que tienen que ver con el tema de la seguridad de las redes:

Cuestiones principales relacionadas con la seguridad:

– C.2/5 – Compatibilidad electromagnética relacionada con sistemas de acceso de banda ancha (*El control de emisiones no deseadas de los sistemas de acceso con banda ancha contribuye a reducir la posibilidad de fugas de información).*

– C.4/5 – Resistibilidad de nuevos tipos de equipos de telecomunicación y redes de acceso (*La resistencia de los equipos contra los rayos mejora la misma contra los HEMP*).

– C.5/5 – Protección contra la descarga de rayos de sistemas fijos, móviles e inalámbricos (*Las técnicas útiles para proteger contra la descarga de rayos también permiten obtener un cierto grado de protección contra los HEMP y los HPE*).

– C.6/5 – Configuraciones de conexión equipotencial y puesta a tierra de los sistemas de telecomunicaciones en el plano mundial (*Una conexión equipotencial y puesta a tierra adecuadas también conceden un cierto grado de protección contra los HEMP y los HPE*).

– C.12/5 – Mantenimiento y mejora de las Recomendaciones existentes sobre compatibilidad electromagnética (*La EMC de los equipos de telecomunicacionesmejora su inmunidad dentro de un entorno HEMP conductivo y radiado, así como en uno HPE radiado. De otra parte, la EMC de los equipos de telecomunicaciones reduce la posibilidad de fugas de información*).

– C.13/5 – Mantenimiento y mejora de las Recomendaciones sobre resistibilidad existentes (*La resistencia de los equipos contra los rayos mejora la misma contra los HEMP*).

CE 6	Planta exterior

Mandato: Se encarga de los estudios relativos a la planta exterior, tales como la construcción, instalación, empalme, unión, terminación, protección contra la corrosión y otros daños causados por el medio ambiente, exceptuados los procesos electromagnéticos, de todos los tipos de cables utilizados por las telecomunicaciones públicas y estructuras asociadas.

Cuestiones principales relacionadas con la seguridad:

– C.1/6 – Consideraciones ambientales para la planta exterior

– C.2/6 – Seguridad contra el fuego en las instalaciones de telecomunicación

– C.5/6 – Mantenimiento de la red de cables de fibra óptica

CE 9	Redes de cable integradas de banda ancha y trasmisión de televisión y sonido *Comisión de Estudio Rectora sobre redes integradas de cable de banda ancha y de televisión.*

Se encarga de preparar y mantener Recomendaciones relacionadas con:

- El empleo de redes de cable y redes híbridas, principalmente diseñadas para la entrega de programas radiofónicos y de televisión a los hogares, como redes integradas de banda ancha, que también pueden transportar servicios vocales u otros servicios que dependen críticamente de la secuencia temporal, vídeo según demanda, servicios interactivos, etc.
- El empleo de sistemas de telecomunicación para contribución, distribución primaria y distribución secundaria de programas radiofónicos y de televisión y servicios de datos similares.

En cumplimiento de sus objetivos, la CE 9 evalúa las amenazas y vulnerabilidades de las redes y servicios de banda ancha, los objetivos de seguridad de documentos y las posibles medidas para contrarrestarlas, y define la arquitectura de seguridad. Los principales temas relativos a la seguridad que se tratan son los servicios seguros de banda ancha, de VoIP , y de redes propias, así como la aplicación de entornos seguros de aplicación para servicios de televisión interactiva.

Las actividades relacionadas con la seguridad se concentran en:

