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

UIT-T

Sector de Normalización de las Telecomunicaciones de la UIT

2006

Unión Internacional de Telecomunicaciones

UIT-T – Oficina de Normalización de las Telecomunicaciones (TSB)
Place des Nations – CH-1211 Ginebra 20 – Suiza
E-mail: tsbmail@itu.int Web: www.itu.int/ITU-T

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

Junio de 2006

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: Herb Bertine, David Chadwick, Martin Euchner, Mike Harrop, Sándor Mazgon, Stephen Mettler, Chris Radelet, Lakshmi Raman, Eric Rosenfeld, Neal Seitz, Rao Vasireddy, Tim Walker, Heung-Youl Youm, Joe Zebarth y a los Consejeros de la UIT/TSB.

Índice

Página

Página

Prefacio

Hasta hace relativamente poco tiempo, la seguridad de las telecomunicaciones y de las tecnologías de la información se limitaba a ámbitos como la banca o las aplicaciones aeroespaciales o militares. No obstante, con el rápido y amplio crecimiento de las comunicaciones de datos, particularmente gracias a Internet, la seguridad se ha convertido en una preocupación para todos.

Es posible que la importancia cada día mayor de la seguridad de las ICT se deba al gran número de incidentes debidos a virus, gusanos, piratas y amenazas a la privacidad de las personas. Pero la informática y el trabajo en redes son tan importantes para la vida de todos, que es absolutamente necesario aplicar medidas de seguridad eficaces para proteger los ordenadores y los sistemas de telecomunicaciones de los gobiernos, las industrias, los comercios, las infraestructuras críticas y los consumidores. Además, un número cada vez mayor de países disponen hoy en día de una legislación de protección de datos que requiere el cumplimiento de normas reconocidas de confidencialidad e integridad de datos.

Es evidente que la seguridad tiene que ser un proceso cuidadosamente desarrollado en todas sus fases, desde la concepción y el diseño hasta la implementación e instalación. Es indispensable que la seguridad esté presente desde un principio en el desarrollo de las normas y no durante su aplicación. De no considerarse adecuadamente estos aspectos de la seguridad durante la fase de diseño de las normas y el desarrollo de los sistemas se pueden crear muy fácilmente vulnerabilidades a la hora de su aplicación. Los comités normativos tienen una función fundamental que desempeñar en la protección de las telecomunicaciones y los sistemas de tecnologías de la información manteniendo una conciencia de seguridad, velando para que se tenga debidamente en cuenta la seguridad en las especificaciones y prestando ayuda a los implementadores y los usuarios para garantizar la robustez de los sistemas y servicios de comunicaciones.

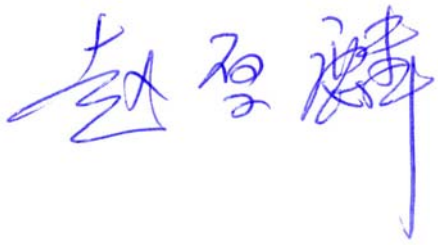
Si bien desde hace muchos años el UIT-T ha tratado el tema de la seguridad de las telecomunicaciones y de las tecnologías de la información, no siempre ha sido fácil disponer del material elaborado al respecto o simplemente saber dónde encontrarlo. Con este manual se pretende reunir toda la información disponible al respecto sobre la labor desempeñada por el UIT-T.

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.

La primera versión de este manual, la versión de 2003, se publicó en diciembre de 2003 justo antes de la celebración de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información (CMSI). Alentados por la entusiasta acogida que tuvo entre la comunidad de ICT mundial y en vista de las valiosas propuestas y comentarios recibidos de los lectores, publicamos una segunda versión. La versión publicada en octubre de 2004 tenía una nueva estructura además de nuevo material y algunos capítulos más ampliados. Esta tercera versión, de 2006, tiene en cuenta la nueva estructura de las Comisiones de Estudio y las Cuestiones dimanantes de la Asamblea Mundial sobre Normalización de las Telecomunicaciones que se celebró en Florianópolis del 5 al 14 de octubre de 2004 (AMNT-04).

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, realizaron la mayor parte del trabajo de la primera versión. También quiero expresar mi agradecimiento a todos aquellos que nos han presentado sus propuestas y que han contribuido con su trabajo a esta nueva versión. En especial quiero dar las gracias al Sr. Herbert Bertine, Presidente de la Comisión de Estudios 17 del UIT-T, Comisión de Estudio Rectora en materia de seguridad, y a todo el equipo de colaboradores de la Comisión de Estudio 17 y de otras Comisiones de Estudio del UIT-T.

Confío en que este manual será una guía útil para todos aquellos que deseen resolver problemas relativos a la seguridad y agradeceré todo comentario procedente de los lectores para las futuras ediciones.



Houlin Zhao

Director de la Oficina de Normalización
de las Telecomunicaciones, UIT

Ginebra, junio de 2006

Resumen y comentarios

La industria de las comunicaciones ha contribuido de manera sobresaliente a la mejora de la productividad y la eficiencia en todo el mundo, con el desarrollo de infraestructuras de comunicaciones que conectan a las comunidades de prácticamente todos los segmentos industriales y todas las partes del mundo. Esto es posible en gran parte gracias a la implementación de normas elaboradas por organizaciones como el UIT-T. Estas normas garantizan la compatibilidad y eficacia de las operaciones de red y sientan las bases para las redes de la próxima generación (NGN). Si bien las normas existentes satisfacen las necesidades de los usuarios y de la industria, la mayor utilización de protocolos e interfaces abiertos, la variedad de nuevos actores, la impresionante diversidad de aplicaciones y plataformas, así como la presencia de implementaciones no siempre adecuadamente probadas, han abierto nuevas posibilidades de utilización malintencionada de las redes. En estos años han aumentado significativamente las violaciones de seguridad informática en todo el mundo (por ejemplo, la diseminación de virus y ataques que han resultado en una violación de la confidencialidad de datos almacenados), con importantes secuelas de costos en muchos casos. Así las cosas, cabe preguntarse cómo se puede soportar una infraestructura abierta de comunicaciones sin que se exponga su información a problemas de seguridad. En general, la respuesta reside en la elaboración de especificaciones suficientemente robustas para garantizar que pueden contrarrestarse las amenazas a la seguridad en cualquier esfera de la infraestructura de comunicaciones. Con este objetivo en mente, los esfuerzos que realizan los grupos de normalización incluyen la elaboración de arquitecturas y marcos de seguridad normalizados, normas para la gestión de la seguridad, protocolos y técnicas específicos a la seguridad para proteger los protocolos de comunicaciones, así como la adopción de medidas adecuadas para minimizar las posibles vulnerabilidades de las normas de comunicaciones en general.

Con este manual de seguridad se pretende presentar de manera general las Recomendaciones desarrolladas por el UIT-T –en algunos casos en colaboración con otras organizaciones de normalización, para proteger 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 que proporcionen una taxonomía común que permita discutir los conceptos correspondientes.

En la sección 2 se presentan las arquitecturas y elementos de seguridad básicos definidos en las Recomendaciones del UIT-T, 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 de los datos, no repudio, control de acceso, seguridad de las comunicaciones y disponibilidad. Estos principios generales se utilizan como base para la elaboración de las normas relativas a servicios y mecanismos de seguridad.

En la sección 3 se presentan los conceptos de seguridad fundamentales de amenazas, vulnerabilidades y riesgos, se explican las relaciones entre estos conceptos y su relevancia para los organismos de normalización.

En la sección 4, basándose en la información suministrada en las secciones anteriores, se determinan los requisitos de seguridad para las redes de telecomunicaciones. En concreto, en esta sección se analizan los objetivos de seguridad de las redes de telecomunicaciones y los servicios que pueden utilizarse para lograr estos objetivos.

En la sección 5 se exponen conceptos importantes como son las claves públicas y las infraestructuras de gestión de privilegios. Estas infraestructuras, y los mecanismos que los soportan son de particular relevancia a la hora de proporcionar servicios de autenticación y autorización.

El UIT-T ha elaborado disposiciones de seguridad en diversos sistemas y servicios que se definen en sus Recomendaciones, y este manual trata principalmente de las aplicaciones, como se muestra en la sección 6. En la sección 6 se analizan las aplicaciones de voz y multimedias por IP (H.323 e IPCablecom), de atención de 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, también para la infraestructura de red y la gestión de los servicios. En la sección 6 se incluyen también ejemplos de normas en las que hay disposiciones de seguridad que conciernen a los aspectos de gestión de red.

En la sección 7 se aborda el tema de la disponibilidad y las capas de infraestructura de seguridad. Se trata de dos esferas muy importantes que son competencia del UIT-T y que no siempre se han considerado como factores de seguridad. Se ofrece información sobre los cálculos de disponibilidad y las maneras de mejorarla en una red de transporte. Esta sección concluye con unas directrices de seguridad para las instalaciones exteriores.

En la sección 8 se enumeran las directrices recientemente aprobadas por el UIT-T sobre organización de incidentes y tratamiento de incidentes de seguridad. Se admite fácilmente que este asunto es de importancia capital, frente al creciente problema de las amenazas de seguridad que sufren las infraestructuras de los sistemas de telecomunicaciones e información.

Además, este Manual contiene la actual versión del Catálogo de Recomendaciones del UIT-T sobre aspectos de seguridad –la lista presentada en el anexo A es extensa y reafirma la importancia del trabajo del UIT-T sobre la seguridad. Se presenta asimismo 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 de definiciones de seguridad aprobadas por el UIT-T, desarrollado por la Comisión de Estudio 17 del UIT-T). Todo esto se incluye en el anexo B. 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. Este manual abarca otros aspectos de la seguridad, en particular la disponibilidad –sobre la que el UIT-T tiene mucha experiencia– y la degradación ambiental, tema en el que también trabaja el Sector. También incluye los resultados que se han obtenido en la labor de normalización para la seguridad desde la publicación de la segunda edición. Además, sólo se cubren aspectos basados en el trabajo ya concluido; los resultados de trabajos en curso se tratarán en ediciones futuras del manual.

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

2 Arquitecturas y servicios de seguridad básicos

En la labor de normalización de las comunicaciones llevada a cabo en la década de 1980 se reconoció la necesidad de abordar los elementos de la arquitectura de seguridad y se definió una arquitectura de seguridad de sistemas abiertos (Rec. UIT-T X.800). No obstante, también quedó claro que se trataba sólo de la primera fase de desarrollo de una serie de normas para soportar servicios y mecanismos de seguridad. Esta labor, que en gran parte se llevó a cabo en colaboración con la ISO, dio lugar a más Recomendaciones, por ejemplo con modelos y marcos de seguridad que especifican los tipos de protección que pueden aplicarse a cada entorno. Además, se identificó la necesidad de crear otras arquitecturas de seguridad, por ejemplo para el procesamiento distribuido abierto y para los sistemas de comunicaciones de extremo a extremo. La recientemente publicada Rec. UIT-T X.805 colma esta necesidad y sirve de complemento a otras Recomendaciones de la serie X.800 con soluciones para la seguridad de las redes de extremo a extremo.

2.1 Arquitectura de seguridad de sistemas abiertos (X.800)

La primera arquitectura de seguridad de comunicaciones normalizada fue la arquitectura de seguridad de sistemas abiertos de la Rec. UIT-T X.800. En esta Recomendación se definen los elementos de la arquitectura de seguridad generales que pueden aplicarse según los requisitos de protección. En concreto, X.800 presenta una descripción general de los servicios de seguridad y los mecanismos que son necesarios. También se define la forma más apropiada de implementación de los servicios (OSI, *open systems interconnection*) de seguridad, definiendo un modelo de referencia básico de la interconexión de sistemas abiertos de siete capas.

La Rec. UIT-T X.800 sólo trata de los aspectos visibles del trayecto de comunicaciones que permiten a los sistemas extremos realizar una transferencia segura de información entre ellos. No es una especificación para la implementación de sistemas ni define procedimientos para determinar si un sistema es conforme con ésta o cualquier otra norma de seguridad. Tampoco indica detalladamente las medidas de seguridad adicionales que puedan ser necesarias en los sistemas extremos para soportar las características de seguridad de interconexión de sistemas abiertos (OSI).

Aunque X.800 se elaboró específicamente como una estructura de seguridad OSI, la aplicabilidad y aceptación de los conceptos subyacentes de esta Recomendación es mucho más amplia. La norma es especialmente importante porque representa el primer consenso a nivel internacional sobre las definiciones de servicios de seguridad básicos (*autenticación, control de acceso, confidencialidad de los datos, integridad de los datos* y *no repudio*) así como de servicios (invasivos) más generales:

funcionalidad fiable, detección de eventos, auditoría de seguridad y *recuperación*. Antes de la publicación de X.800 había una gran divergencia de opiniones sobre los servicios de seguridad básicos necesarios y las funciones de cada uno de ellos. X.800 es el fruto de un consenso internacional muy claro sobre estos servicios (los servicios de seguridad básicos se explican más detalladamente en la sección 2.3).

El valor y la aplicabilidad general de X.800 se deben a su carácter de consenso amplio sobre el significado de los términos utilizados para describir las características de seguridad, sobre los servicios de seguridad necesarios para proteger las comunicaciones de datos, y sobre la naturaleza de estos servicios de seguridad.

Durante la elaboración de X.800 se identificó la necesidad de elaborar más normas de seguridad relacionadas con las comunicaciones. Se empezó a trabajar en la definición de distintas normas y Recomendaciones sobre arquitecturas complementarias. Algunas de éstas se exponen a continuación.

2.2 Modelos de seguridad de capas inferiores y de capas superiores (X.802 y X.803)

El objetivo de los modelos de seguridad de capas inferiores y capas superiores (Recs. UIT-T X.802 y X.803, respectivamente) es mostrar de qué manera pueden aplicarse los conceptos de seguridad desarrollados en los marcos de seguridad a esferas específicas de las arquitecturas de sistemas abiertos.

El objetivo del modelo en seguridad de capas superiores (X.803) es proporcionar a los normalizadores un modelo de arquitectura para el desarrollo de servicios de seguridad y protocolos independientes de la aplicación, en las capas superiores del modelo OSI de siete capas. La Recomendación indica dónde es conveniente implantar los servicios de seguridad y cómo están relacionados los servicios de las capas de sesión, presentación y aplicación. En concreto, en la Recomendación se describe cómo se tratan las funciones de transformación de seguridad (como el cifrado) en las capas de aplicación y presentación. Además, se introduce el concepto de *intercambio de seguridad*, y se explican los principios de *política de seguridad y estado de seguridad*.

El modelo de seguridad de capas inferiores (X.802) orienta el desarrollo de los protocolos y elementos de protocolos relacionados con la seguridad adecuados para las capas inferiores del modelo OSI. Describe las bases de las interacciones de seguridad entre las capas inferiores así como la ubicación de los protocolos de seguridad.

2.3 Los marcos de seguridad (X.810-X.816)

Los marcos de seguridad son representaciones completas y uniformes de los servicios de seguridad definidos en X.800. Su objetivo es tratar todos los aspectos de la aplicación de los servicios de seguridad en una arquitectura de seguridad específica, incluidas posibles futuras arquitecturas de seguridad. El objetivo de estos marcos es la protección de sistemas y objetos dentro de los sistemas, así como la interacción entre ellos. No se trata en estas Recomendaciones de metodología para la construcción de sistemas o mecanismos.

Los marcos tratan tanto de elementos de datos como de secuencias de operaciones (excluidos los elementos de protocolo) que se utilizan para obtener servicios de seguridad específicos. Estos servicios pueden aplicarse a las entidades comunicantes de los sistemas así como a los datos intercambiados y gestionados por los sistemas.

2.3.1 Presentación general de los marcos de seguridad (X.810)

La Recomendación general sobre los marcos de seguridad presenta otros marcos y describe conceptos comunes (dominios de seguridad, autoridades de seguridad y políticas de seguridad) que se utilizan en todos estos marcos. También se especifica un formato de datos genérico que puede utilizarse para transmitir de manera segura la información de autenticación y de control de acceso.

2.3.2 El marco de autenticación (X.811)

Autenticar es garantizar que una entidad tiene efectivamente la identidad que pretende. Las entidades incluyen no sólo a los usuarios humanos, sino también a los dispositivos, servicios y aplicaciones. La autenticación puede asimismo garantizar que no se trata de un caso de usurpación de identidad o reproducción no autorizada de una comunicación anterior. En X.800 se identifican dos tipos de autenticación: *autenticación de origen de los datos* (es decir, comprobar si es la fuente que se pretende) y *autenticación de la entidad par* (es decir, comprobar si es efectivamente la entidad par que se pretende).

El marco de autenticación ocupa el primer lugar en una jerarquía de normas de autenticación que determinan los conceptos, la nomenclatura y una clasificación de los métodos de autenticación. Este marco define los conceptos básicos de autenticación, identifica las posibles clases de mecanismos de autenticación, define los servicios de estas clases de mecanismos, identifica los requisitos funcionales de los protocolos que soportan estas clases de mecanismos e identifica los requisitos generales de gestión de la autenticación.

La autenticación suele ir después de la identificación. La información utilizada para la identificación, la autenticación y la autorización debe estar protegida.

2.3.3 Marco de control de acceso (X.812)

El *control de acceso* es la prevención de la utilización no autorizada de un recurso, incluida la prevención de utilización de un recurso de manera no autorizada. El control de acceso garantiza que sólo el personal o los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y aplicaciones.

El marco de control de acceso describe un modelo que incluye todos estos aspectos del control de acceso en los sistemas abiertos, su relación con otras funciones de seguridad (como la autenticación y la auditoría), y los requisitos de gestión del control de acceso.

2.3.4 Marco de no repudio (X.813)

El *no repudio* es la capacidad de evitar que las entidades puedan negar en etapas posteriores que han realizado una acción. El no repudio supone la creación de pruebas que más adelante se podían utilizar para demostrar la falsedad de un argumento. En X.800 se describen dos formas de servicio de no repudio: *el no repudio con prueba de entrega*, que se utiliza contra la falsa denegación del receptor de que ha recibido los datos, y el *no repudio con prueba de origen* que se utiliza contra la falsa denegación del envío de los datos por parte del emisor. No obstante, en términos más generales, el concepto de no repudio puede aplicarse a muchos contextos distintos, como el no repudio de creación, presentación, almacenamiento, transmisión y recepción de datos.

El marco de no repudio amplía los conceptos de los servicios de seguridad de no repudio descritos en X.800 y establece un marco para su aplicación. Identifica asimismo posibles mecanismos para soportar estos servicios y los requisitos de gestión generales del no repudio.

2.3.5 Marco de confidencialidad (X.814)

La *confidencialidad* es la garantía de que la información no se divulgará ni se pondrá a disposición de individuos, entidades o procesos no autorizados.

El objetivo del servicio de confidencialidad es proteger la información contra la divulgación no autorizada. El marco de confidencialidad prevé esta garantía para la consulta, la transferencia y la gestión de la información, definiendo conceptos básicos de confidencialidad, las posibles clases de confidencialidad así como las instalaciones requeridas para cada mecanismo de confidencialidad, identificando los servicios de gestión y los servicios anexos necesarios y definiendo la interacción con otros servicios y mecanismos de seguridad.

2.3.6 Marco de integridad (X.815)

La *integridad de los datos* es la garantía de que los datos no han sido alterados sin autorización. En general, un servicio de integridad colma la necesidad de garantizar que los datos no han sido alterados o de señalar las alteraciones al usuario. Aunque hay diversos aspectos de integridad (como la integridad de los datos y la integridad del sistema), X.800 se centra casi exclusivamente en la integridad de los datos.

En este marco se consideran los distintos aspectos de integridad de los datos: en la consulta, la transferencia y la gestión de información. Define los conceptos básicos de integridad, identifica posibles clases de mecanismos de integridad así como las herramientas de cada uno de ellos, identifica los procesos de gestión necesarios para cada clase de mecanismo y aborda la interacción del mecanismo de integridad y los servicios anexos con otros servicios y mecanismos de seguridad.

2.3.7 El marco de auditoría y alarmas (X.816)

Una *auditoría de servicio* es un examen y control independientes de los archivos y actividades del sistema para comprobar si los controles del sistema son adecuados, garantizar el cumplimiento de la política y los procedimientos operativos establecidos, detectar infracciones de seguridad y recomendar cualquier cambio de control, política o procedimiento. Una *alarma de seguridad* es un mensaje generado cuando se detecta un evento relacionado con la seguridad, que según la política de seguridad es una situación de alarma.

El marco de auditoría y alarmas define los conceptos básicos y establece un modelo general de auditoría y alarmas de seguridad, identifica los criterios para la realización de una auditoría de seguridad y la creación de una alarma, identifica posibles clases de mecanismos de auditoría y alarma, define los servicios de estas clases de mecanismos, identifica los requisitos funcionales para soportar estos mecanismos e identifica los requisitos generales de gestión de la auditoría y las alarmas de seguridad.