- *Los servicios seguros de banda ancha:* Suministro de servicios de seguridad para las redes de acceso de banda ancha. Concretamente, autenticación del módem de cable, gestión de clave criptográfica, privacidad e integridad de los datos transmitidos, y descarga segura de *software* para el módem de cable.
- *Los servicios seguros VoIP:* IPCablecom es un proyecto especial relacionado con servicios interactivos altamente dependientes del tiempo, en redes de televisión por cable y mediante el IP, en particular la transmisión de voz y video por el IP. Los servicios de seguridad que se ofrecen en el IPCablecom son: autenticación del adaptador de terminal multimedios (MTA, *multimedia terminal adapter*) al proveedor de servicio, autenticación del proveedor de servicio al MTA, preparación y configuración segura de dispositivos, gestión segura de dispositivos, señalización segura, y seguridad de medios.
- *Servicios seguros de redes propias (domésticas):* Gracias a los módem de cable mejorados se pueden ofrecer servicios en redes domésticas del tipo cortafuegos (firewalls) y traducción de dirección de red. Los servicios de seguridad con que se cuenta para dichos módems son: autenticación del MTA al proveedor de servicio, autenticación del proveedor de servicio al MTA, preparación y configuración segura de dispositivos, gestión segura de dispositivos, funcionalidad de filtrado de paquetes/cortafuegos, gestión segura de cortafuegos, y descarga segura de software para el módem mejorado.
- *Entornos seguros de aplicación para servicios de televisión interactivos:* Los servicios de televisión interactivos dependen de los servicios de seguridad definidos en la especificación de Java y la plataforma doméstica multimedios (MHP, *multimedia home platform*).

Cuestiones principales relacionadas con la seguridad:

– C.6/9 – Métodos y prácticas para el acceso condicional y copias de protección para la distribución de televisión digital por cable a los hogares

– C.13/9 – Aplicaciones de señales vocales y vídeo con protocolos Internet a través de redes de televisión por cable

CE 11	Requisitos y protocolos de señalización *Comisión de Estudio Rectora sobre redes inteligentes.*

Mandato: Se encarga de los estudios relativos a los requisitos y protocolos de señalización para funciones relacionadas con el protocolo Internet (IP), algunas funciones relacionadas con la movilidad, funciones multimedios y la mejora de las Recomendaciones actuales sobre protocolos de señalización de interfuncionamiento y acceso de ATM, RDSI-BE y RTPC.

Cuestiones principales relacionadas con la seguridad:

– C.1/11 – Requisitos de señalización para soporte de nuevos servicios, servicios de valor añadido, servicios basados en el protocolo Internet y en la red inteligente.

– C.6/11 – Requisitos de señalización para el interfuncionamiento de los servicios de acceso a Internet por marcación telefónica y de comunicaciones de voz, datos y multimedios a través de redes basadas en el protocolo Internet.

– C.12/11 – Señalización de acceso y de red para servicios de banda estrecha y de banda ancha avanzados.

CE 12	Calidad de transmisión de extremo a extremo de redes y terminales *Comisión de Estudio Rectora sobre la calidad de servicio y la calidad de funcionamiento.*

Mandato: Se encarga de dar orientación sobre la calidad de transmisión de extremo a extremo de redes, terminales y sus interacciones, en relación con la calidad percibida, y la aceptación de aplicaciones de texto, voz e imagen por los usuarios. Esta labor comprende las implicaciones relacionadas con la transmisión en todas las redes (por ejemplo, las basadas en PDH, SDH, ATM e IP) y para todos los terminales de telecomunicaciones (por ejemplo, microteléfonos, de manos libres, auriculares, móviles, audiovisuales e interactivos de voz).

Cuestiones principales relacionadas con la seguridad:

– C.12/12 – Consideraciones relativas a la calidad de la transmisión en los servicios en banda vocal transportados por redes que utilizan el protocolo Internet (IP)

– C.13/12 – Requisitos de QoS/calidad de funcionamiento de multimedios

CE 13	Redes basadas en IP, redes multiprotocolo y su interconexión *Comisión de Estudio Rectora sobre temas relacionados con IP, RDSI-BA, infraestructura mundial de la información y asuntos de satélites.*

Dada su naturaleza, la CE 13 se encarga de los estudios relativos a:

- la interconexión de redes heterogéneas que comprenden múltiples dominios,
- múltiples protocolos y tecnologías innovadoras a los efectos de proporcionar un interfuncionamiento de gran calidad y fiabilidad.
- aspectos específicos son la arquitectura, el interfuncionamiento y la adaptación, consideraciones de extremo a extremo, encaminamiento y requisitos de transporte.