2.4 Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo (X.805)

Se ha revisado recientemente la arquitectura de seguridad de redes. El resultado se refleja en la Rec. UIT-T X.805 que define una arquitectura para garantizar la seguridad extremo a extremo. Esta arquitectura puede aplicarse a distintos tipos de redes en los que es importante garantizar la seguridad extremo a extremo, independientemente de la tecnología que utilice la red. 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 contrarrestarlas o preverlas dependen de cada aplicación.

Esta arquitectura de seguridad se define teniendo en cuenta dos conceptos principales, a saber las capas y los planos. El concepto de 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, 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 concepto 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 sección 6.4, tiene que ver con las actividades, operaciones, administración, mantenimiento y aprovisionamiento (OAM&P, *operations, administration, maintenance and provisioning*) 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 que son las capas de seguridad y los planos de seguridad (tres de cada uno de ellos), en la arquitectura se definen ocho dimensiones de seguridad, descritas a continuación que tratan la seguridad de red. Desde el punto de vista de la arquitectura, 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 2-1 se indican los planos, capas y dimensiones de seguridad de la arquitectura de seguridad. En la sección 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.

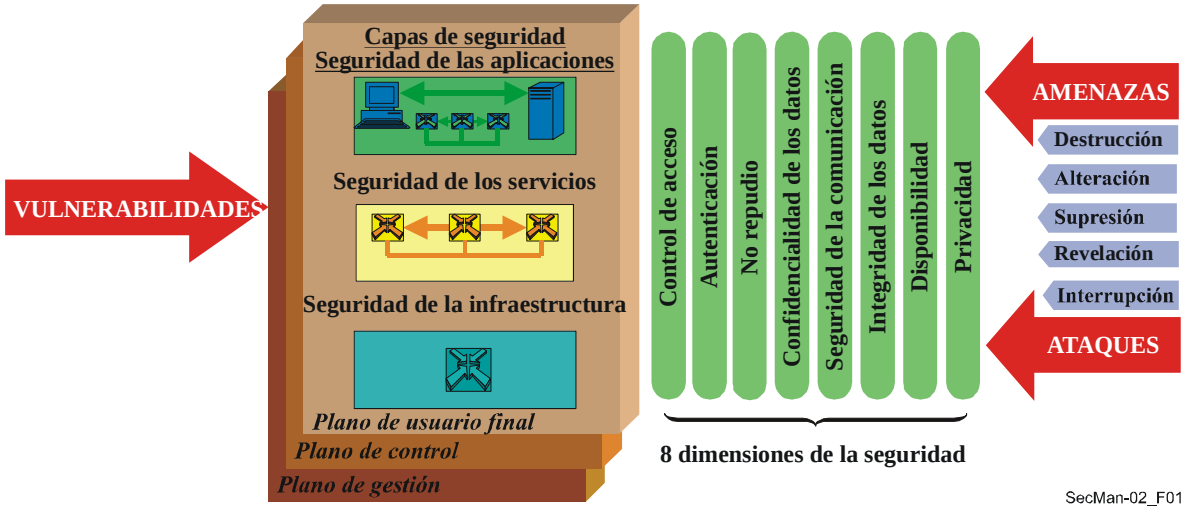


Figura 2-1 – Elementos de la arquitectura de seguridad de la Rec. UIT-T X.805

X.805 se basa en algunos conceptos de X.800 y en los marcos de seguridad (X.810-X.816) que se han expuesto anteriormente. Las funciones de los servicios de seguridad básicos de X.800 (*control de acceso, autenticación, confidencialidad de los datos, integridad de los datos y no repudio*) reflejan las correspondientes funciones de las dimensiones de seguridad de X.805 (que se muestran en la figura 2-1). Además, las dimensiones de seguridad de seguridad de las comunicaciones, disponibilidad y privacidad de X.805 ofrecen nuevos tipos de protección para la red. Estas ocho dimensiones de seguridad se exponen a continuación.

– 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 aplicaciones.

– La dimensión de seguridad *autenticación* permite comprobar la identidad de las entidades comunicantes. La autenticación garantiza la validez de las identidades que anuncian las entidades que participan en la comunicación (persona, dispositivo, servicio o aplicación) y garantiza que ninguna de estas entidades ha usurpado una identidad o está reproduciendo una comunicación anterior sin autorización.

– La dimensión de seguridad *no repudio* impide que una persona o una entidad nieguen haber realizado una acción concreta en relación con los datos, presentando las pruebas de esas acciones en la red (prueba de obligación, intención o compromiso; prueba de origen de los datos, prueba de propiedad, prueba de utilización de recursos). Garantiza la disponibilidad de pruebas que pueden presentarse a terceros y que permiten demostrar que ha ocurrido algún tipo de evento o acción.

– La dimensión de seguridad *confidencialidad de los datos* impide la divulgación no autorizada de los datos. La confidencialidad de los datos garantiza que las entidades no autorizadas no pueden entender el contenido de los datos. A menudo se utilizan métodos tales como la criptación, listas de control de acceso y permisos de acceso a ficheros para garantizar la confidencialidad de datos.

– La dimensión de seguridad *seguridad de la comunicación* garantiza que los flujos de información sólo tienen lugar entre puntos extremos autorizados (la información no puede desviarse ni ser interceptada cuando fluye entre estos dos puntos extremos).

– La dimensión de seguridad *integridad de los datos* garantiza que los datos son correctos y exactos. Los datos están protegidos contra las acciones no autorizadas de modificación, supresión, creación y copia, y en su caso se señalan estas acciones no autorizadas.

– La dimensión de seguridad *disponibilidad* garantiza que ningún evento que pueda ocurrir en la red impedirá el acceso autorizado a los elementos, la información almacenada, los flujos de información, los servicios y las aplicaciones de la red. Las soluciones de recuperación en caso de desastre y para reestablecimiento de la red se incluyen en esta categoría.

– La dimensión de seguridad *privacidad* impide conocer información observando las actividades de la red, por ejemplo los sitios web que un usuario ha visitado, la ubicación geográfica del usuario y las direcciones IP y los nombres DNS de los dispositivos de una red del proveedor de servicios.

La arquitectura de seguridad X.805 es una referencia para definir políticas de seguridad globales, planes de respuesta ante incidentes y recuperación, y arquitecturas tecnológicas teniendo en cuenta cada una de las dimensiones de seguridad en cada una de las capas y planos durante la fase de

definición y planificación. La arquitectura de seguridad X.805 también puede servir de base para una evaluación de la seguridad, para determinar los efectos del programa de seguridad en las dimensiones, capas y planos de seguridad, cuando se aplican las políticas y procedimientos y se hace efectiva la tecnología. Una vez implantado, es necesario mantener el programa de seguridad, es decir, adaptarlo al entorno de seguridad cambiante. La arquitectura de seguridad X.805 puede contribuir a la gestión de las políticas y procedimientos de seguridad, los planes de respuesta ante incidentes y recuperación, y las arquitecturas tecnológicas, con modificaciones del programa de seguridad adaptadas a cada una de las dimensiones de seguridad en las capas y planos correspondientes.

3 Fundamentos de la protección: amenazas, vulnerabilidades y riesgos

Cuando se define un marco de seguridad es fundamental tener una visión clara de los elementos que hay que proteger, las amenazas de que pueden ser objeto, las vulnerabilidades que tiene cada uno de estos elementos y el riesgo general que corren tales elementos con respecto a las amenazas y vulnerabilidades.

En términos generales, en lo que concierne a la seguridad de las ICT, será necesario proteger los siguientes elementos:

- servicios de comunicaciones y de informática;
- información y datos, incluido el software y los datos relacionados con los servicios de seguridad; y
- los equipos y las instalaciones.

Según la definición de X.800, una *amenaza de seguridad* es una posible violación de seguridad, por ejemplo:

- divulgación no autorizada de la información;
- destrucción o modificación no autorizadas de los datos, los equipos u otros recursos;
- robo, eliminación o pérdida de información u otros recursos;
- interrupción o denegación de servicios; y
- usurpación de identidad o simulación de una entidad autorizada.

Las amenazas pueden ser *accidentales* o *intencionales* así como *activas* o *pasivas*. Una amenaza accidental es aquélla no premeditada, como un disfuncionamiento o fallo físico de un sistema o del software. Una amenaza intencionada es aquélla que una persona realiza como un acto deliberado. (Cuando la amenaza es intencionada se denomina *ataque*.) Una amenaza activa es la que ocasiona un cambio de estado, por ejemplo alteración de los datos o destrucción de equipos físicos. Una amenaza pasiva no ocasiona ningún cambio de estado. Las escuchas clandestinas son un ejemplo de amenaza pasiva.

Una *vulnerabilidad de seguridad* es un defecto o debilidad que puede explotarse para violar un sistema o la información que contiene (X.800). Una vulnerabilidad permite la ejecución de una amenaza.

Hay cuatro tipos de vulnerabilidades: vulnerabilidad por forma *de amenaza* que resulta de la dificultad de prever posibles amenazas futuras; vulnerabilidad por *diseño y especificación*, producida por errores o descuidos en el diseño de un sistema o del protocolo, que los hacen inherentemente vulnerables; vulnerabilidad por *implementación* que se produce como resultado de errores en la implementación del sistema o el protocolo; y vulnerabilidad por *funcionamiento y configuración* que resulta de la utilización errónea de opciones en las implementaciones o de políticas insuficientes de instalación (por ejemplo, no se impone la utilización de la criptación en una red WiFi).

El *riesgo de seguridad* es la medida de los efectos negativos que pueden resultar de explotarse una vulnerabilidad de seguridad, es decir, si se ejecuta una amenaza. Si bien nunca puede eliminarse el riesgo, uno de los objetivos de la seguridad es reducirlos a un nivel aceptable. Para ello es necesario entender las amenazas y vulnerabilidades para aplicar las contramedidas adecuadas (es decir, los servicios y mecanismos de seguridad).

Las amenazas y los agentes que las originan pueden cambiar, pero siempre habrá vulnerabilidades de seguridad durante toda la vida del sistema o el protocolo, a menos que se adopten las medidas necesarias para solventarlas. Si se trata de protocolos normalizados, los riesgos de seguridad relativos al protocolo pueden ser bastante importantes y de escala global, por lo que es importante entender e identificar estas vulnerabilidades y adoptar las medidas necesarias para contrarrestarlas.

Los organismos de normalización tienen la responsabilidad y también tienen medios privilegiados para solventar las vulnerabilidades de seguridad inherentes a las arquitecturas, los marcos, los protocolos y otras especificaciones. Incluso con un conocimiento adecuado de los riesgos, las vulnerabilidades y las amenazas que acechan al procesamiento de la información y las redes de comunicaciones, no podrá lograrse una seguridad adecuada a menos que se aplique una acción sistemática y conforme a las políticas pertinentes, políticas que es necesario examinar y actualizar periódicamente. Además, debe garantizarse una gestión de seguridad y un tratamiento de incidentes adecuados: identificación de la responsabilidad y determinación de acciones específicas para evitar cualquier incidente de seguridad o reaccionar ante él (las disposiciones, controles, contramedidas y salvaguardias que han de adoptarse o las medidas que han de aplicarse). El UIT-T está elaborando nuevas Recomendaciones que tratan de estos aspectos de la gestión de la seguridad.

4 Requisitos de seguridad de las redes de telecomunicaciones

En esta sección se exponen las consideraciones básicas sobre la necesidad y las características de la seguridad desde el punto de vista de los usuarios, incluidos los operadores de las redes de telecomunicaciones. Reflejan los requisitos expresados por las distintas partes del mercado de las telecomunicaciones. Este texto se refiere principalmente a la labor llevada a cabo con la aprobación de la Rec. UIT-T E.408, *Requisitos de seguridad de las redes de telecomunicaciones*. Esta Recomendación propone una visión general de los requisitos de seguridad y un marco que identifica las amenazas de seguridad para las redes de telecomunicaciones en general (tanto fijas como móviles, de voz y datos) y sirve de orientación en la planificación de contramedidas que pueden adoptarse para reducir los riesgos que suponen tales amenazas.

Se trata de una Recomendación genérica que no identifica ni aborda requisitos de redes específicas.

En vez de definir nuevos servicios de seguridad, se ha considerado la utilización de los servicios existentes definidos en otras Recomendaciones del UIT-T y en las normas pertinentes de otros organismos.

La implementación de los requisitos establecidos facilitará la cooperación internacional en las siguientes esferas, en lo que a seguridad de redes de telecomunicaciones atañe:

- compartición y diseminación de la información;
- coordinación en caso de incidentes y respuesta en caso de crisis;
- contratación y formación de profesionales de seguridad;
- coordinación en la aplicación de la normativa;
- protección de infraestructura y servicios críticos; y
- creación de una legislación adecuada.

Para que esta cooperación sea efectiva es fundamental que se implementen a nivel nacional los requisitos para los componentes nacionales de la red.

4.1 Motivos

La necesidad de un marco de seguridad de red genérico para las telecomunicaciones internacionales resulta 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 actos de violencia civil.

- Las *autoridades/comunidades públicas* 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 a nivel nacional e internacional.

Conviene que los requisitos de seguridad de las redes de telecomunicaciones se basen en normas de seguridad internacionalmente aceptadas: es preferible adherir a normas existentes y no crear nuevas. La prestación y utilización de servicios y mecanismos de seguridad puede ser muy costosa con respecto al valor de las transacciones que se protegen. Siendo así, es importante ser capaz de adaptar la seguridad a los servicios que se protegen, crear mecanismos y servicios de seguridad flexibles. Debido a la gran cantidad de combinaciones de características de seguridad posibles, es conveniente definir *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.

Es necesario proporcionar los servicios y mecanismos de seguridad para proteger las redes de telecomunicaciones contra ataques malintencionados, como la negación de servicio, la escucha clandestina, la simulación, la manipulación de mensajes (modificación, retardo, supresión, inserción, reproducción, reencaminamiento, encaminamiento erróneo, o reordenamiento de mensajes), el repudio o la falsificación. La protección incluye la prevención, detección y recuperación tras ataques, así como la gestión de la información relacionada con la seguridad. La protección también debe comprender medidas para evitar cortes de servicio debido a eventos naturales (clima, etc.) o ataques malintencionados (acciones violentas). Es necesario prever disposiciones que permitan las escuchas y la supervisión con autorización de las autoridades correspondientes.

4.2 Objetivos generales de seguridad para las redes de telecomunicaciones

En esta sección se describe el objetivo último de las medidas de seguridad adoptadas en las redes de telecomunicaciones, principalmente lo que deben lograr los requisitos de seguridad, más que la forma de aplicación.

Los objetivos de seguridad de las redes de telecomunicaciones son:

a) Únicamente los usuarios autorizados deben poder acceder y utilizar las redes de telecomunicaciones.

b) Los usuarios autorizados han de poder acceder a los elementos autorizados y utilizarlos.

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

d) Todos los usuarios deben ser responsables únicamente y exclusivamente de sus acciones en las redes de telecomunicaciones.

e) Para garantizar la disponibilidad, las redes de telecomunicaciones deben estar protegidas contra accesos u operaciones no solicitadas.

f) Debe ser posible extraer información relacionada con la seguridad de las redes de telecomunicaciones (pero sólo por parte de los usuarios autorizados).

g) Si se detectan violaciones de seguridad, deberán tratarse de manera controlada de conformidad con un plan predefinido para minimizar los posibles daños.

h) Cuando se detecte una violación de seguridad, debe ser posible restaurar los niveles de seguridad normales.

i) La arquitectura de seguridad de las redes de telecomunicaciones debe proporcionar cierta flexibilidad para soportar diversas políticas de seguridad, por ejemplo, una aplicación más o menos estricta de los mecanismos de seguridad.

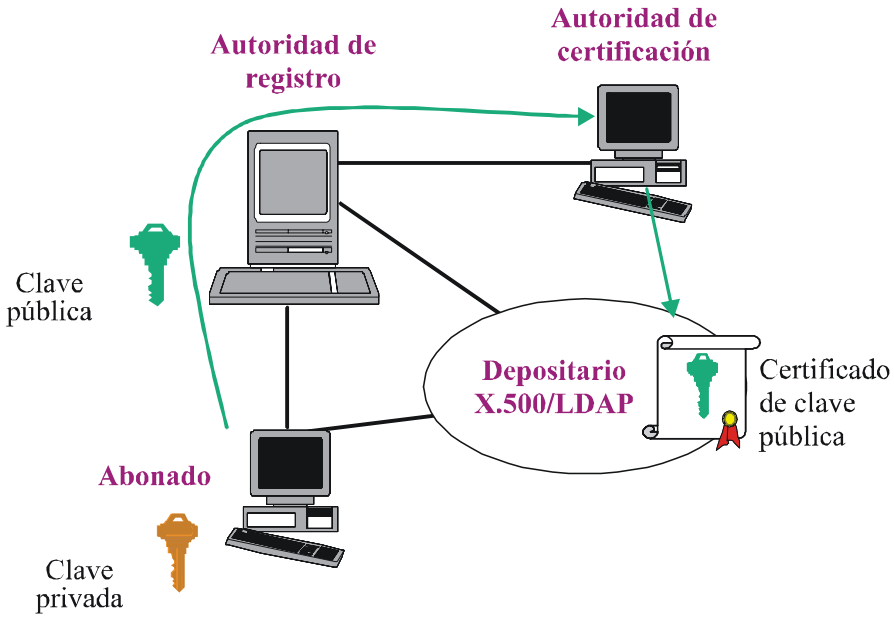
Por el término "acceder a los elementos" se entiende no sólo la posibilidad de realizar determinadas funciones, sino también leer la información.

La implementación de las siguientes medidas de seguridad permite lograr los primeros cinco objetivos de seguridad para las redes de telecomunicaciones antes mencionados:

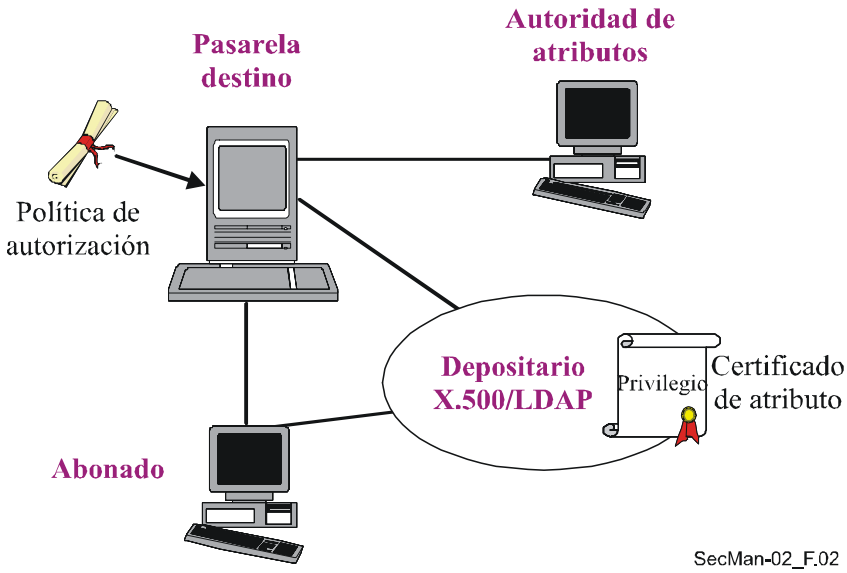
- confidencialidad;
- integridad de los datos; (evidentemente también se requiere la integridad de los programas del sistema);
- responsabilidad, incluida la autenticación, no repudio y control de acceso; y
- disponibilidad.

5 Infraestructuras de clave pública y de gestión de privilegios

La Rec. UIT-T X.509, *El Directorio: Marcos para certificados de claves públicas y atributos* proporciona una infraestructura de clave pública (PKI, *public key infrastructure*) para autenticación robusta basada en certificados de clave pública y en autoridades de certificación. Una PKI soporta la gestión de claves públicas necesarias para los servicios de autenticación, criptación, integridad y no repudio. Una PKI está compuesta fundamentalmente por la tecnología de criptografía de clave que se describe a continuación. Además de definir un marco de autenticación para la infraestructura PKI, X.509 también propone una infraestructura de gestión de privilegios (PMI, *privilege management infrastructure*) que se utiliza para establecer los derechos y privilegios de los usuarios en el contexto de una autorización robusta basándose en certificados de atributos y autoridades de atributos. En la figura 5-1 se muestran los componentes de la PKI y la PMI.