Al tratarse de la CE rectora en asuntos relacionados con el IP, la RDSI-BA, la Infraestructura mundial de la información (GII) y los satélites, así como del nuevo proyecto sobre redes de próxima generación (NGN), su trabajo tendrá influencia en múltiples aspectos relacionados con la seguridad en el sentido más amplio de la palabra.

La seguridad no es un concepto ajeno al trabajo de la CE 13: desde hace tiempo la Comisión ha venido trabajando en temas implícitamente relacionados con ella, mientras trataba el tema de la arquitectura y la estructura de red y sabiendo que era indispensable tenerlos en cuenta (tanto desde un punto de vista arquitectural como de implementación) a fin de garantizar que la red sea funcional y fiable.

A medida que se imponen las tecnologías digitales con conmutación de paquetes (relativamente abiertas) y un entorno liberalizado como el descrito en el concepto GII, la seguridad deviene cada ve más compleja e importante. Esto es particularmente cierto cuando en la "cadena de valor añadido", conforme al enfoque GII (o a su subconjunto en las NGN), se involucran terceras partes. Siendo así, la seguridad será fundamental y deberá considerarse de una manera explícita.

La CE 13 ha decidido entonces incorporar en cada Recomendación nueva o revisada una cláusula dedicada a la seguridad para que se haga referencia en aquellas cláusulas que traten sobre temas relativos a ésta, y aún si no hay aspectos relativos a la seguridad en una determinada Recomendación este hecho deberá consignarse en dicha cláusula. La CE 17 estuvo de acuerdo con esa decisión y se propuso presentarla a las demás CE.

De igual manera, la CE 13 decidió informar a la CE 17 cada vez que una Recomendación contenga especificaciones relacionadas con la seguridad, a fin de permitir la actualización del "Catálogo de Recomendaciones de seguridad aprobadas" y del "Compendio de definiciones de seguridad del UIT-T aprobadas"

En el nuevo proyecto sobre las NGN se tratan aspectos de seguridad en varias cláusulas, en particular en 6.6.

Cuestiones principales relacionadas con la seguridad:

– C.1/13 – Principios, requisitos, marcos y arquitecturas para un entorno mundial de redes heterogéneas
– C.3/13 – Explotación, administración y mantenimiento (OAM) y gestión de red en redes basadas en el protocolo Internet (IP) y otras redes
– C.4/13 – Gestión de recursos en la RDSI-BA y en relación con el protocolo Internet (IP)
– C.6/13 – Calidad de funcionamiento de las redes basadas en el protocolo Internet (IP) y la infraestructura mundial de la información emergente
– C.7/13 – Calidad de funcionamiento respecto a la transferencia de células del modo de transferencia asíncrona (ATM) de la RDSI-BA y la disponibilidad
– C.8/13 – Calidad de funcionamiento respecto a errores de transmisión y disponibilidad
– C.10/13 – Arquitectura de la red medular y principios de interfuncionamiento
– C.11/13 – Mecanismos para hacer posible que los servicios basados en el protocolo Internet (IP) funcionen en redes públicas

CE 15	Redes de fibra óptica y otras redes de transporte *Comisión de Estudio Rectora sobre transporte por la red de acceso y sobre tecnología óptica.*

La CE 15 (C. 14/15), en su Cuestión 14, se encarga de especificar los requisitos de gestión y control, y el soporte de los modelos de información para equipos de transporte. Las Cuestiones 14/15 siguen los lineamientos del marco y conceptos para la RGT establecidos por el UIT-T para la definición de dichos requisitos y modelos. La gestión de la seguridad es una de las cinco categorías funcionales clave en la gestión de la RGT. La gestión de la seguridad ha estado, y sigue estando, dentro del alcance de las Cuestiones 14/15.

- Requisitos para la gestión de equipos de transporte: En G.7710/Y.1701, G.784, y G.874 se tratan las funciones de gestión de equipos (EMF, *equipment management functions*) dentro de un elemento de red (NE, *network element*) de transporte que son comunes a varias tecnologías, específicas a los NE de la SDH, y de la OTN, respectivamente. Se describen aplicaciones para Fecha & hora, gestión de averías, gestión de configuración, gestión de cuenta, gestión de seguridad y gestión de calidad de funcionamiento. De estas aplicaciones salen las especificaciones de funciones EMF y sus requisitos. Actualmente se estudian los requisitos de seguridad en estas Recomendaciones.

- Requisitos y arquitecturas de redes de comunicación de datos: En G.7712/Y.1703 se definen los requisitos arquitecturales para una RCD capaz de soportar las comunicaciones de gestión distribuida relacionadas con la RGT, las comunicaciones de señalización distribuida relacionadas con la Red de transporte con conmutación automática (ASTN, *automatically switched transport network*), y otras comunicaciones distribuidas (por ejemplo, Comunicaciones vocales o de servicios, o descarga de Software). En diversas aplicaciones (por ejemplo, RGT, ASTN, etc.) se requiere una red de comunicaciones basada en paquetes para transportar información entre los componentes. Por ejemplo, en la RGT se necesita una red de comunicación, denominada red de comunicaciones de gestión (RCG) para el transporte de mensajes de gestión entre los componentes de la RGT (por ejemplo, componentes NEF y OSF). En la ASTN se necesita una red de comunicación, denominada red de comunicaciones de señalización (RCS) para el transporte de mensajes de señalización entre los componentes de la ASTN (CC, por ejemplo). En la Rec. UIT-T G.7712/Y.1703 se hace referencia a la Rec. UIT-T M.3016 en lo que concierne a los requisitos de seguridad de la RCG. De otra parte, los requisitos de seguridad de la SCN se definen en G.7712/Y.1703.
- Gestión de conexión y llamada distribuida: En G.7713/Y.1704 se proporcionan los requisitos para la gestión de conexión y llamada distribuida, tanto para la interfaz de red de usuario (UNI, *user network interface*) como para la interfaz de nodo de red (NNI, *network node interface*). Gracias a estos requisitos se especifican las comunicaciones a través de las interfaces, a fin lograr operaciones de conexión y llamada automatizadas. Se especifican los atributos de seguridad, entre otros, para permitir la verificación de las operaciones de llamada y conexión (por ejemplo, puede haber información que permita la autenticación de la petición de llamada, y tal vez la verificación de su integridad).

- Arquitectura y requisitos para el encaminamiento en redes ópticas con conmutación automática: En G.7715/Y.1706 se especifican los requisitos y arquitectura para las funciones de encaminamiento que se utilizan para el establecimiento de conexiones conmutadas (SC, *switched connections*) y conexiones lógicas permanentes (SPC, *soft permanent connections*) en el marco de la red óptica con conmutación automática (ASON, *automatically switched optical network*). Los temas principales cubiertos en esta Recomendación son: arquitectura de encaminamiento ASON, componentes funcionales incluida la selección de trayecto, atributos de encaminamiento, mensajes abstractos y diagramas de estado. En esta Recomendación se hace referencia a las Recomendaciones UIT-T M.3016 y X.800 en lo que concierne a los requisitos de seguridad. En particular, se afirma que, según el contexto de utilización de un protocolo de encaminamiento, los objetivos globales de seguridad definidos en M.3016, en lo que tiene que ver con confidencialidad, integridad de datos, imputabilidad y disponibilidad, pueden adquirir diversos niveles de importancia. Conviene efectuar un análisis de amenazas para un protocolo de encaminamiento propuesto que tenga en cuenta, basándose en X.800: la suplantación de identidad, la escucha clandestina, el acceso no autorizado, la pérdida o degradación de información (incluidos los ataques por respuesta), el repudio, la falsificación y la negación de servicio.
- Marco de gestión de la ASON: En G.fame se tratan aspectos de gestión del plano de control ASON y las interacciones entre ésta y el plano de gestión. Se incluirán requisitos de gestión para el plano de control de: averías, configuración, contabilidad, calidad de funcionamiento y seguridad.