(a) Componentes de una infraestructura de claves públicas



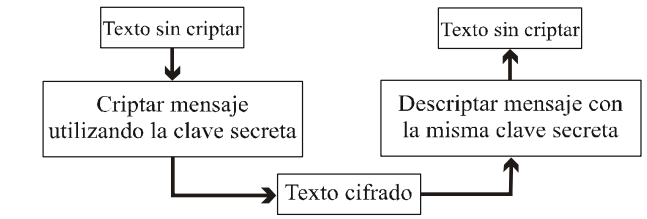
(b) Componentes de una infraestructura de gestión de privilegios

Figura 5-1 – Componentes de una PKI y una PMI

5.1 Criptografía de clave pública y clave secreta

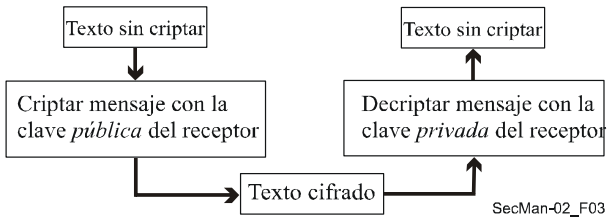
Por criptografía *simétrica* (o *clave secreta*) se entiende un sistema criptográfico en que se utilizan las mismas claves para el cifrado y el descifrado, tal como se muestra en la figura 5-2(a). En estos sistemas es necesario que los participantes compartan una clave secreta única desde un principio, 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 5-2(b), un sistema de criptografía *asimétrica* (o de *clave pública*) involucra un par de claves, a saber una pública y una privada. Si bien las claves públicas pueden comunicarse a todos, las privadas siempre se mantienen secretas. La clave privada suele almacenarse en una tarjeta inteligente o en una llave. La clave pública se genera a partir de la clave privada y, aunque estén matemáticamente relacionadas, no hay manera de invertir el proceso para extraer la clave privada a partir de la clave pública. Para enviar datos confidenciales a una persona de manera segura utilizando la criptación por clave pública, el remitente cripta los datos con la clave pública del receptor. El receptor los descripta con su correspondiente clave privada. La criptación por clave pública también puede utilizarse para asignar una firma digital a los datos para confirmar que un documento o mensaje tiene su origen en la persona que pretende ser el emisor (u originador). La firma digital es en realidad un sumario de los datos, que se produce utilizando la clave privada del signatario y que se anexa al documento o mensaje. El receptor utiliza la clave pública del signatario para confirmar la validez de la firma digital (NOTA – Algunos sistemas de clave pública utilizan dos pares de claves públicas/privadas, una para la criptación/descriptación y otra para la firma digital/ verificación).



– Ambas partes comparten una clave secreta única
– Problema: hay dificultad para el intercambio de claves en secreto total
– Ejemplo más conocido: norma de criptación de datos (DES *data encryption standard*)

(a) Criptación por clave secreta (simétrica)



– *Cada* participante tiene
  - una clave privada que no comparte con nadie más
  - una clave pública que conocen todos
– Problema: es más lenta que la criptación por clave secreta
– Ejemplo más conocido: RSA

(b) Criptación por clave pública (asimétrica)

Figura 5-2 – Ilustración de los procesos de criptación de clave simétrica (privada) y asimétrica (pública) y sus características principales

En el caso de la criptación simétrica, cada par de usuarios debe tener un par distinto de claves que se distribuyen y almacenan de manera segura. En el caso de la criptación asimétrica, las claves de criptación públicas pueden indicarse en un directorio y cualquiera puede utilizar la misma clave de criptación (pública) para enviar datos a un usuario. Esto hace que la criptación asimétrica pueda

adaptarse a otros casos mucho más fácilmente que la criptación simétrica. No obstante, esta criptación asimétrica consume demasiados recursos de computación, por lo que no es eficiente para mensajes completos. Por lo general, la criptación asimétrica se utiliza generalmente para intercambiar claves simétricas que se utilizan a continuación para criptar el cuerpo del mensaje utilizando un algoritmo simétrico más rentable a nivel computacional. De requerirse una firma digital, se aplica al mensaje una función generadora segura unidireccional (SHA1 o MD5) y el número generador de 160 ó 128 bits resultante se cripta asimétricamente mediante la clave privada del remitente y se anexa al mensaje.

Téngase presente que, independientemente del tipo de criptación (simétrica o asimétrica), no es posible encaminar mensajes a sus receptores si todo el mensaje está criptado, puesto que los nodos intermediarios no podrán determinar la dirección del receptor. Por tanto, el encabezamiento del mensaje está normalmente sin criptar.

El funcionamiento seguro de un sistema de clave pública depende en gran medida de la validez de las claves públicas. Éstas generalmente se publican como certificados digitales que se incluyen en un directorio X.500. Un certificado contiene la clave pública de criptación y, según proceda, la clave de verificación de firma para un individuo, y también información adicional que incluye la validez del certificado. Los certificados que se hayan revocado por cualquier motivo suelen incluirse en el directorio en la lista de revocación de certificados (CRL, *certificate revocation list*). Antes de utilizar las claves públicas, se comprueba su validez consultando la CRL.

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, *certification authority*). En la Rec. UIT-T 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 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.

Para poder confirmar la validez de 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. 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 puede suponer la existencia de una cadena de certificación. Este proceso termina normalmente cuando se llega al certificado de la CA que es nuestra "raíz de confianza". Las claves públicas de la 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. La Rec. UIT-T X.509 determina los mecanismos para distribuir una parte de 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. Estos documentos forman parte de una base común que permite evaluar hasta qué punto son fiables los certificados de clave pública emitidos por las CA, internacionalmente y entre los diferentes sectores. Asimismo, estos mecanismos facilitan (en 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 extremos 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

Las versiones anteriores de la Rec. UIT-T X.509 (1988, 1993 y 1997), *El Directorio: Marco de autenticación*, especificaba los elementos básicos necesarios para la infraestructura de clave pública, incluida la definición de los certificados de clave pública. En la Rec. UIT-T X.509 revisada, aprobada en 2000, se amplía significativamente el concepto de certificados de atributo y se proporciona un marco para la infraestructura de gestión de privilegios (PMI). (Una PMI gestiona los privilegios para soportar un servicio de autorización completo relacionado con una PKI.) De esta manera es posible fijar privilegios de acceso a un usuario en un entorno en que haya equipos de múltiples fabricantes y se cuenta con diversas aplicaciones.

Los conceptos de PMI y PKI son similares pero la PMI tiene que ver con la autorización, mientras que la PKI se concentra en la autenticación. En la figura 5-1 y el cuadro 5-1 se muestran las similitudes entre ambas infraestructuras.

Cuadro 5-1 – Características de la infraestructura de gestión de privilegios y la infraestructura de 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 5-3.

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

Figura 5-3 – 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 asertor de privilegios, el verificador de privilegios, el método de objeto[1], la política de privilegios, y las variables ambientales (véase la figura 5-4). Con estas técnicas el verificador de privilegios puede controlar el acceso al método de objeto mediante el asertor de privilegios, de conformidad con la política de privilegios.

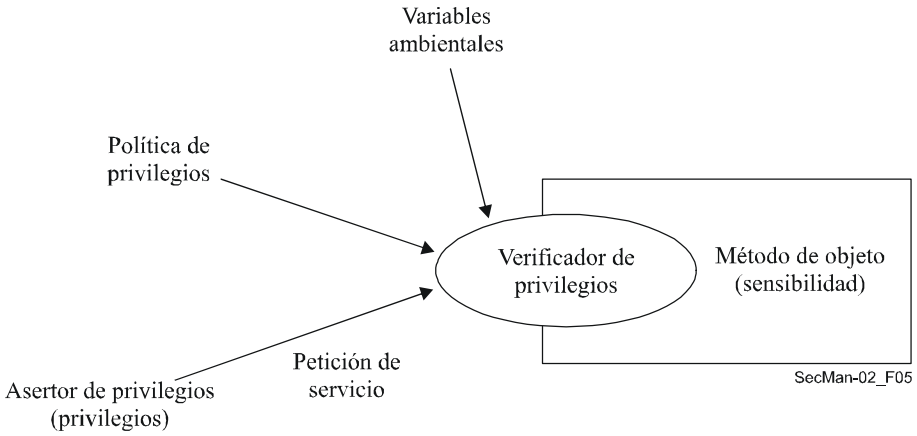


Figura 5-4 – Modelo de control de una PMI de la Rec. UIT-T X.509

Cuando sea necesario delegar un privilegio en una implementación, la Rec. UIT-T X.509 determina cuatro componentes del modelo de delegación para PMI, a saber: el verificador de privilegios, la fuente de autoridad, otras autoridades de atributos y el asertor de privilegios (véase la figura 5-5).

[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).

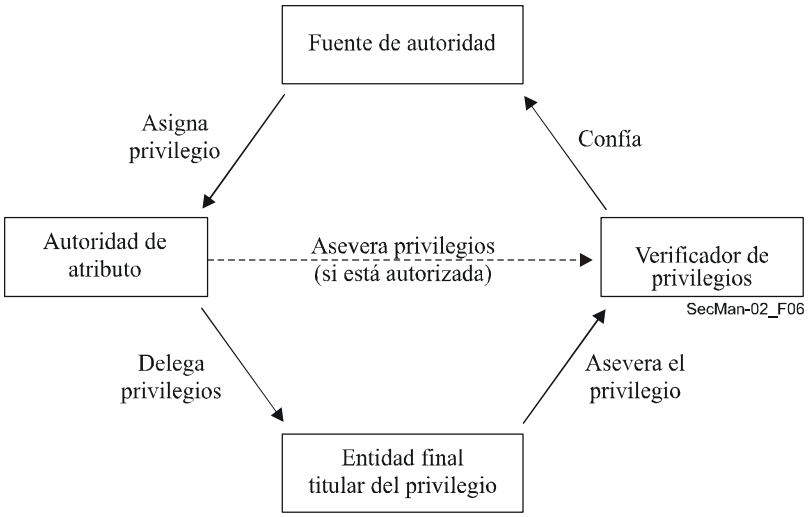


Figura 5-5 – Modelo de delegación de la PMI de la Rec. UIT-T X.509

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 sección 6.5.2 se muestra la utilización de un sistema RBAC: la aplicación de recetas médicas por Internet (*e-prescriptions*).

6 Aplicaciones

En esta sección se tratan aplicaciones de dos clases diferentes. La primera incluye las aplicaciones de usuario extremo, por ejemplo de voz sobre IP (VoIP, *voice-over-IP*), para la que se describen la arquitectura y los componentes de red utilizados. Se discuten aspectos de seguridad y soluciones relacionados con los tres planos que soportan las aplicaciones multimedias, siendo la VoIP un caso particular. Además, se consideran otras aplicaciones de usuario extremo como el sistema IPCablecom, con el que se ofrecen servicios en tiempo real basados en IP por una red de cable, y la transmisión de fax. También se tratan algunas aplicaciones que no son específicas de la industria de las telecomunicaciones, como los servicios de salud por Internet (cibersalud), en particular un sistema de ciberrecetas médicas. 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, pero también otras formas de medios, incluidos el vídeo y los datos, como son la compartición de aplicaciones y la funcionalidad de pizarra electrónica. El sistema VoIP también incluye los servicios suplementarios correspondientes, tales como la conferencia (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 los sistemas VoIP, en el que el tráfico vocal se hace pasar a través de la red troncal pública de Internet.

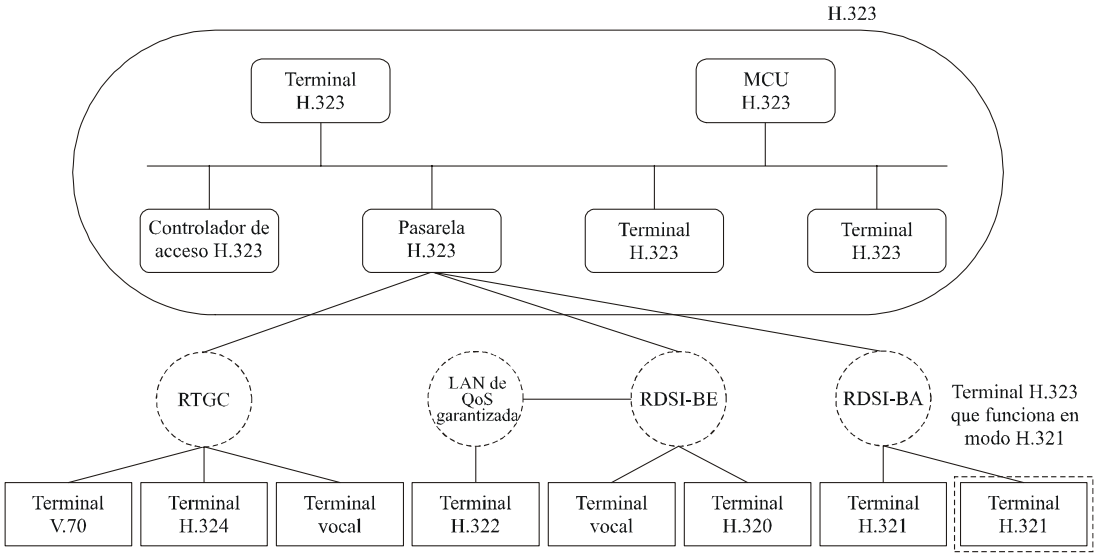
La Recomendación UIT-T H.323 es una Recomendación general que proporciona los fundamentos de las comunicaciones de audio, vídeo y datos por redes con conmutación de paquetes, incluida Internet, redes de área local (LAN, *local-area networks*) y redes de área extensa (WAN, *wide-area networks*) que no proporcionan una calidad de servicio (QoS, *quality of service*) 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 H.323, los productos y aplicaciones multimedias 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 VoIP para aplicaciones del mercado de consumo, de empresas, de proveedores de servicios, de ocio y 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 multimedias 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 multimedias (común para H.310, H.323 y H.324).
- H.235.x – Seguridad en los sistemas basados en H.323.
- 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 multimedias.
- H.510 – Movilidad de usuario, de terminal y de servicio.
- H.530 – Especificación de seguridad para H.510.

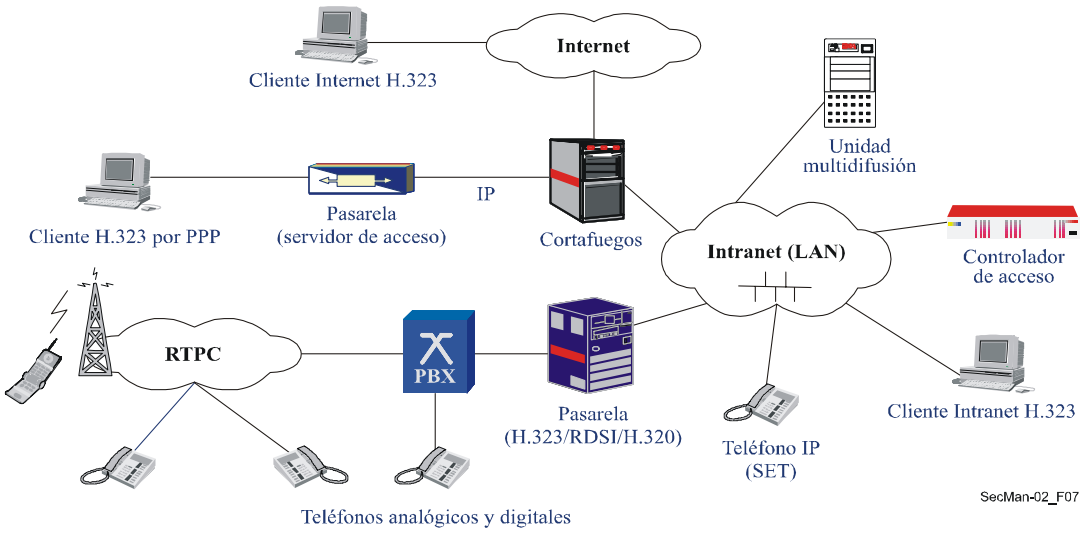
En 1996 el UIT-T aprobó la primera versión de la Recomendación H.323, mientras que la segunda fue aprobada en enero de 1998 y la actual versión 6 en 2006. Dicha norma es bastante amplia en cuanto a su alcance e incluye tanto dispositivos autónomos como tecnologías integradas en las computadoras personales, así como las conferencias punto a punto y multipunto. En dicha Recomendación se especifican el control de llamadas, la gestión de multimedias y la gestión de ancho de banda, así como las interfaces entre redes diferentes.

La Recomendación H.323 forma parte de una serie más general de normas de comunicaciones que permiten las videoconferencias con redes diferentes. Esta serie H.32x incluye las Recomendaciones H.320 y H.324, sobre las comunicaciones RDSI y RTPC, respectivamente. Este manual básico contiene una presentación general de la norma H.323, sus ventajas, la arquitectura y las aplicaciones.

En la Recomendación H.323 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 6-1 se pueden ver todos estos elementos.



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



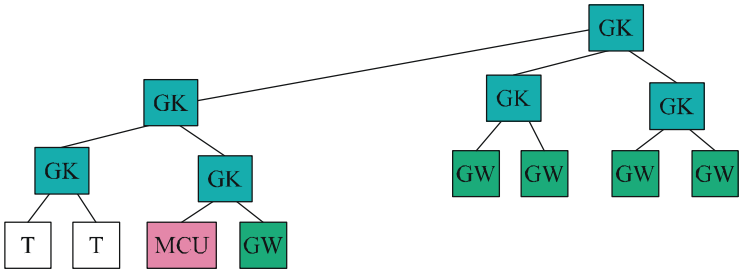
(b) Casos de implementación H.323 [Euchner]

Figura 6-1 – Sistema H.323: componentes y casos de implementación

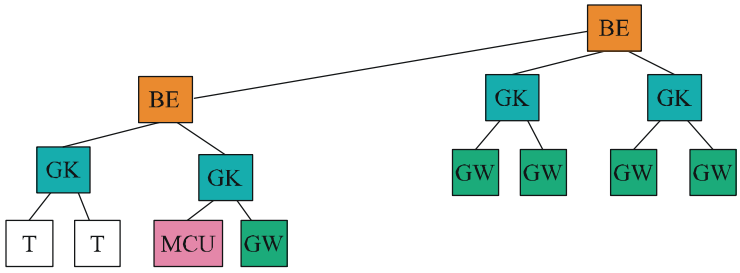
Los *terminales (T)* son los puntos extremos del cliente en la red troncal IP que proporcionan comunicaciones bidireccionales. Los terminales H.323 deben soportar comunicaciones vocales y pueden soportar códecs de vídeo, protocolos de conferencia de datos T.120, y capacidades MCU. Algunos ejemplos son: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

La *pasarela (GW)* proporciona muchos servicios, en particular la función de traducción entre los puntos extremos 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, establece y libera la llamada tanto en el lado con conmutación de paquetes como en el de la red con conmutación de circuitos.

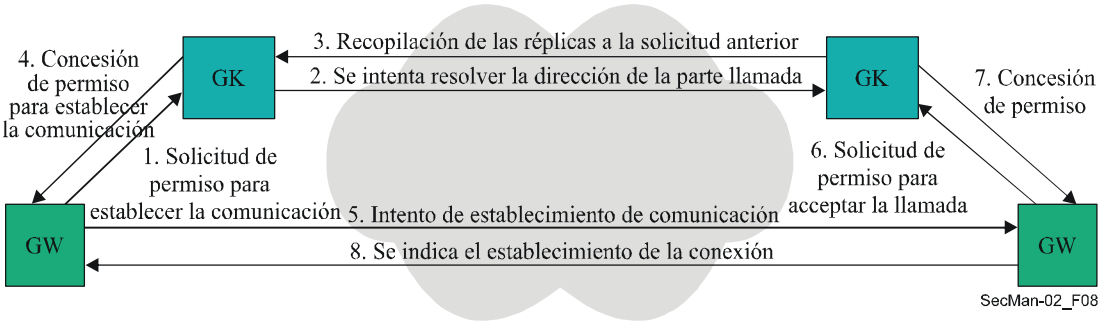
El *controlador de acceso (GK)* es una parte importante de toda red en la que se utiliza la H.323. Actúa como punto central para todas las llamadas dentro de su zona y suministra los servicios de control de llamada a todos los puntos extremos registrados. Cabe decir que un controlador de acceso H.323 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/encuéntrame (*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 (o dentro de los mismos). 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 6-2.



(a) Topología con RAS



(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
RAS: protocolo de registro, admisión y estado

Figura 6-2 – Comunicación entre dominios administrativos

Una *unidad de control multipunto (MCU)* soporta conferencias entre tres o más puntos extremos. Conforme a 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.

Las redes H.323 que funcionan actualmente transportan miles de millones de minutos de tráfico de voz y vídeo cada mes. 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 y el tráfico de vídeo H.323 sigue aumentando. 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. Los productos H.323 van desde las pilas de protocolos y los circuitos integrados hasta los teléfonos inalámbricos y los dispositivos necesarios para la conferencia de vídeo.

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 Internet;
- soporte de fax, texto por IP y módem por IP, conforme a T.38;
- muchos servicios suplementarios (reenvío de llamada, extracción de llamada, etc.);
- interoperabilidad robusta con otros sistemas de la serie H.32x, incluidos los de H.320 (RDSI) y H.323M (servicios móviles inalámbricos 3GPP);
- especificación de la subdivisión de la pasarela de medios (mediante el protocolo de control de pasarelas H.248);
- soporte de seguridad de señalización y medios;
- movilidad de usuario, terminal y terminal de servicio; y
- soporte de la señalización de los servicios de urgencia.

H.323 es utilizada, por ejemplo, por los operadores para el tráfico al por mayor, en especial por las rutas troncales de VoIP (similar a los conmutadores de clase 4 para el tráfico vocal), y los servicios de llamada con tarjetas. En las empresas, H.323 se utiliza, por ejemplo, para centralitas (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. Entre los particulares se utiliza para el acceso audiovisual de banda ancha, PC a teléfono, teléfono a PC, llamada PC a PC, y también puede utilizarse para la prestación de servicios de noticias e información adaptados a cada persona.

6.1.1 Aspectos de seguridad de los sistemas multimedias 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 6-3.

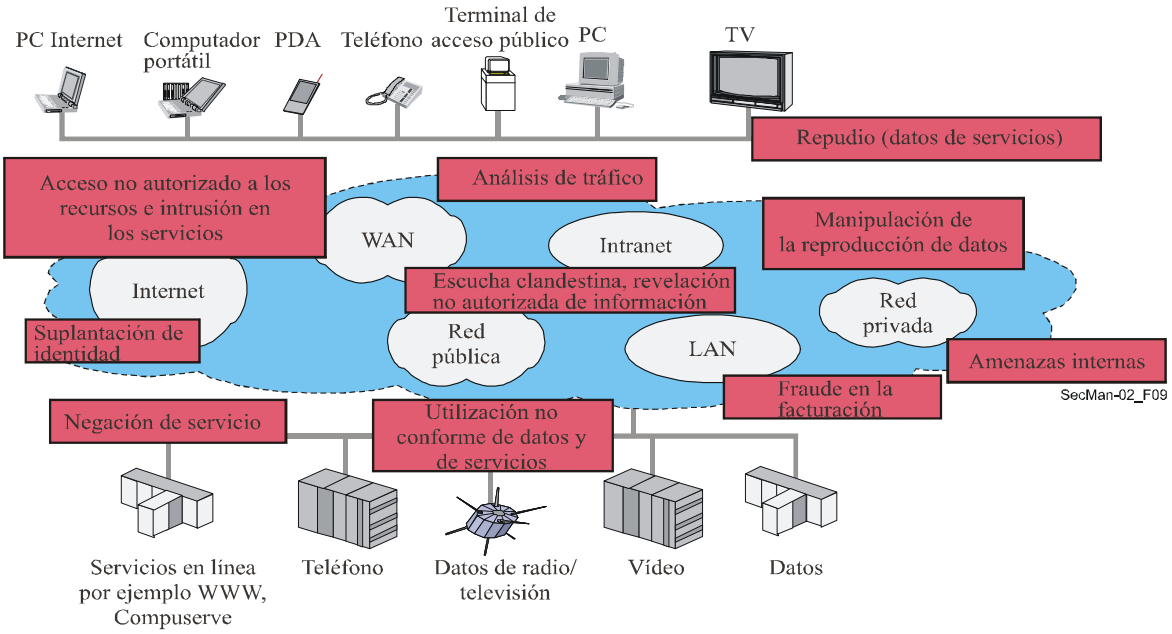


Figura 6-3 – Amenazas contra la seguridad en las comunicaciones multimedias

Los aspectos de seguridad más importantes en las comunicaciones multimedias y en la telefonía IP en general son los siguientes [Euchner]:

- 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 la criptación 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 comunicación 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 criptan los paquetes de medios (por ejemplo vídeo) de las aplicaciones multimedias. 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.
- 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, *network address translation*) 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 Recomendaciones de la subserie H.235.x

En un sistema multimedias H.323, la Rec. UIT-T H.235.0 define el marco de seguridad, incluida la especificación de los mecanismos y protocolos de seguridad para H.323. H.235 fue redactada en 1998 para los sistemas de la versión 2 de H.323. Desde entonces ha evolucionado, consolidando los mecanismos de seguridad ofrecidos, adicionando algoritmos de seguridad más sofisticados (por ejemplo, criptación AES de alta seguridad y alta velocidad) y desarrollando perfiles de seguridad más útiles y eficaces para determinados entornos y casos. La versión 4 de H.235.0-H.235.9 son actualmente las series de Recomendaciones de seguridad del UIT-T para los sistemas basados en H.323, una seguridad escalable que va desde pequeños grupos hasta empresas enteras y operadores de gran tamaño.

La antigua versión 3 de la Rec. UIT-T H.235 ha sufrido una importante reestructuración de todas sus partes y anexos y se ha transformado en la subserie de Recomendaciones autónomas H.235.x. La Rec. UIT-T H.235.0 especifica un "Marco de seguridad para sistemas multimedias de la serie H (H.323 y otros basados en H.245)". Esta Recomendación resume toda la subserie H.235.x y expone los procedimientos comunes en un texto básico.

En resumen, las Recomendaciones de la serie H.235.x especifican la protección criptográfica de los protocolos de control (RAS y señalización de llamada H.225.0 y H.245), así como de los datos de trenes de medios de audio/vídeo. La Recomendación UIT-T H.235 especifica los mecanismos de negociación de los servicios criptográficos deseados y requeridos, los algoritmos de criptografía y las capacidades de seguridad través de las diversas etapas de la señalización H.323. 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 (es decir, MCU), siempre que se comuniquen varias terminales multimedias dentro de un grupo.

H.235 utiliza técnicas especiales de seguridad optimizada como la criptografía de curva elíptica y la criptación más moderna 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 la criptación 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 6-4 se muestra el alcance de H.235, que comprende disposiciones para el establecimiento de comunicaciones (bloques H.225.0 y H.245) y la comunicación bidireccional (criptación 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 H.323 y H.235, suele implementarse utilizando los protocolos de seguridad IP (IPSec, *IP security*) y de seguridad de capa de transporte (TLS, *transport layer security*) del IETF. En general, estos dos protocolos se pueden utilizar con fines de autenticación y, facultativamente, confidencialidad (es decir criptación) 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.

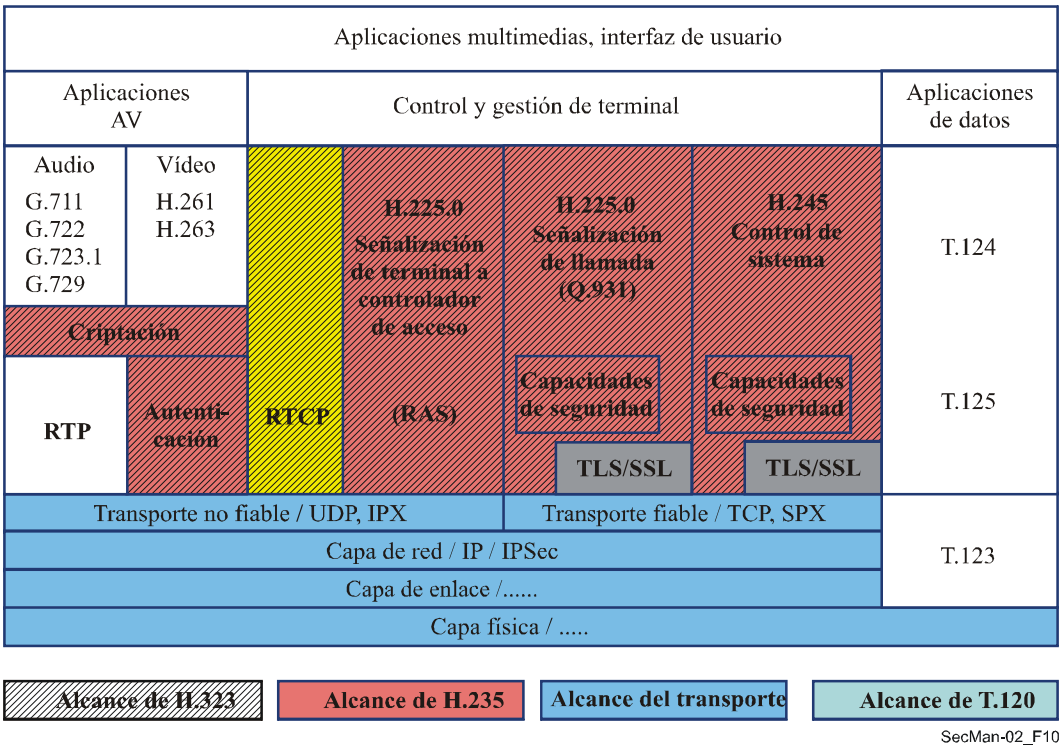


Figura 6-4 – Seguridad en los sistemas H.323 proporcionada por H.235 [Euchner]

La serie de Recomendaciones UIT-T H.235.x cubre una amplia gama de medidas de seguridad para distintos entornos: de una empresa, entre empresas y de operadores. Dependiendo de las hipótesis (infraestructura de seguridad disponible y capacidades del terminal) y de las plataformas (puntos extremos simples o inteligentes), H.235.x ofrece una variedad de perfiles de seguridad compatibles adaptados a cada caso. Estos perfiles ofrecen distintos técnicas de seguridad, desde perfiles simples de secreto compartido, algunos con contraseña protegida (H.235.1 para la autenticación e integridad del mensaje de señalización H.225.0) hasta los más sofisticados que contienen firmas digitales y certificados PKI X.509 (H.235.2). De esta manera se puede ofrecer protección salto por salto utilizando técnicas más simples, pero menos escalables, o bien extremo a extremo utilizando técnicas PKI escalables. H.235.3 se denomina perfil de seguridad híbrido ya que esta Recomendación combina procedimientos de seguridad simétricos de H.235.1 y certificados PKI y firmas H.235.2, optimizando así la calidad de funcionamiento y reduciendo el tiempo de establecimiento de comunicación. H.235.3 ofrece además la posibilidad de implementar operaciones de gran carga computacional en una entidad con procesador de seguridad funcional por intermediario (es facultativo).

Los mecanismos de H.235.4 para "Seguridad de llamada con encaminamiento directo y selectivo" consisten en disminuir la dependencia estricta de una arquitectura de encaminamiento por controlador de acceso y centrada en el servidor, y proporciona medidas de seguridad para el modelo de comunicación entre entidades pares. Esta Recomendación define procedimientos para la gestión de claves en entornos empresariales y entre dominios. En concreto, H.235.4 cubre todos los casos en que un controlador de acceso funciona con encaminamiento directo, y los casos en que el controlador de acceso puede llevar a cabo de manera selectiva parte del encaminamiento del tráfico de señalización de llamada H.225.0.

Si bien muchos perfiles de seguridad H.235 están basados en una hipótesis de modelo con encaminamiento por controlador de acceso H.323, H.235.4 trata más concretamente de la comunicación segura entre pares con el objetivo de eliminar las acciones de encaminamiento de señalización H.323 que tendrían que realizar los controladores de acceso y de mejorar las condiciones generales de escalabilidad y calidad de funcionamiento. En H.235.4, gracias al soporte de las llamadas con encaminamiento directo, los controladores de acceso operan principalmente a nivel local dentro de su dominio para realizar la autenticación de usuarios/terminales y el registro, la admisión, la resolución de dirección y el control de anchura de banda. Por otra parte, los terminales realizan el establecimiento de comunicación H.323 directamente entre puntos extremos, de extremo a extremo, como se muestra en la figura 6-5.

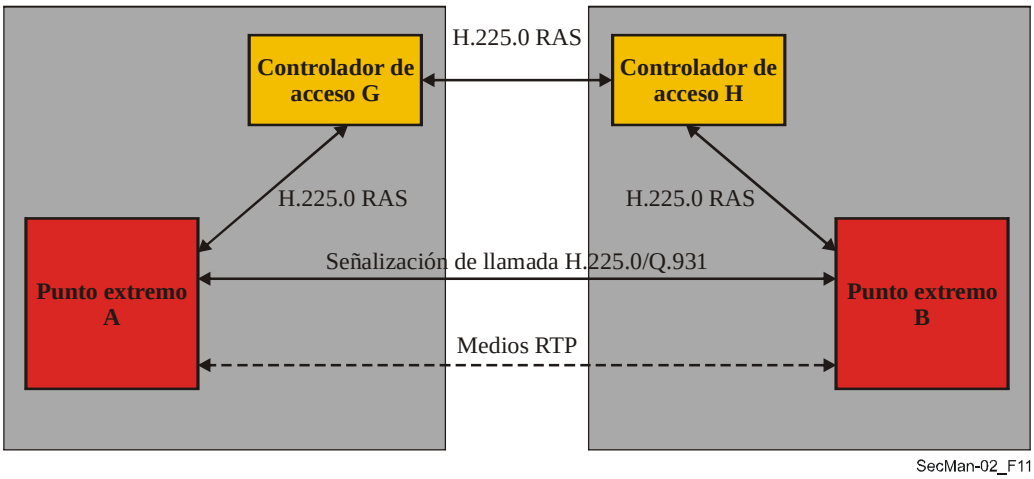


Figura 6-5 – Encaminamiento directo H.235.4

Cuando el punto extremo (EP) A pide al controlador de acceso GK (G) la admisión de llamada para transmitir una llamada al punto extremo B, un controlador de acceso (G en el entorno de una empresa o H en entornos interdominios) genera una clave de señalización de llamada de extremo a extremo para ambos puntos extremos A y B. De manera muy similar a Kerberos (véase la aplicación en la Rec. UIT-T J.191), el punto extremo A obtiene de manera segura la clave generada y una llave de seguridad, y también otra llave de seguridad con la misma clave para el punto extremo B. Al realizar la llamada, el punto extremo A aplica directamente la clave para proteger la señalización de llamada hacia el punto extremo B, pero también retransmite la otra llave de seguridad con la clave hacia el punto extremo B. Los sistemas H.235.4 pueden utilizar los perfiles de seguridad H.235.1 o H.235.3.

Otros procedimientos anexos para el funcionamiento interdominios que se contempla en H.235.4 permiten distinguir los casos en que los puntos extremos o los controladores de acceso no soportan la capacidad de acuerdo de clave Diffie-Hellman. Aún así, al cabo los puntos extremos A y B obtienen una sesión secreta compartida que protege de extremo a extremo la señalización H.323 en términos de autenticación, integridad o confidencialidad.

Para proporcionar mayor seguridad a los sistemas que utilizan números de identificación personal (PIN, *personal identification numbers*) o contraseñas para autenticar a los usuarios, H.235.5 proporciona otro "*Marco para la autenticación segura en RAS utilizando secretos compartidos débiles*", con métodos de clave pública para proteger el uso de PIN/contraseñas. Se define en la

actualidad un perfil específico que explota el método de intercambio de claves criptadas para negociar un secreto compartido fuerte, protegido contra ataques pasivos o activos (de intruso – *man-in-the-middle*). Este marco permite la definición de nuevos perfiles utilizando otros métodos de negociación basados en claves públicas.

La Rec. UIT-T H.235.6, "*Perfil de criptación vocal con gestión de claves H.235/H.245 nativas"* recoge todos los procedimientos necesarios para criptar un tren de medios RTP, incluida la gestión de claves circundante que se expresa enteramente en los campos de señalización H.245.

Para lograr una mayor convergencia entre SIP y SRTP, la Rec. H.235.7, "*Utilización del protocolo de gestión de claves MIKEY para el protocolo de transporte en tiempo real seguro en H.235"*, utiliza el protocolo en tiempo real seguro (RSTP, RFC 3711) en H.235. Esta Recomendación especifica cómo utilizar la gestión de claves MIKEY de IETF en H.235.7 para una distribución de claves de medios SRTP de extremo a extremo.

La Rec. UIT-T H.235.8 "*Intercambio de claves para el protocolo de transporte en tiempo real seguro utilizando canales de señalización seguros"* especifica un método complementario para transmitir los parámetros de claves SRTP extremo a extremo, suponiendo que se utiliza un tipo de transporte seguro. Este enfoque es similar al adoptado por las descripciones de SDP en IETF. Estos canales seguros para el transporte de señalización pueden lograrse gracias a IPSec (protocolo de seguridad Internet), TLS (protocolo de seguridad de capa de transporte), o CMS (sintaxis de mensaje criptográfico).

Permitir que la señalización H.323 pase a través de los puntos NAT (traducción de dirección de red) y los cortafuegos (FW, *firewalls*) ha sido uno de los mayores obstáculos en la práctica. En la Rec. UIT-T H.235.9, "*Soporte de pasarela de seguridad para H.323"*, se recogen los procedimientos de seguridad que permiten a un punto extremo/terminal H.323 descubrir las pasarelas de seguridad H.323, entendiéndose que estas entidades incluyen las funciones de una pasarela de capa de aplicación (ALG, *application layer gateway*) NAT/FW H.323. Esta supuesta pasarela de señalización fiable detecta las transacciones de señalización en curso y participa en la gestión de claves en la señalización H.225.0.

Si bien en H.235.0 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.

En la figura 6-6 se muestra el caso básico de H.530 donde un terminal móvil (MT) H.323 puede entrar directamente al dominio propio mediante el controlador de acceso propio (H-GK, *home gatekeeper*) o conectarse a un controlador de acceso foráneo (V-GK, *foreign gatekeeper*) en un dominio visitado. Dado que el terminal móvil y el usuario son desconocidos para el dominio visitado, antes que nada el controlador de acceso visitado tiene que solicitar la función de autenticación (AuF, *authentication function*) al dominio propio del MT, donde está abonado y es conocido. Así, el dominio visitado delega la tarea de la autenticación a la AuF del dominio propio y deja que ésta autentifique el terminal y decida de la autorización. Además, la AuF garantiza al controlador V-GK una vinculación criptográfica del MT y una clave dinámica V-GK utilizando un protocolo de seguridad criptográfico de H.530. La AuF comunica de manera segura su decisión al controlador de acceso visitado durante la fase de registro del terminal.

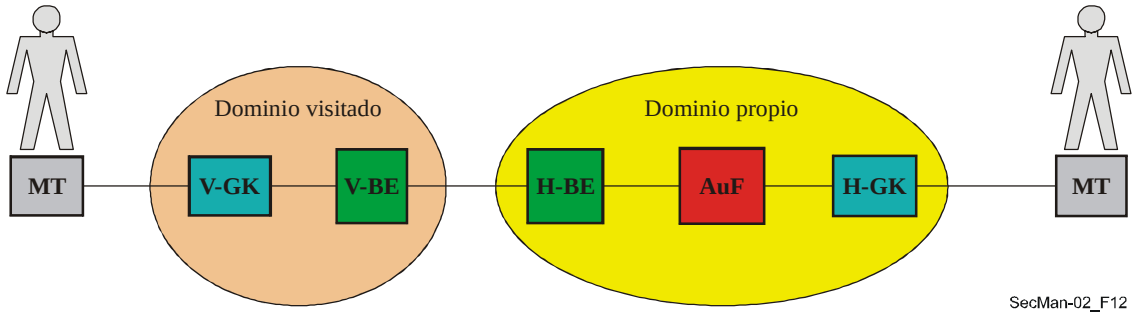


Figura 6-6 – Hipótesis H.530

La comunicación entre los dominios visitado y propio utiliza el protocolo genérico H.501 para la gestión de movilidad H.323 y la comunicación intradominio e interdominios. Una vez recibida la autenticación y la decisión de autorización de la AuF, el controlador de acceso visitado y el MT acuerdan una clave de vinculación dinámica nueva que ambos comparten durante la asociación de seguridad. Esta clave de enlace es utilizada para la protección de cualquier otra comunicación de señalización H.323 entre el MT y el V-GK. La comunicación de señalización multimedias ocurre a nivel local en el dominio visitado y no requiere la interacción con el dominio propio.

H.530 adopta una arquitectura de seguridad muy simple en la que el MT sólo comparte un secreto compartido preconfigurado (por ejemplo, una contraseña de abono) con su AuF en el dominio propio, sin que el HT tenga que compartir asociaciones de seguridad *a priori* con los dominios visitados. La protección de seguridad entre entidades dentro de un dominio y entre dominios requiere únicamente secretos compartidos simétricos: pueden establecerse, por ejemplo, mediante acuerdos de nivel de servicio entre dominios. H.530 reutiliza los perfiles de seguridad H.235 existentes, como H.235.1, para la seguridad de los mensajes de señalización H.501/H.530 entre dominios.