Cuestiones principales relacionadas con la seguridad:
– C.14/15 – Gestión de red para sistemas y equipos de transporte

CE 16	Servicios, sistemas y terminales multimedios *Comisión de Estudio Rectora sobre terminales, servicios y sistemas multimedios comercio electrónico y empresa electrónica.*

La CE 16 es la Comisión de Estudio Rectora sobre terminales, servicios y sistemas multimedios y sobre comercio electrónico y empresa electrónica. La Cuestión G (del GT2/16) trata sobre "Seguridad de sistemas y servicios multimedios", en particular sobre:

Aplicaciones multimedios (MM, *advanced multimedia*) avanzadas como la telefonía a través de redes basadas en paquetes, la VoIP, la conferencia y colaboración interactivas; mensajería MM, la transmisión en flujo continuo de Audio/Video y otras, que están sujetas a diversas amenazas cruciales de seguridad en entornos heterogéneos. Algunos de los riesgos en potencia, en particular tratándose de redes basadas en el IP, son la utilización inadecuada, la manipulación con malas intenciones, la escucha clandestina y la negación de servicio.

Se suele aceptar que todas estas aplicaciones tienen necesidades similares de seguridad que, por ende, se pueden satisfacer mediante medidas genéricas de seguridad; p.ej. de seguridad de red. Ahora bien, con frecuencia las aplicaciones MM tienen necesidades particulares de seguridad especifica para cada aplicación que es necesario suplir con medidas en la capa de aplicación. La Cuestión G se centra en los aspectos de seguridad de aplicación de las aplicaciones MM y toma medidas complementarias de seguridad de red cuando conviene.

Cuestiones principales relacionadas con la seguridad:
– C.G/16 – Seguridad de los sistemas y servicios multimedios

CE 17	Redes de datos y Software para las telecomunicaciones *Comisión de Estudio Rectora sobre retransmisión de trama, seguridad de sistemas de comunicación, lenguajes y técnicas de descripción.*

Mandato: Se encarga de los estudios sobre redes de comunicación de datos, y comunicaciones de sistemas abiertos, incluidos el interfuncionamiento de redes, sistemas de directorio y servicios de seguridad, así como lenguajes técnicos, el método para su utilización y otros asuntos relacionados con aspectos de soporte lógico de los sistemas de telecomunicaciones.

Cuestiones principales relacionadas con la seguridad:
– C.9/17 – Servicios y sistemas directorio
– C.10/17 – Requisitos de seguridad, modelos y directrices para los servicios y sistemas de comunicaciones
(NOTA – La CE 17 aceptó dividir la Cuestión 10/17 en seis Cuestiones independientes, a saber la G/17 – Proyecto de seguridad; H/17 – Arquitectura y marco de seguridad; I/17 – Ciberseguridad; J/17 – Gestión de la seguridad; K/17 –Telebiométrica; y L/17 – Servicios de comunicación seguros)

CEE	Comisión de Estudio Especial sobre las IMT y sistemas ulteriores *Comisión de Estudio Rectora sobre las IMT-2000 y sistemas ulteriores, y para movilidad.*
La CEE ha incluido el tema de la seguridad como aspecto clave en sus Recomendaciones de referencia para los miembros de la familia IMT-2000 (3G) identificados en sus series de Recomendaciones UIT-T Q.1741.x (3GPP) y Q.1742.x (3GPP2). Se incluye una evaluación de las amenazas previstas y una lista de los requisitos de seguridad para enfrentarlas, los objetivos y principios de seguridad, una arquitectura de seguridad definida (es decir, las características y mecanismos de seguridad), los requisitos del algoritmo criptográfico, los requisitos de intercepción legal, y la arquitectura y funciones para esta última. De ello se encargan las Cuestiones 3, 6&7/CEE. El objetivo básico de los estudios sobre la intercepción legal es poder identificar información útil sobre intercepción y verificación que los operadores deben proporcionar a las autoridades en cada país. La información relacionada con la intercepción y el contenido de las comunicaciones puede ser o no tecnológicamente independiente de las redes móviles 3G o 3G evolucionadas.	
Cuestiones principales relacionadas con la seguridad: – 3/CEE – Identificación de los sistemas IMT-2000 actuales y de los que evolucionan – 6/CEE – Armonización de los sistemas IMT-2000 que evolucionan – 7/CEE – Convergencia de sistemas fijos y sistemas IMT-2000 actuales	