Además de H.235.0, los mecanismos de H.350 y H.350.2 también permiten una gestión de claves escalable gracias al protocolo de acceso al directorio ligero (LDAP, *lightweight directory access protocol*) y el protocolo de capa segura entre puntos extremos *Secure Sockets Layer* (SSL/TLS). En la serie de Recs. 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 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 multimedias. Más aún, gracias a esta arquitectura se cuenta con un lugar normalizado para almacenar las credenciales de seguridad de estos protocolos.

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). Obsérvese que tanto H.323 como SIP soportan la autenticación de secreto compartido (H.235.1 y HTTP Digest, respectivamente). Con estos métodos es necesario que el servidor de llamada tenga acceso a las contraseñas. Por tanto, de haber una amenaza para el servidor de llamada o el directorio H.350, también la hay para las contraseñas. Probablemente esta debilidad se debe más a una debilidad en los sistemas y su funcionamiento (directorio H.350 o servidores de llamada), y no 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.

6.1.3 Dispositivos H.323 y NAT/FW

Internet fue creado como un sistema "extremo a extremo", es decir, que cualquier dispositivo de la red puede comunicar directamente con otro dispositivo de la red. No obstante, por problemas de seguridad y carencia de direcciones de red IPv4, a menudo se emplean en las fronteras de las redes dispositivos cortafuegos y de traducción de dirección de red (NAT). Se encuentran en las fronteras del dominio de particular, el dominio de proveedor de servicio, el dominio de empresa y algunas veces el dominio de país. En un dominio puede haber más de un dispositivo cortafuegos o NAT.

Los dispositivos cortafuegos están diseñados para controlar estrictamente el movimiento de la información a través de las fronteras de la red y suelen estar configurados para bloquear la mayor parte de las comunicaciones IP. A menos que el cortafuegos esté explícitamente configurado para permitir el tráfico H.323 procedente de dispositivos externos hacia los dispositivos H.323 internos, la comunicación simplemente no es posible, lo que supone un problema para cualquier usuario de equipos H.323.

Los dispositivos NAT traducen las direcciones utilizadas dentro del dominio interno en direcciones utilizadas en el dominio externo y viceversa. Las direcciones utilizadas dentro de un dominio de particular o de empresa son generalmente, aunque no siempre, asignadas a partir de espacios de direcciones de red privadas, definidos en RFC 1597, es decir:

Clase	Gama de direcciones	Número de direcciones IP
A	10.0.0.0 – 10.255.255.255	16,777,215
B	172.16.0.0 – 172.31.255.255	1,048,575
C	192.168.0.0 – 192.168.255.255	65,535

Los dispositivos NAT plantean un problema aún mayor a la mayoría de los protocolos IP, especialmente aquellos que transportan direcciones IP dentro del protocolo. Los protocolos H.323, SIP y otros protocolos de comunicación en tiempo real que funcionan en redes con conmutación de paquetes deben proporcionar la dirección IP y la información de puerto para que las otras partes en la comunicación sepan dónde enviar los trenes de medios (por ejemplo, trenes de audio y vídeo).

El UIT-T ha estudiado los problemas del paso de dispositivos NAT/FW y ha creado una serie de tres Recomendaciones con soluciones para permitir el paso de sistemas H.323 por uno o más dispositivos NAT/FW. Estas Recomendaciones son: H.460.17 ("*Utilización de la conexión de señalización de llamadas H.225.0 como transporte de mensajes RAS H.323*"), H.460.18 ("*Paso de señalización H.323 a través de traductores de dirección de red y cortafuegos*") y H.460.19 ("*Paso de medios H.323 por traductores de dirección de red y cortafuegos*").

Todas estas Recomendaciones utilizan el marco de extensibilidad genérico que se presenta en la versión 4 de H.323, lo que significa que cualquier dispositivo conforme a la versión 4 de H.323 o versiones superiores puede adaptarse para soportar estos procedimientos de paso de dispositivos NAT/FW. Además, H.460.18 contiene disposiciones para permitir a dispositivos más antiguos, que no se ajustan a estas Recomendaciones, el paso a través de fronteras NAT/FW con la asistencia de un dispositivo "intermediario".

En la figura 6-7 se muestra cómo puede utilizarse el dispositivo "intermediario" especial para ayudar a los dispositivos "que desconocen" NAT/FW a pasar adecuadamente la frontera NAT/FW:

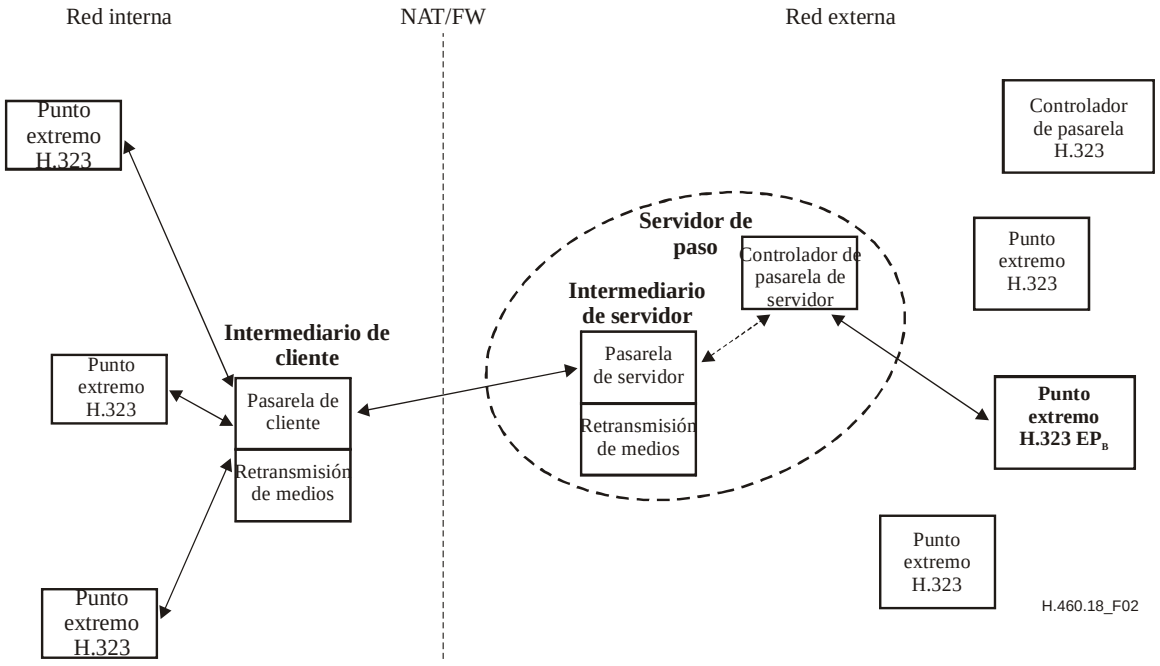


Figura 6-7 – Arquitectura H.460.18 plenamente fraccionada

Esta topología también puede resultar útil en otros casos, por ejemplo cuando una empresa desea la vía de la señalización de llamada H.323 y de los flujos de medios en la red. No obstante, H.460.17 y H.460.18 (que tratan de los aspectos de señalización del paso por NAT/FW) permiten a los puntos extremos atravesar las fronteras NAT/FW sin ayuda de ningún dispositivo "intermediario" interno especial. Este tipo de topología se muestra en la figura 6-8:

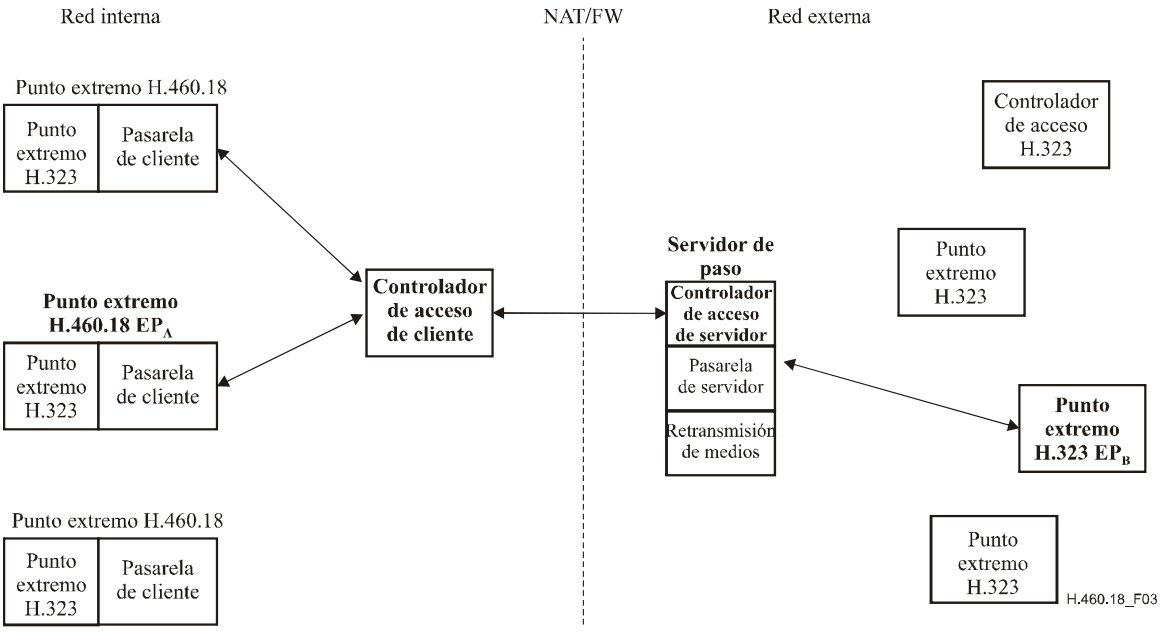


Figura 6-8 – Arquitectura de comunicación de controlador de acceso

En esta topología H.460.18, los puntos extremos de la red interna comunican con el controlador de acceso, que también reside en la red interna, para resolver la dirección de las entidades externas (por ejemplo, un número de teléfono o un URL H.323 para una dirección IP). El controlador de acceso de la red interna comunica con un controlador de acceso en la red externa para intercambiar esa información de dirección y la devuelve al punto extremo llamante. Cuando un dispositivo de la red interna llame a un dispositivo de la red externa, utilizará los procedimientos definidos en H.460.18 para abrir los "huecos" necesarios a través de los dispositivo NAT/FW para pasar la señalización de la red interna hacia la red externa. Además, utilizará los procedimientos definidos en H.460.19 para abrir los "huecos" necesarios para permitir el paso de trenes de medios de la red interna a la red externa y viceversa.

Cuando los dispositivos llamado y llamante residen en redes privadas distintas separadas por dispositivos NAT/FW y el Internet público, será necesario al menos un dispositivo "pasarela de servidor" y un dispositivo "retransmisión de medios" (definidos en H.460.18) para encaminar adecuadamente la señalización y los medios entre las dos redes privadas. Esta combinación de dispositivos suele denominarse "controlador de frontera de sesión". Se hace así simplemente porque el diseño no permite que un paquete IP de una red privada pase a otra red privada sin la ayuda de alguna entidad de la red pública que hace de "intermediario" del paquete.

Por supuesto, las llamadas con origen y terminación dentro de la misma red privada funcionan normalmente sin procedimientos de tratamiento de llamada especiales. H.460.17, H.460.18 y H.460.19 no impiden el funcionamiento de los dispositivos H.323 dentro de la misma red interna.

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, *access node*) permite la conectividad entre la primera y la segunda de dichas redes. Tanto la pasarela de señalización (SG, *signalling gateway*) como la de medios (MG, *media gateway*) hacen posible la conectividad entre "la red IP gestionada" y la RTPC. En la figura 6-9 se muestra la arquitectura de referencia de IPCablecom.

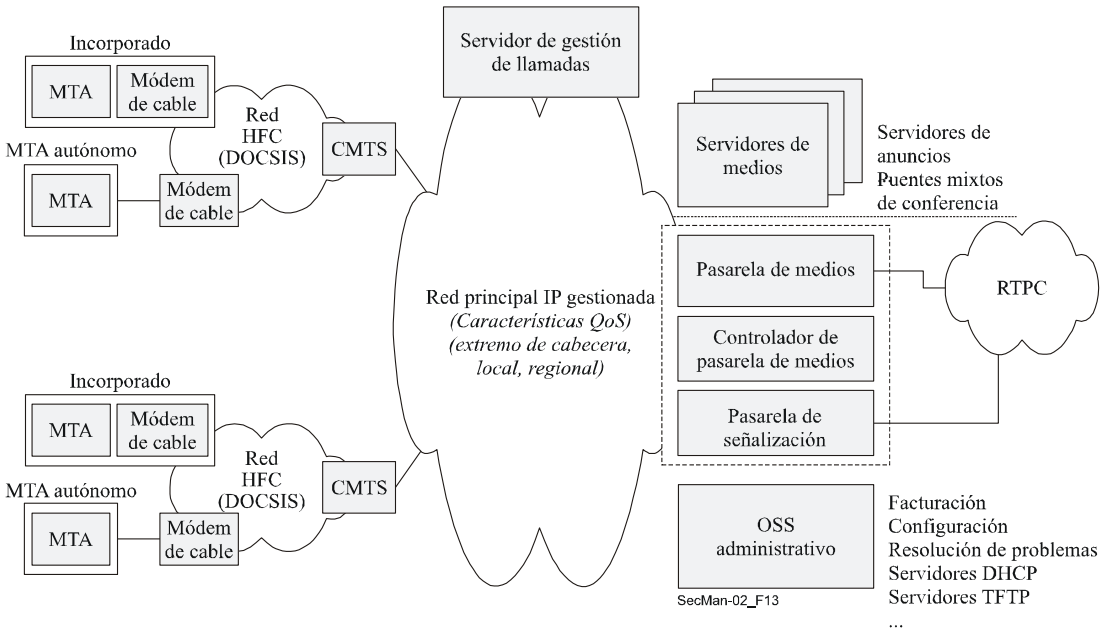


Figura 6-9 – Arquitectura de referencia IPCablecom [J.165]

En la red de acceso que utiliza el sistema híbrido de fibra óptica/cable coaxial (HFC, *hybrid fibre-coaxial cable*) 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, *cable modem termination system*).

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, *operational support system*).

El *servidor de gestión de llamadas* (CMS, *call management server*) 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, *media gateway controller*) 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, *media gateway*) 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 2-1. 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 6-10 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.

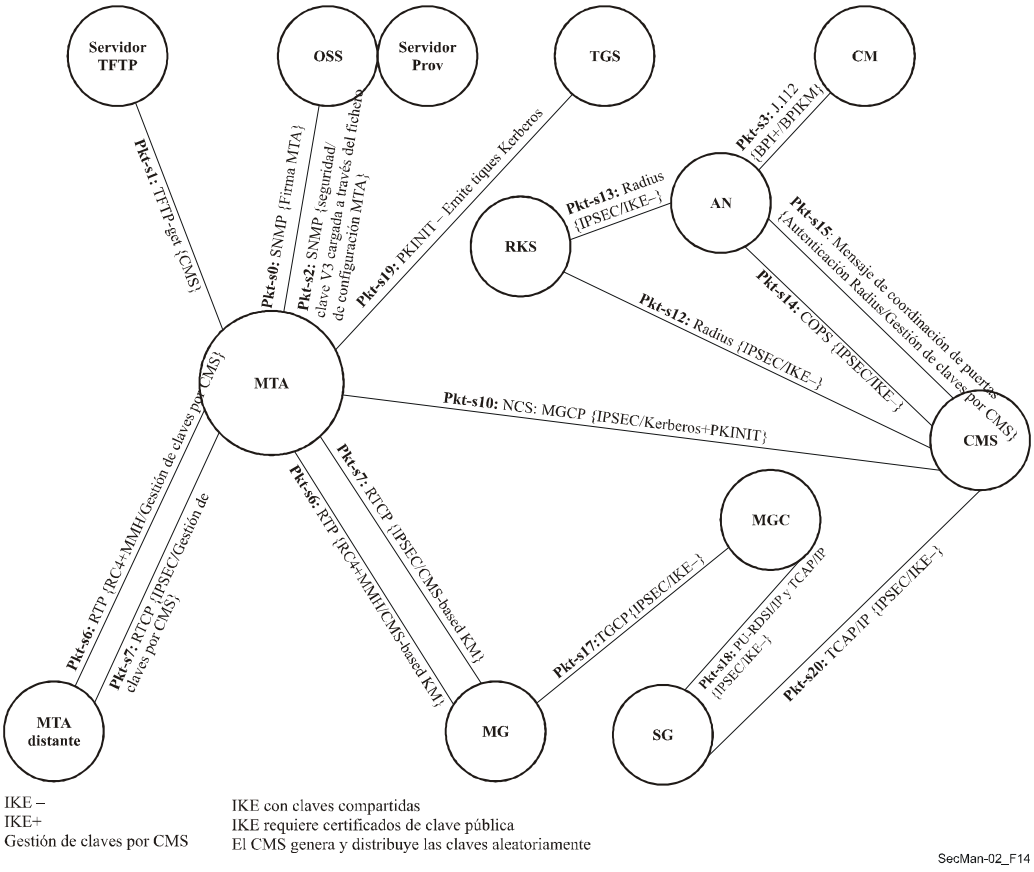


Figura 6-10 – Interfaces de seguridad IPCablecom (el nombre está formado por los siguientes elementos <etiqueta>: <protocolo> { <protocolo de seguridad> / <protocolo de gestión de claves> })

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, *message authentication code*). 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, *record keeping server*) 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 de facsímil

El facsímil es una aplicación muy extendida 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 Rec. UIT-T 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 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/T.36 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 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 (criptación), 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 (criptación), 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 6-1 a continuación.

Cuadro 6-1 – 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, *Hawthorne key management*) y *cifrado de facsímil Hawthorne* (HFX, *Hawthorne facsimile cipher*) 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 Rec. UIT-T T.36 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.

Para proteger la transmisión de un documento, el 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 descriptarlo.

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 Recs. 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 cripta 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/T.30.

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/T.30 se describen los medios para transmitir el certificado de clave pública del remitente, el formato preciso de éste queda en estudio 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 las normas ISO/CEI de la serie 18033.

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

Basándose en la arquitectura de seguridad de la sección 2.4, es imperativo proteger el tráfico en el plano de gestión, que se utiliza para supervisar y controlar la red de telecomunicaciones. Dicho tráfico se suele catalogar en diferentes categorías conforme a la información necesaria para ejecutar las funciones de gestión de fallos, configuración, calidad de funcionamiento, contabilidad y seguridad. La gestión de seguridad supone 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 sección se describe el segundo aspecto.

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 (RGT), que se describe en la Rec. UIT-T M.3010. La RGT 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 la 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, *network elements*) y sistemas de gestión (MS, *management systems*) 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 la gestión de una red de telecomunicaciones se define en la Rec. UIT-T M.3010, mientras que la arquitectura física se muestra en la figura 6-11. La red de gestión define interfaces que establecen los intercambios necesarios para realizar las funciones OAM&P en distintos niveles.

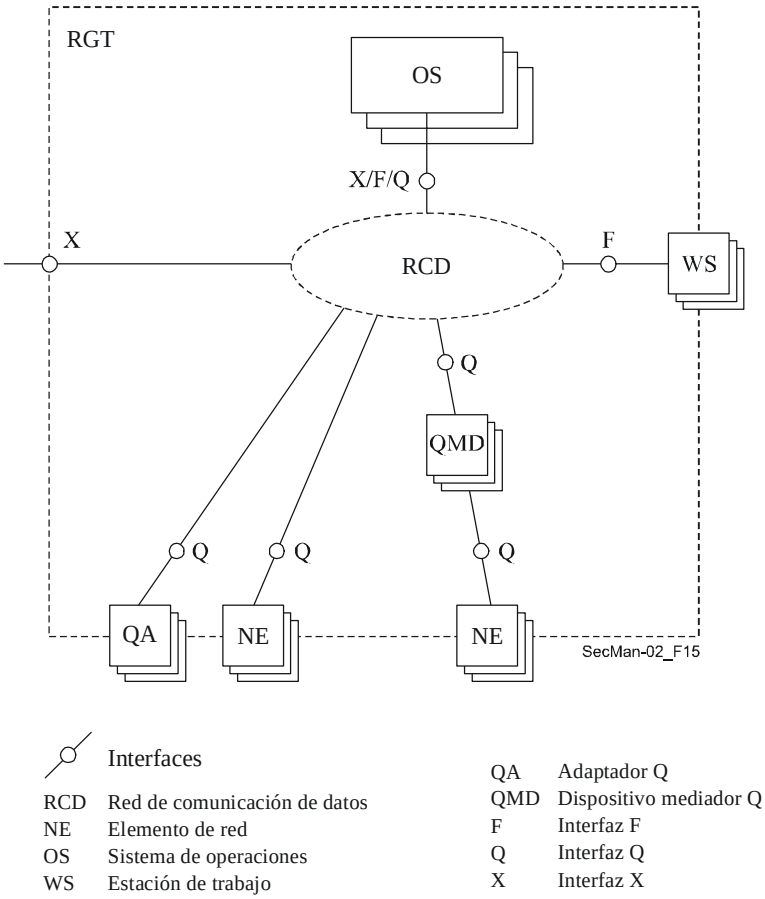


Figura 6-11 – Ejemplo de arquitectura física conforme a M.3010

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 se sitúa entre dominios diferentes que pueden pertenecer a diversos proveedores. Si bien en ambos casos hay que tomar medidas de seguridad, es necesario aplicar medidas más robustas a la interfaz X para contrarrestar las amenazas. En la Rec. UIT-T M.3016.0 se presenta un panorama general y un marco que identifica las amenazas de seguridad para la RGT. Dentro de la serie de Recomendaciones UIT-T M.3016, la Rec. M.3016.1 define los requisitos en detalle, la Rec. M.3016.2 los servicios de seguridad y la Rec. M.3016.3 los mecanismos que pueden contrarrestar las amenazas dentro del contexto de la arquitectura funcional de la RGT, como se indica en la Rec. UIT-T M.3010. Como no es necesario que las diversas organizaciones normalizadoras admitan todos los requisitos, la Rec. M.3016.4 proporciona un modelo para crear perfiles basados en los requisitos, servicios y mecanismos de seguridad que pueden utilizarse para adaptarse a la política de seguridad de cada organización. En la Rec. UIT-T M.3320 se dan detalles específicos de la interfaz X. En las Recs. 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 sección anterior es un ejemplo de esta última faceta. En la Rec. UIT-T M.3400 se definen varias funciones relacionadas con ambas facetas.

Con el marco de X.805, varias Recomendaciones especifican las funciones de gestión para las tres componentes del plano de gestión (véase la figura 2-1). En las siguientes subsecciones se describen algunas de estas Recomendaciones y se muestran las soluciones de seguridad. Además de las Recomendaciones para las tres capas del plano de gestión, hay otras que definen servicios genéricos o comunes, por ejemplo la notificación de alarmas 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), en las que pueden utilizarse diversas tecnologías y para las que se han elaborado varias Recomendaciones. Se presenta aquí el caso de la red de acceso óptica pasiva de banda ancha (BPON, *broadband passive optical network*). Para la administración de privilegios de usuario de esta red de acceso se utiliza la metodología de modelado unificado de la Rec. UIT-T Q.834.3. Los intercambios de gestión por el método CORBA (arquitectura de intermediario de petición de objetos común) se especifican en Q.834.4. La interfaz que se describe en dichas Recomendaciones es la interfaz Q que se muestra en la figura 6-11 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 6-12 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.

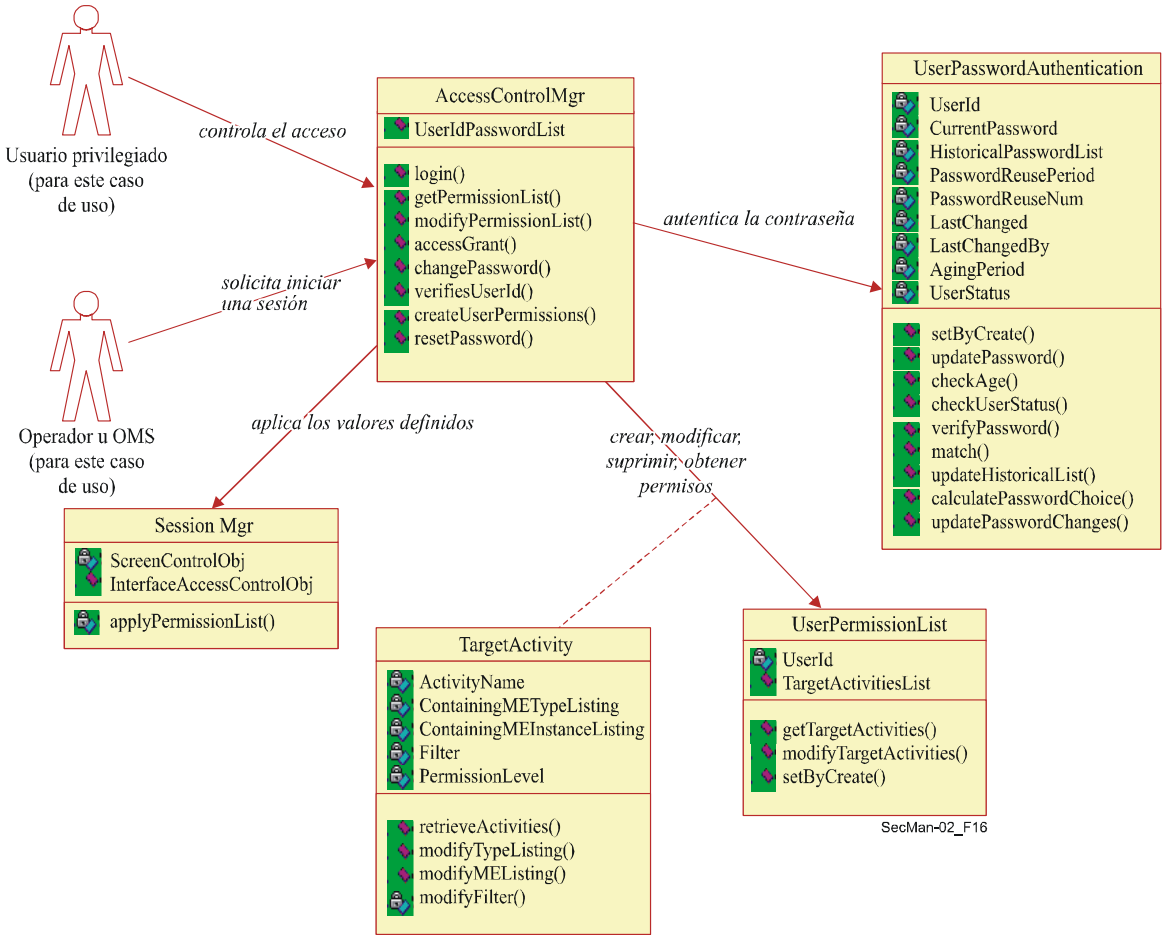


Figura 6-12 – Administración de privilegios de usuarios conforme a Q.834.3

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 es una de las especificaciones para el primer aspecto, la actividad de gestión de un servicio. El usuario que tiene enlaces preconfigurados utiliza este servicio 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 sólo los usuarios autorizados pueden 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 sección 2.4 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 6-13 se presentan los escenarios a) y b) relativos al inicio de la actividad de gestión de supervisión efectuado bien sea por la red propia o por la visitada. El sistema detección de fraude en la red propia pide información sobre las actividades cuando un abonado se inscribe en una red visitada hasta que deja esta red o suspende el registro. Se pueden definir perfiles de acuerdo con la utilización, basados en los registros detallados de llamadas y al rastreo (análisis) a nivel de servicio o de un abonado. El sistema detección de fraude puede entonces analizar y generar las alarmas adecuadas para comportamientos fraudulentos.

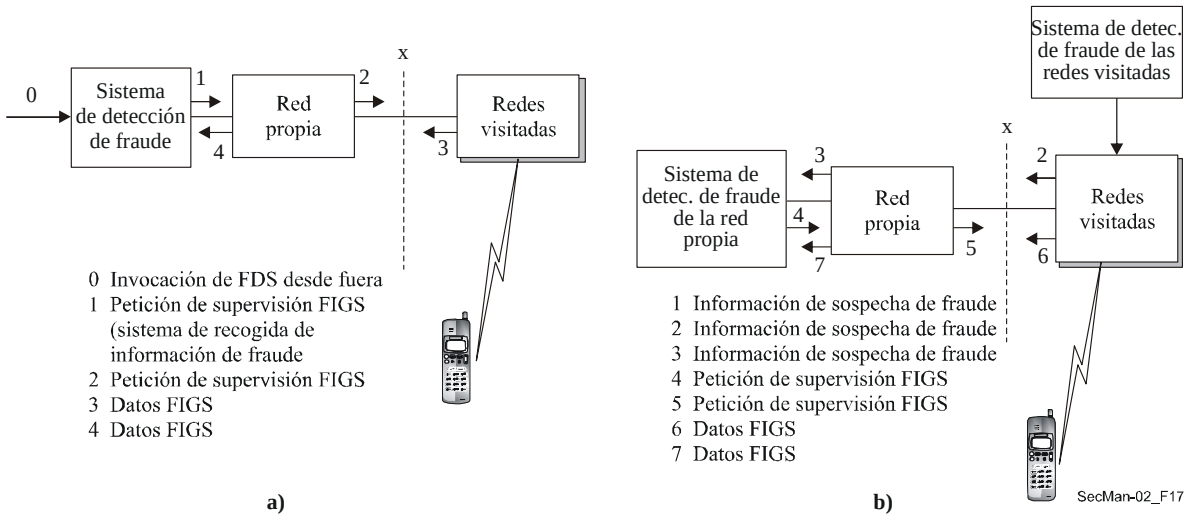


Figura 6-13 – Servicio de gestión de fraudes para los servicios inalámbricos conforme a la Rec. UIT-T M.3210.1

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 proteger 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 gestión (de operaciones) 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, los *operadores entre centrales*, ofrecen 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 señalar estos problemas en los servicios. Se recomienda también que los sistemas y usuarios autorizados hagan lo necesario para conocer el estado de los problemas señalados.

En la figura 6-14 se muestran las interacciones que necesitan protección. 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.

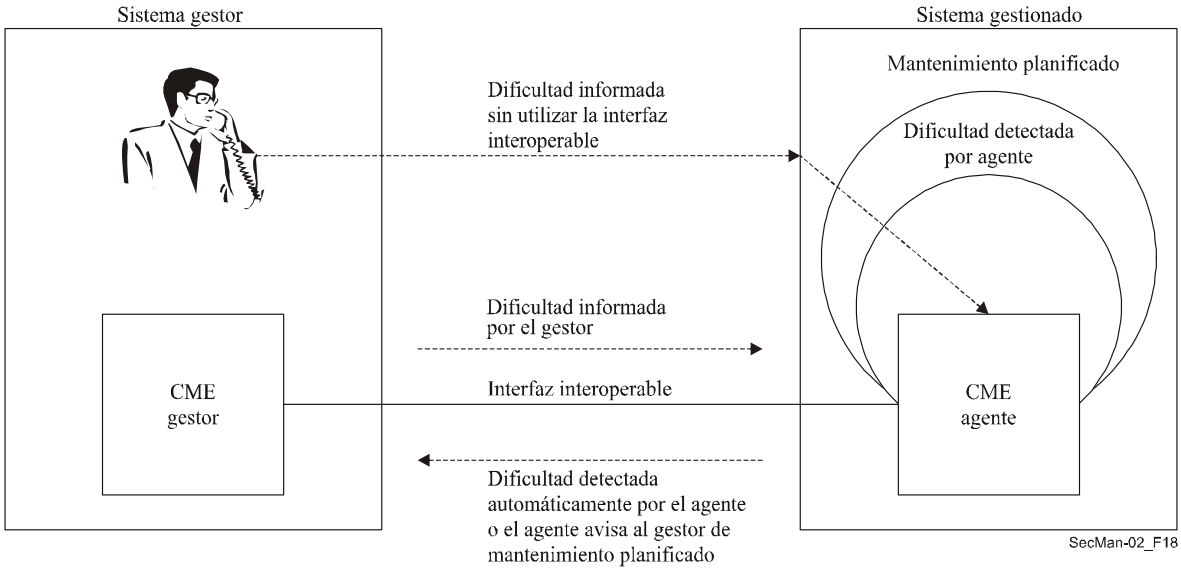


Figura 6-14 – Creación de informe de gestión de dificultades conforme a la Rec. UIT-T X.790

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.

6.4.5 Servicios comunes de gestión de seguridad

En las Recs. 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 el protocolo CMIP en la interfaz. A continuación se hace una breve descripción de los servicios incluidos en estas Recomendaciones. Cabe señalar que todas estas funciones se consideran adecuadamente como actividades del plano de gestión.

6.4.5.1 Función de informe de alarmas de seguridad: La notificación de alarmas en general es una función clave de las interfaces de gestión. Cuando se detecta un fallo operacional (un fallo del paquete de circuitos) o por una violación de la política de seguridad, se envía una alarma al sistema de gestión. En los informes de alarma se incluye una serie de parámetros que permiten al sistema de gestión determinar la causa del fallo y tomar las medidas correctivas necesarias. Los parámetros de cualquier evento incluyen un campo obligatorio denominado tipo de evento y un conjunto de otros campos de información de evento, que son la gravedad de la alarma, las causas probables de la alarma, el detector de la violación de seguridad, etc. Las causas de alarma están asociadas con los tipos de eventos como se muestra en el cuadro 6-2.

Cuadro 6-2 – Causas de alarmas de seguridad

Tipo de evento	Causas de alarmas de seguridad
Violación de integridad	Duplicación de información Pérdida de información Detección de modificación e información Información fuera de secuencia Información inesperada
Violación operativa	Denegación de servicio Fuera de servicio Error de procedimiento Motivo no especificado
Violación física	Problemas del cable Detección de intrusión Motivo no especificado
Violación del mecanismo o el servicio de seguridad	Fallo de autenticación Infracción de confidencialidad Fallo del mecanismo de no repudio Intento de acceso no autorizado Motivo no especificado
Violación del dominio temporal	Retardo de la información Expiración de claves Actividad extemporánea

Estas causas de alarma están más detalladas en X.736. Varias de ellas están relacionadas con las amenazas que se han expuesto en las cláusulas anteriores.

6.4.5.2 Función pista de auditoría de seguridad: Para que un usuario de gestión de seguridad pueda registrar las violaciones y llevar un registro de auditoría, la Rec. UIT-T X.740 identifica una serie de eventos que pueden someterse a auditoría. Se trata de conexiones, desconexiones, utilizaciones de mecanismos de seguridad, operaciones de gestión y contabilidad de la utilización. El modelo utiliza un mecanismo de registro definido en la Rec. UIT-T X.735, que es un registro temporal general donde se inscriben todos los eventos generados en el sistema gestionado. En la función pista de auditoría se definen dos eventos que tienen que ver con las violaciones de seguridad: informe de servicio e informe de utilización. El informe de servicio atañe a la prestación, denegación o recuperación de un servicio. El informe de utilización se emplea para indicar que se ha creado un registro con datos estadísticos pertinentes a la seguridad. Se han definido, como se hace para cualquier otro evento, una serie de causas relativas al informe de servicios: la petición de servicio, la denegación de servicio, el fallo de servicio, la recuperación de servicio, etc. Se podrán definir en un futuro nuevos tipos de eventos, ya que es posible que los dos eventos de esta Recomendación no sean suficientes.

6.4.5.3 En la Rec. UIT-T X.741 se presenta una definición muy detallada del modelo utilizado para asignar un control de acceso a las distintas entidades gestionadas. Las definiciones de control de acceso de esta Recomendación satisfacen varios requisitos: protección de la información de gestión para impedir la creación, supresión o modificación no autorizada, adecuación de las operaciones permitidas en las entidades según los derechos de acceso de los iniciadores de las operaciones, y la prevención de la transmisión de información de gestión a receptores no autorizados. Se definen distintos niveles de control de acceso para satisfacer los requisitos mencionados. En lo que atañe a las operaciones de gestión, la Recomendación permite restringir el acceso en múltiples niveles: la entidad gestionada en su conjunto, los atributos de la entidad, los valores de los atributos, el contexto del acceso y acciones sobre la entidad. Se ha identificado una serie de procedimientos: lista de control de acceso, gestión basada en la capacidad, en las etiquetas o en el contexto. La política de control de acceso puede aplicar uno o más de estos procedimientos. En este modelo, basado en la política y en la información de control de acceso (ACI, *access control information*), se determina la decisión de permitir o denegar la operación solicitada. La ACI incluye, por ejemplo, las normas, la identidad del iniciador, las identidades de los objetivos cuyo acceso se requiere, la información atinente a la autenticación del iniciador, etc. Este modelo tiene muchas características y todas las aplicaciones no requieren necesariamente todas las capacidades.

6.4.5.4 Servicios de seguridad basados en CORBA: Si bien las series de Recomendaciones UIT-T X.700 están basadas en la hipótesis de utilización de CMIP como protocolo de interfaz de gestión, la industria ha optado en ocasiones por introducir un protocolo, servicios y modelos de objetos basados en el intermediario de petición de objetos común para las interfaces de gestión. En la Rec. UIT-T Q.816 se define un marco para la utilización de estos servicios en el contexto de las interfaces de gestión. Para soportar los requisitos de seguridad para estas interfaces, esta Recomendación se refiere a la especificación OMG de servicios comunes para la seguridad.

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 tecnologías de comunicación e información (ICT, *information and communications technologies*) 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 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 ICT 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, *management information systems*) 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 Rec. UIT-T 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 profesional de la salud ha de existir un órgano superior que le 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, *national health system*), 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 (o directorios) 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, 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 6-15 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.

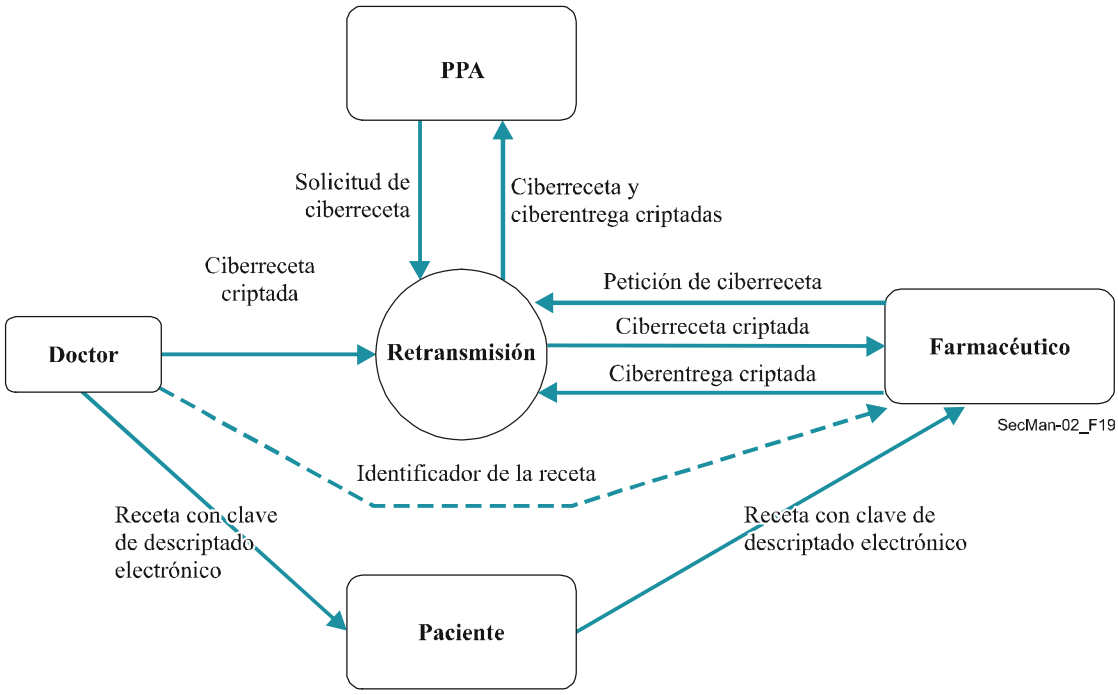


Figura 6-15 – Sistema de ciberrecetas de Salford

En el ejemplo de la figura 6-15, 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 farmacéutico, 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 farmacéuticos, 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 Rec. UIT-T X.509 a fin de lograr un acceso más generalizado y global a las ciberrecetas médicas.

6.6 Comunicaciones de datos móviles seguras de extremo a extremo

Hay muchos terminales móviles con capacidad de comunicación de datos (los teléfonos móviles IMT-2000, las computadoras portátiles, las agendas digitales personales (PDA) con tarjeta inalámbrica) y están surgiendo nuevos servicios de aplicación (por ejemplo, comercio electrónico móvil) para los terminales móviles conectados a la red móvil. La seguridad es necesaria, incluso esencial, en el entorno del comercio electrónico.

Hay muchas esferas de seguridad que se están estudiando desde el punto de vista de los operadores móviles (por ejemplo, arquitectura de seguridad para la red telefónica móvil IMT-2000). No obstante, también es importante estudiarlas desde el punto de vista del usuario móvil y del proveedor de servicios de aplicaciones (ASP, *application service provider*).

En el contexto de la seguridad de las comunicaciones móviles desde el punto de vista del usuario y del ASP, uno de los aspectos más importantes es la seguridad de las comunicaciones móviles de datos de extremo a extremo entre un terminal móvil y un servidor de aplicación.