Elementos de seguridad del UIT-T

Marco de arquitectura de seguridad

X.800 – Arquitectura de seguridad
X.802 – Modelo de seguridad de capas más bajas
X.803 – Modelo de seguridad de capas superiores
X.805 – Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo
X.810 – Marcos de seguridad para sistemas abiertos: Visión general
X.811 – Marcos de seguridad para sistemas abiertos: Marco de autenticación
X.812 – Marcos de seguridad para sistemas abiertos: Marco de control de acceso
X.813 – Marcos de seguridad en sistemas abiertos: Marco de no rechazo
X.814 – Marcos de seguridad para sistemas abiertos: Marco de confidencialidad
X.815 – Marcos de seguridad para sistemas abiertos: Marco de integridad
X.816 – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad

Protocolos

X.273 – Protocolo de seguridad de la capa de red
X.274 – Protocolo de seguridad de la capa de transporte

Seguridad en la retransmisión de tramas

X.272 – Compresión de datos y privacidad en las redes con retransmisión de tramas

Técnicas de seguridad

X.841 – Objetos de información de seguridad
X.842 – Directrices para el uso y gestión de servicios a tercera parte confiable
X.843 – Especificación de servicios de tercera parte confiable para soportar la aplicación de firmas digitales

Servicios de directorio y autenticación

X.500 – Visión de conjunto de conceptos, modelos y servicios
X.501 – Modelos
X.509 – Marco para los certificados de claves públicas y de atributos
X.519 – Especificaciones de protocolo

Seguridad de gestión de redes

M.3010 – Principios para una red de gestión de las telecomunicaciones
M.3016 – Visión general de la seguridad en la red de gestión de las telecomunicaciones
M.3210.1 – Servicios de gestión de red de gestión de las telecomunicaciones para la seguridad de las IMT-2000
M.3320 – Marco de los requisitos de gestión para la interfaz X de la RGT
M.3400 – Funciones de gestión de la red de gestión de las telecomunicaciones

Gestión de sistemas

X.733 – Función señaladora de alarmas
X.735 – Función control de ficheros registro cronológico
X.736 – Función señaladora de alarmas de seguridad
X.740 – Función de pista de auditoría de seguridad
X.741 – Objetos y atributos para el control de acceso

Facsímil

T.30 Anexo G – Procedimientos para la transmisión segura de documentos por facsímil grupo 3 mediante la utilización de los sistemas HKM y HFX
T.30 Anexo H – Seguridad en facsímil del grupo 3 basada en el algoritmo RSA
T.36 – Capacidades de seguridad para su utilización con terminales facsímil del grupo 3
T.503 – Perfil de aplicación de documento para el intercambio de documentos facsímil del grupo 4
T.563 – Características de terminal para aparatos facsímil del grupo 4

Sistemas de televisión y cable

J.91 – Métodos técnicos para asegurar la privacidad de las transmisiones internacionales de televisión a larga distancia
J.93 – Requisitos del acceso condicional en la distribución secundaria de televisión digital por sistemas de televisión por cable
J.170 – Especificación de seguridad de IPCablecom

Comunicaciones multimedios

H.233 – Sistemas de confidencialidad para servicios audiovisuales
H.234 – Sistema de gestión de claves de criptación y de autenticación para servicios audiovisuales
H.235 – Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)
H.323 Anexo J – Sistemas de comunicación multimedios basados en paquetes – Seguridad para el anexo F/H.323 (Tipos de punto extremo simples)
H.350.2 – Arquitectura de servicios de directorio para H.235
H.530 – Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510

Las Recomendaciones del UIT-T pueden consultarse en el sitio de la UIT en la red: http://www.itu.int/publications/bookshop/how-to-buy.html (en este sitio figura también información sobre el acceso gratuito a un número limitado de Recomendaciones del UIT-T).

Entre otros importantes trabajos relativos a la seguridad que está realizando actualmente el UIT-T, cabe señalar los siguientes:

Telebiometría, gestión de la seguridad, seguridad de la movilidad, telecomunicaciones de urgencia

Para más información sobre el UIT-T y sus Comisiones de Estudio, consultar la siguiente dirección: http://www.itu.int/ITU-T