Además, en el caso de un sistema móvil con una red móvil conectada a una red abierta, es necesario hacer un estudio de la seguridad de las capas superiores (aplicaciones, presentación y sesión) del modelo de referencia OSI, puesto que hay varias implementaciones posibles para las redes móviles (por ejemplo, red de telefonía móvil IMT-2000, LAN inalámbrica, Bluetooth) o las redes abiertas.

6.6.1 Marcas de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo

En la Rec. UIT-T X.1121 se describen modelos de comunicaciones móviles de datos de extremo a extremo seguras entre terminales móviles y servidores de aplicación en las capas superiores. Se definen dos tipos de modelos de seguridad para el marco de las comunicaciones móviles de datos de extremo a extremo entre un usuario móvil y un ASP: el modelo general y el modelo de pasarela. Un usuario móvil utiliza el terminal móvil para acceder a diversos servicios móviles de los ASP. Un ASP proporciona servicios móviles a los usuarios móviles a través de un servidor de aplicación. La pasarela de seguridad del servicio móvil retransmite paquetes de los terminales móviles al servidor de aplicación, transforma un protocolo de comunicaciones de red móvil en un protocolo de red abierta y viceversa.

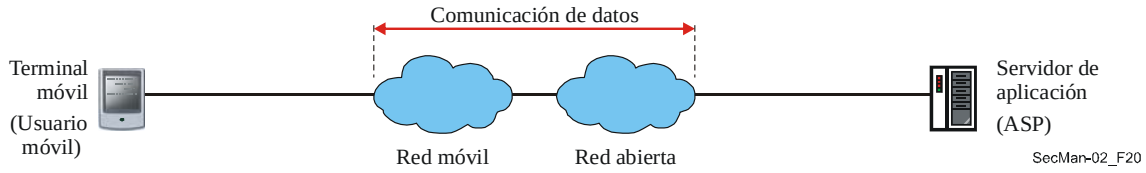


Figura 6-16 – Modelo general de comunicación de datos de extremo a extremo entre un usuario y un ASP

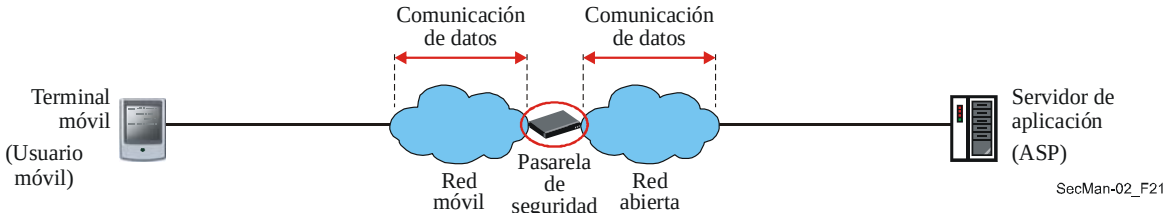


Figura 6-17 – Modelo de pasarela para las comunicaciones móviles de datos de extremo a extremo entre un usuario móvil y un ASP

En la Rec. UIT-T X.1121 también se describen las amenazas de seguridad que pueden afectar las comunicaciones móviles de datos de extremo a extremo y los requisitos de seguridad desde el punto de vista del usuario móvil y del ASP para ambos modelos. Hay dos tipos de amenazas: la general de todas las redes abiertas, y otra específica a las comunicaciones móviles. En la figura 6-18 se muestran las amenazas que pueden afectar la red de comunicaciones móviles de datos de extremo a extremo.

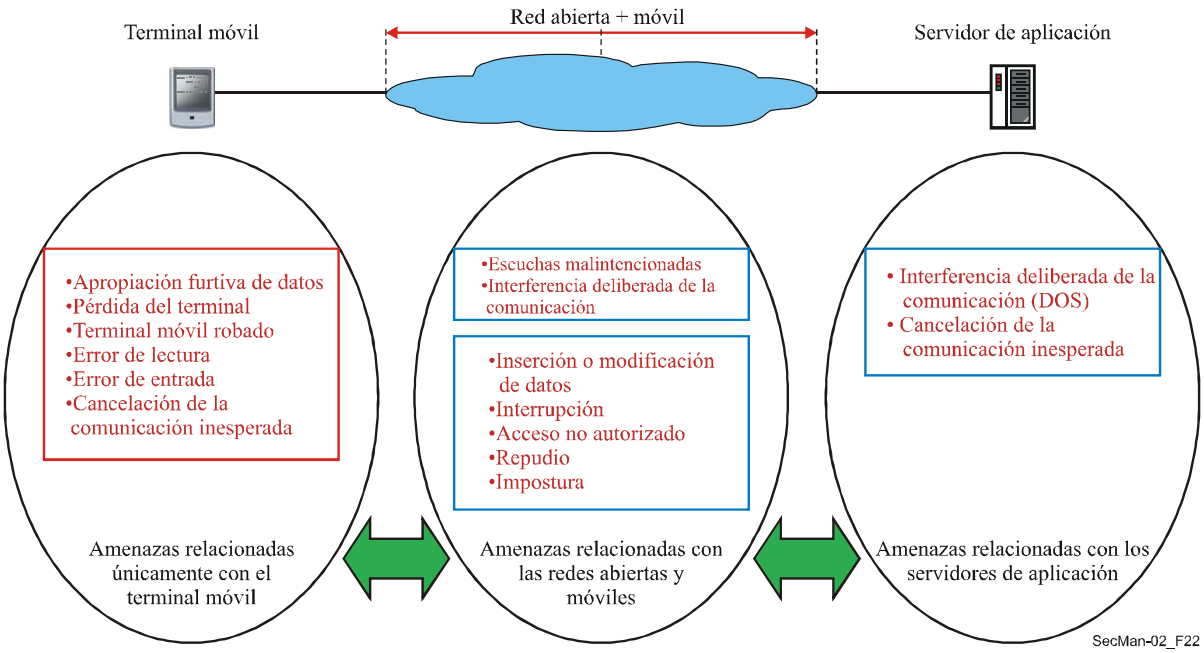


Figura 6-18 – Amenazas para las comunicaciones móviles de extremo a extremo

Además, en la Rec. UIT-T X.1121 se identifican los puntos en que se aplican las tecnologías de seguridad, cuando se requieran para cada una de las entidades, y la relación entre las entidades y las entidades en una comunicación de datos móvil de extremo a extremo (véase la figura 6-19).

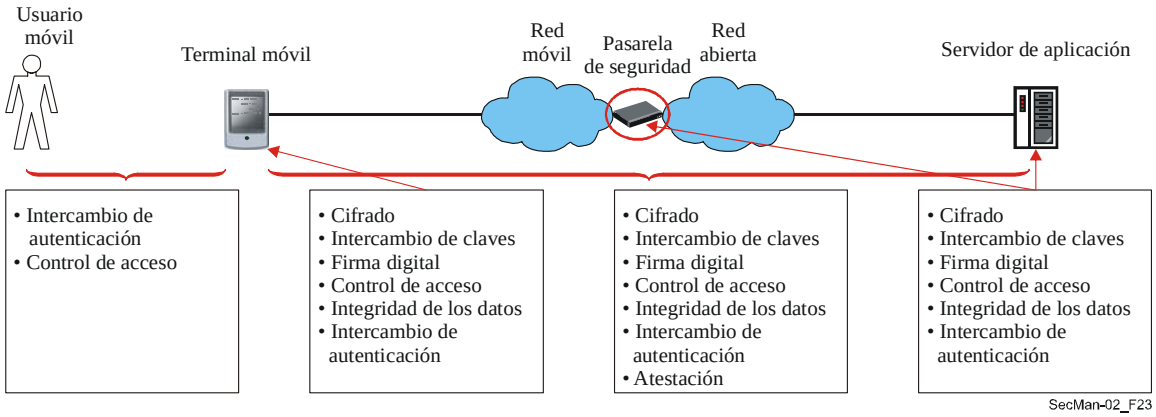


Figura 6-19 – Funciones de seguridad requeridas para cada entidad y relación entre entidades

6.6.2 Consideraciones de PKI para las comunicaciones móviles de datos de extremo a extremo seguras

En esta sección se hace referencia a la Rec. UIT-T X.1122. Aunque la tecnología PKI es muy útil para proteger las comunicaciones móviles de datos de extremo a extremo, algunas características específicas de este tipo de comunicaciones pueden requerir una adaptación de la tecnología PKI para crear sistemas móviles seguros. Se han definido dos modelos de PKI para proporcionar servicios de seguridad a las comunicaciones móviles de extremo a extremo. El es un modelo PKI general que no incluye funciones de pasarela de seguridad en las comunicaciones de datos móviles de extremo a extremo, y el otro es el modelo PKI de pasarela, donde hay una pasarela de seguridad que conecta la red móvil con la red abierta. En la figura 6-20 se muestra el modelo PKI general para las comunicaciones móviles de extremo a extremo. En este modelo participan cuatro entidades. La CA del usuario móvil expide un certificado a este usuario y gestiona un registro donde se almacena la lista de revocación de certificados (CRL, *revocation bit*) que ya ha expedido la CA. La autoridad de validación de usuario móvil (VA, *validation authority*) proporciona un servicio de validación de certificados en línea para los usuarios móviles. La CA del ASP expide un certificado al proveedor de servicios de aplicación y gestiona un registro donde se almacena la lista de revocación de certificados que ya ha expedido la CA del ASP. La autoridad de validación del ASP proporciona un servicio de validación de certificados en línea para los certificados de ASP.

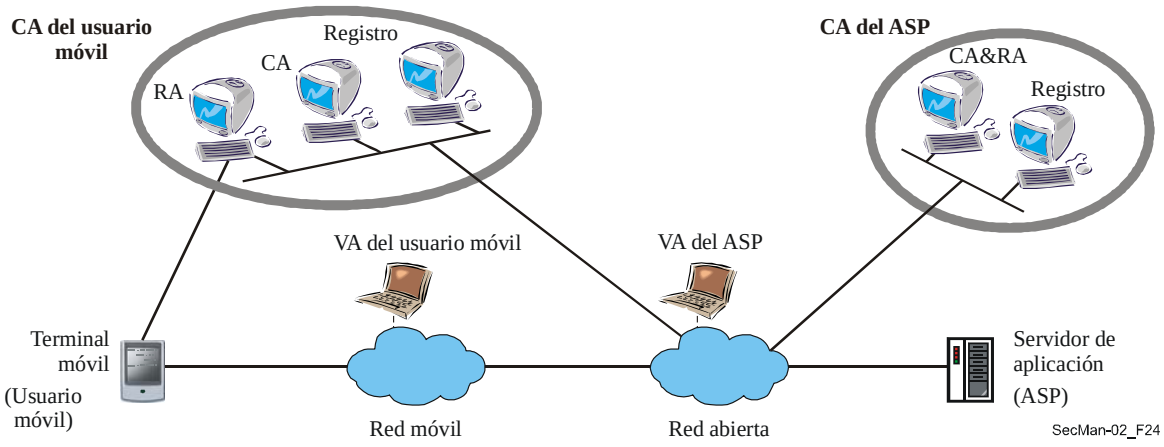


Figura 6-20 – Modelo PKI general para las comunicaciones móviles de datos de extremo a extremo

Hay dos métodos de expedición de certificados, dependiendo de la entidad que genera las claves públicas/privadas. En el primero, la fábrica del terminal móvil genera y fabrica un par de claves criptográficas; en el otro método, el par de claves criptográficas las genera el terminal móvil o una llave protegida contra falsificaciones, por ejemplo una tarjeta inteligente anexa al terminal móvil. En la figura 6-21 se muestra el procedimiento según el cual el terminal móvil adquiere un certificado utilizando el procedimiento de gestión de certificados en el que el par de claves criptográficas se genera en el terminal móvil.

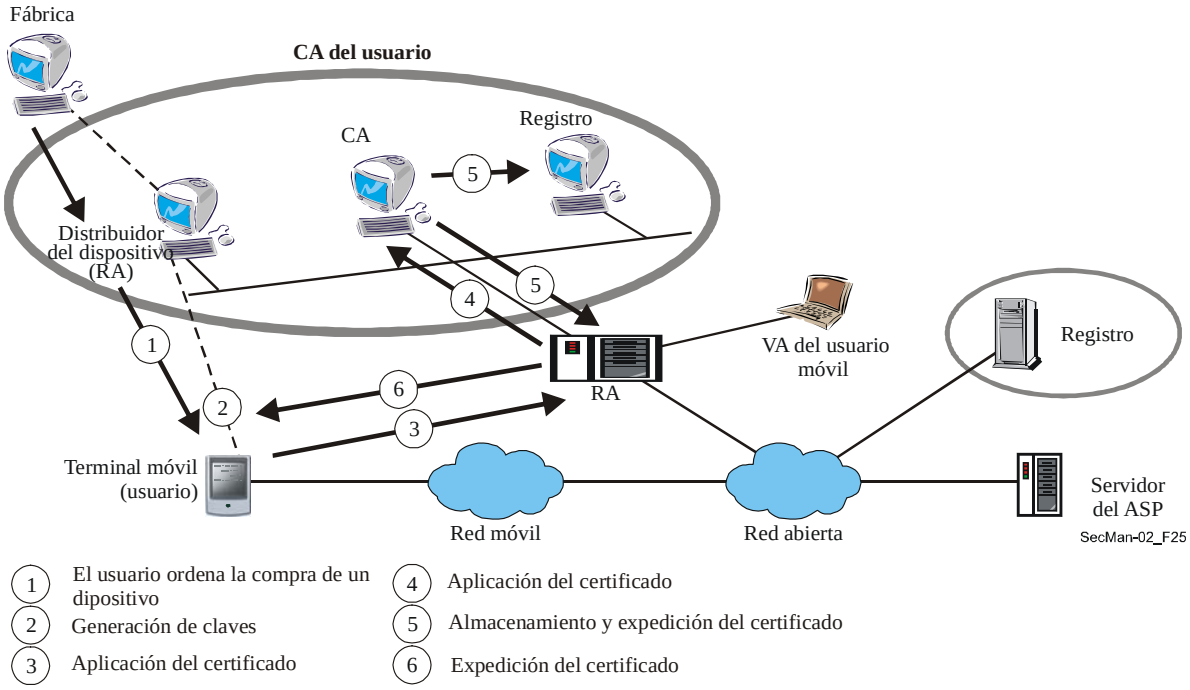


Figura 6-21 – Procedimiento de expedición de certificados por terminal móvil

El terminal móvil tiene una capacidad computacional y una memoria limitadas. Por eso es preferible utilizar un servicio de validación de certificados en línea, más bien que un servicio de validación de certificados fuera de línea basado en la CRL. Cuando el terminal móvil recibe el par mensaje-firma con la cadena de certificados y quiere verificar la validez de la firma, el certificado se utilizará una vez comprobada la validez mediante la función correspondiente. En la figura 6-22 se muestra el procedimiento de validación de certificados en línea para un terminal móvil.

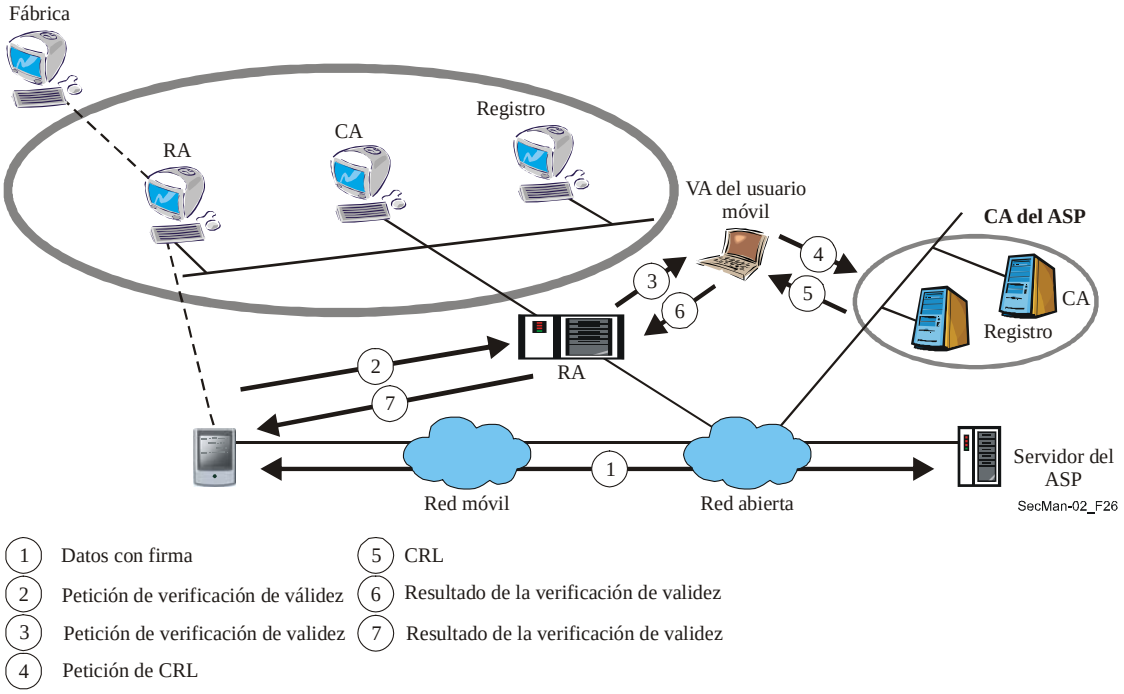


Figura 6-22 – Procedimiento de validación de certificados para las comunicaciones móviles de datos extremo a extremo

El sistema PKI para las comunicaciones móviles de extremo a extremo puede utilizarse con dos modelos: uno para la capa de sesión, y el otro para la capa de aplicación. El modelo para la capa de sesión proporciona servicios de seguridad tales como la autenticación de cliente, la autenticación de servidor y el servicio de confidencialidad e integridad. El modelo de la capa de aplicación proporciona un servicio de no repudio y de confidencialidad para las comunicaciones móviles de datos de extremo a extremo.

En conclusión, la Rec. UIT-T X.1122 describe los elementos que hay que tener en cuenta al elaborar sistemas móviles seguros basados en PKI desde el siguiente punto de vista: la interoperabilidad con los sistemas PKI existentes en redes abiertas, la utilización de PKI en el entorno móvil (incluida la generación de claves, la aplicación y expedición de certificados, la utilización de certificados y las CA) y el PKI en general (incluida la gestión de la expedición de certificados durante el ciclo de utilización). Puede utilizarse como documento orientativo al elaborar sistemas móviles seguros basados en la tecnología PKI.

7 Disponibilidad y capa de infraestructura

En la Rec. UIT-T X.805, que se presenta en la sección 2, se hace referencia a:

- las dimensiones de seguridad, como un conjunto de medidas de seguridad diseñadas para solventar algún aspecto concreto de la seguridad de la red; y

- las capas de seguridad. Las dimensiones de seguridad se aplican a una jerarquía de equipos de red y grupos de instalaciones, que se denominan capas de seguridad.

La dimensión de seguridad disponibilidad garantiza que no se denegará el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones por causa de cualquier evento que ocurra en la red. En esta categoría se incluyen las soluciones de recuperación en caso de catástrofe.

La capa de seguridad de infraestructura está formada por instalaciones de transmisión de red y elementos de red protegidos por las dimensiones de seguridad. La capa de infraestructura representa los componentes básicos de las redes, sus servicios y aplicaciones. Pueden citarse como ejemplos de los componentes de la capa de infraestructura los encaminadores, conmutadores y servidores, así como los enlaces de comunicación entre distintos encaminadores, conmutadores y servidores.

El UIT-T especifica muchos requisitos funcionales, operacionales o de aplicación diversos al determinar estos conceptos, para las características de errores, el control de congestión, el informe de fallos y las acciones correctivas, entre otras. El resto de la presente sección ofrece distintas visiones de los requisitos relacionados con las redes de telecomunicaciones cuyo objetivo es limitar los riesgos y consecuencias de la indisponibilidad de los recursos de transmisión.

Para que los operadores de redes de telecomunicaciones seleccionen la topología de red adecuada en cuanto a los objetivos de disponibilidad, se propone una referencia al anexo A a la Rec. UIT-T G.827, *Ejemplos de topologías de trayectos y cálculos de la disponibilidad de los trayectos de extremo a extremo*.

7.1 Topologías de trayectos y cálculos de disponibilidad de los trayectos de extremo a extremo

En las figuras 7-1 y 7-2 se muestran las topologías de trayecto básicas que pueden construirse utilizando elementos de trayecto predefinidos.

En la figura 7-1 se muestra un trayecto básico simple sin protección, y en la figura 7-2 el mismo trayecto con la adición de una protección de extremo a extremo, que debería tener un encaminamiento distinto para que la protección sea máxima.

Este tipo de protección se denomina 1+1. Cada trayecto es una conexión bidireccional donde la señal transmitida por cada extremo está permanentemente conectada a ambos trayectos y un dispositivo de conmutación en cada receptor selecciona la mejor señal.

Es más económico utilizar un trayecto de protección para proteger varios trayectos. Es la configuración 1:n que requiere conmutadores de selección tanto en los transmisores como en los receptores.

A los efectos de los cálculos de disponibilidad de extremo a extremo, es más conveniente utilizar la tasa de indisponibilidad. En el anexo A a la Rec. UIT-T G.827 pueden encontrarse algunos principios básicos para evaluar la disponibilidad para un trayecto básico simple (figura 7-1), con una protección de extremo a extremo 1+1 (figura 7-2) o una relación de protección 1:n.

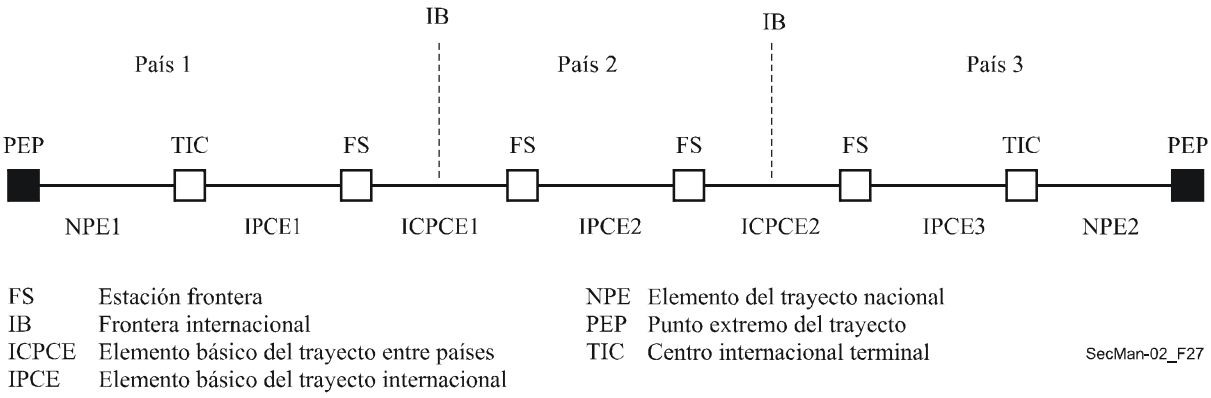


Figura 7-1 – Ejemplo de un trayecto básico simple sin protección

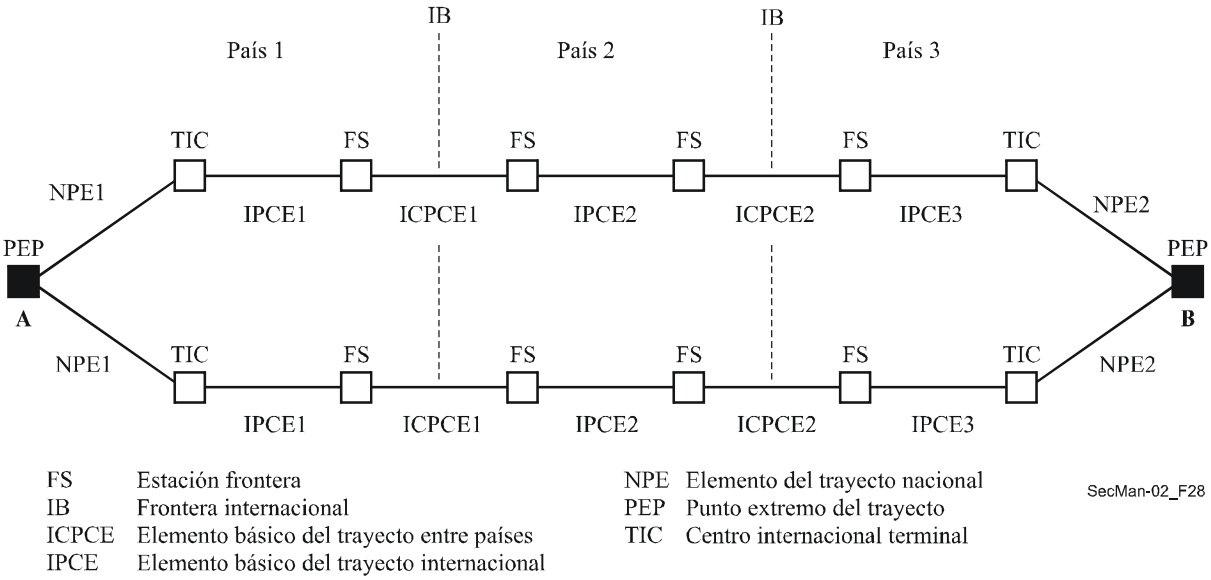


Figura 7-2 – Ejemplo de un trayecto con protección de extremo a extremo

En la sección 7.3 se presentan topologías más complejas, por ejemplo, la topología de anillo de jerarquía digital síncrona (SDH, *synchronous digital hierarchy*) en la que el tráfico puede reencaminarse circunvalando un enlace en estado de fallo, por una ruta de protección que depende de las capacidades de conmutación de los distintos nodos del anillo y que no es necesariamente la distancia más corta entre dos nodos. En el caso de topologías más complejas resulta más difícil evaluar la disponibilidad. Diversos artículos de los que figuran en el apéndice I/G.827 tratan de esta cuestión.

7.2 Mejora de la disponibilidad de una red de transporte – Presentación general

En las secciones 7.2 a 7.4 se describen las características de la arquitectura de los métodos más comúnmente utilizados para mejorar la disponibilidad de una red de transporte. Esta mejora se logra sustituyendo las entidades de transporte en estado de fallo o degradadas, por otras entidades de recursos dedicados o compartidos. La sustitución generalmente se lleva a cabo tras la detección de un defecto, una degradación de la calidad de funcionamiento o una petición externa (por ejemplo, gestión de red).

Protección – Se utiliza una capacidad preasignada entre nodos. La arquitectura más simple está compuesta por una entidad de protección dedicada para cada entidad de trabajo (1+1). La arquitectura más compleja tiene m entidades de protección compartidas entre n entidades de trabajo (m:n). La conmutación de protección puede ser unidireccional o bidireccional. La conmutación de protección bidireccional produce efectos en ambas direcciones del tráfico, incluso cuando el fallo es unidireccional. La conmutación de protección unidireccional produce efectos de conmutación únicamente en la dirección de tráfico afectada en el caso de un fallo unidireccional.

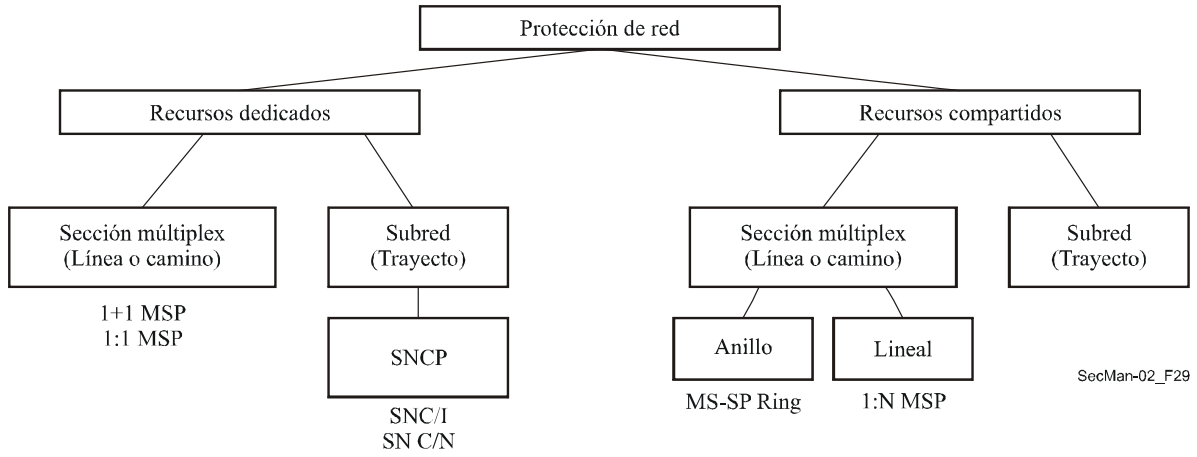
Restablecimiento – Se utiliza cualquier capacidad disponible entre nodos. En general, los algoritmos utilizados para el restablecimiento conllevan un reencaminamiento. En caso de restablecimiento se reserva una parte de la capacidad de la red de transporte para el reencaminamiento del tráfico de trabajo.

En la Rec. UIT-T G.805 puede encontrarse información esencial sobre estos aspectos.

7.3 Protección

Una alta disponibilidad de servicio sólo puede lograrse utilizando una infraestructura de red con gran fiabilidad y supervivencia. Así, de haber un fallo en un equipo de gran fiabilidad, es necesario poder conmutar a una fuente alternativa de señal (canal de protección).

Hay dos tipos de protección. La *protección del equipo* está basada en la creación de grupos de circuitos redundantes: en caso de fallo de hardware en un grupo de circuitos se conmuta automáticamente a otro. La *protección de red* protege contra los cortes de fibra gracias a trayectos alternativos para que la señal pueda seguir su camino. Estos trayectos alternativos pueden ser dedicados o compartidos. Estos mecanismos están representados en la figura 7-3.



SNC/I	Protección de conexión de subred/supervisión inherente
SNC/N	Protección de conexión de subred/supervisión no intrusiva
SNCP	Protección de conexión de subred
1+1 MSP	Conmutación de protección 1+1 de la sección múltiplex
1:N MSP	Conmutación de protección 1:N de la sección múltiplex
MS-SPRing	Anillo de protección compartido de la sección múltiplex

Figura 7-3 – Variaciones de la conmutación de protección

Los mecanismos de protección pueden ser unidireccionales o bidireccionales. También pueden ser reversivos y no reversivos. Los siguientes términos se definen en la Rec. UIT-T G.780/Y.1351.

La *protección unidireccional* se define como aquella que "en caso de un fallo unidireccional (es decir, un fallo que afecta solamente a un sentido de la transmisión), se produce una conmutación únicamente en el sentido afectado (del camino, de la conexión de subred (SNC, *subnetwork connection*), etc.)". Esto significa que sólo se toma una decisión local en el lado del receptor (nodo local) sin tener en cuenta el estado del nodo distante al realizar una conmutación de protección. Esto ocurre en el caso de un fallo unidireccional (es decir, un fallo que afecta solamente a un sentido de la transmisión), y sólo se produce una conmutación de protección en el sentido afectado.

La *protección bidireccional* se define como aquella en la que "en el caso de un fallo unidireccional, se produce una conmutación de protección en los dos sentidos (del camino, de la conexión de subred, etc.)". Esto significa que se tiene en cuenta el estado local y distante al realizar una conmutación de protección. Esto ocurre en el caso de un fallo unidireccional (es decir, que afecta a un solo sentido de la transmisión) y se produce una conmutación de protección en el sentido afectado y también en el otro sentido.

La *operación (de protección) revertiva* se define de la siguiente manera "en la operación revertiva, la señal (servicio) de tráfico siempre vuelve al SNC/camino de trabajo (o se mantiene en él) cuando terminan las peticiones de conmutación, es decir, cuando el SNC/camino de trabajo se ha recuperado del defecto o ha finalizado la petición externa". En el modo revertivo, la señal en el canal de protección se vuelve a conmutar al canal de trabajo cuando éste se ha recuperado del fallo.

La *operación (de protección) no revertiva* se define de la siguiente manera "en la operación no revertiva, la señal (servicio) de tráfico no vuelve al SNC/camino de trabajo cuando las peticiones de conmutación se dan por terminadas". En el modo no revertivo (aplicable únicamente a las arquitecturas 1+1), cuando el canal de trabajo en estado de fallo se recupera, se mantiene la selección de la señal de tráfico normal o protegida en el canal de protección.

Los tipos de protección más comunes son:

- 1:1 MSP (conmutación de protección 1:1 de la cláusula múltiplex, véase 7.3.1)
- 1+1 MSP (conmutación de protección 1+1 de la cláusula múltiplex, véase 7.3.2)
- MS-SPRing (anillo de protección compartido de la cláusula múltiplex, véase 7.3.3)
- SNCP (protección de conexión de subred, véase 7.3.4)

Estos mecanismos de protección se exponen más detalladamente a continuación. No obstante, son de aplicación las siguientes Recomendaciones de referencia: G.841 (características), G.842 (interfuncionamiento), G.783 (modelos funcionales), G.806 (defectos) y G.808.1 (conmutación de protección genérica).

7.3.1 Conmutación de protección 1:1 de la cláusula múltiplex

El diagrama de red se representa en la figura 7-4.

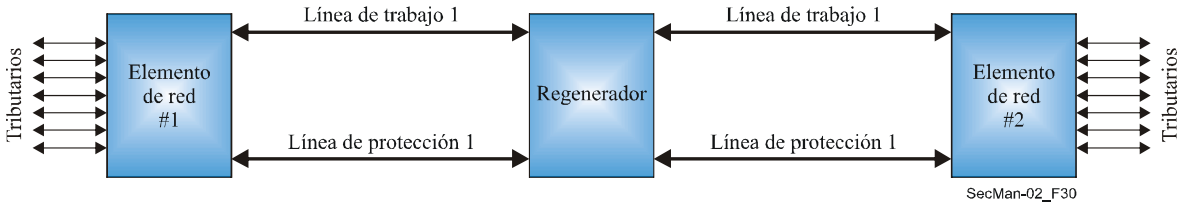


Figura 7-4 – Diagrama de red para la conmutación de protección 1:1

En la conmutación de protección 1:1 hay un canal de protección para cada canal de trabajo. El canal de protección puede transportar otro tráfico, y en ese caso será reemplazado.

La figura 7-5 es un diagrama del elemento de red.

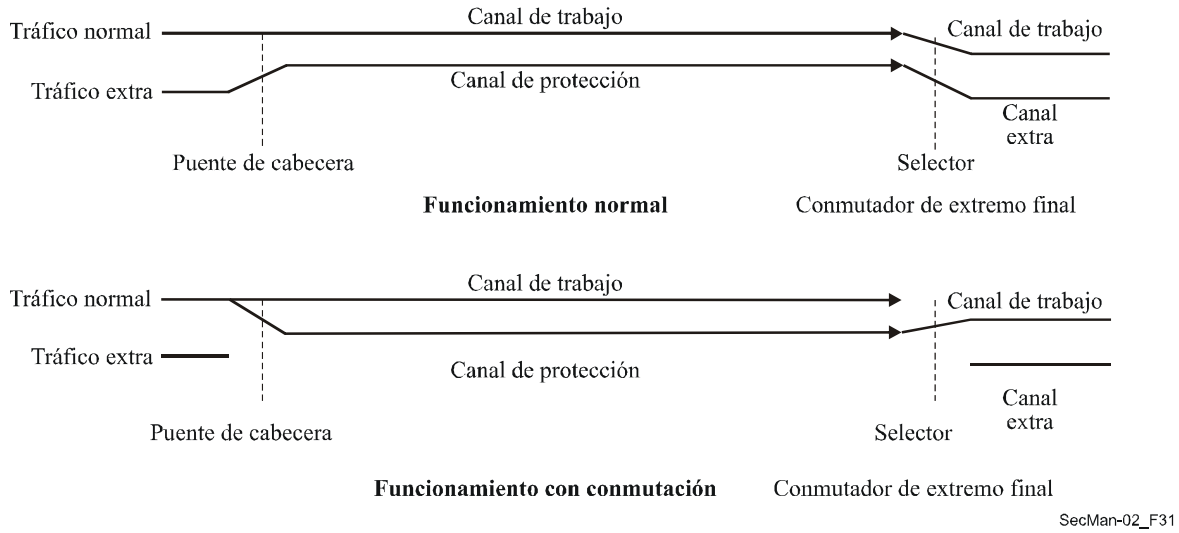


Figura 7-5 – Protección lineal 1:1 de la sección múltiplex

En situación normal, el "tráfico extra" puede transportarse por el canal de protección. No obstante, si se reciben los bytes K1/K2 correctos (activando la función de protección), el "tráfico normal" se puentea al canal de protección en la "cabecera" y se conmuta en el "extremo final". Este control se realiza gracias a los bytes K1 y K2 en el canal de protección.

Es equivalente a la protección de línea en el módulo de transporte síncrono, nivel N (STM-Nivel N (N ≥1)).

Hay varias causas de conmutación: una conmutación forzada y una serie de defectos o condiciones de fallo (por ejemplo, fallo de la señal, pérdida de la señal, pérdida de tramas, exceso de errores, degradación de la señal). Pueden encontrarse más detalles al respecto en la Rec. UIT-T G.806.

7.3.2 Conmutación de protección 1+1 de la sección múltiplex

En la figura 7-6 se muestra el diagrama de red.

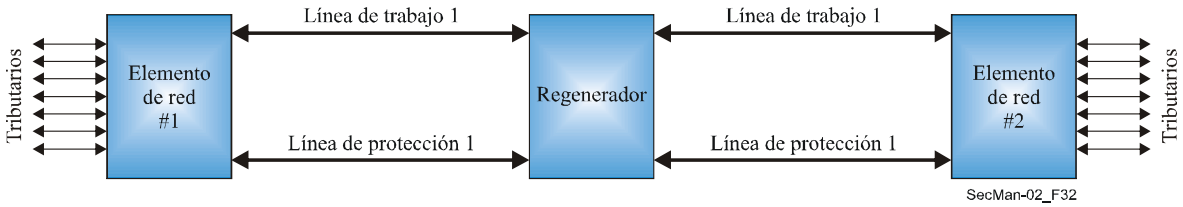


Figura 7-6 – Diagrama de red para la conmutación de protección 1+1

En la conmutación de protección 1+1 hay un canal de protección para cada canal de trabajo. El canal de protección transporta una copia de las señales de los canales de trabajo.

La figura 7-7 es un diagrama del elemento de red.

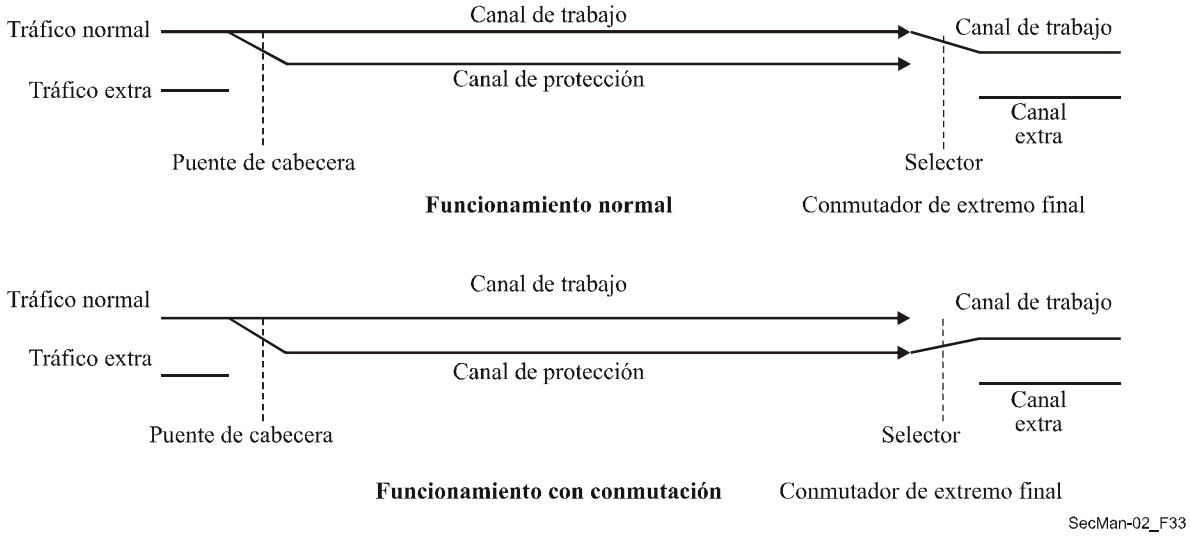


Figura 7-7 – Protección lineal 1+1 de la sección múltiplex

La señal transmitida se puentea permanentemente a la línea de protección. El receptor selecciona la mejor señal.

En este plan de protección 1+1 no hay capacidad para "tráfico extra". Es una función de protección de línea y sólo vale para STM-n sea cuál sea la velocidad de la línea. Puede considerarse como una subfunción de la conmutación de protección 1:1. No requiere un mecanismo de control (bytes K1 y K2 de conmutación de protección automática (APS, *automatic protection switching*) de la tara de la sección múltiplex (MSOH, *multiplex section overhead*)) para funcionar. La conmutación se produce por las mismas condiciones de fallo que se exponen en 7.3.1.

Hay otra versión de este mecanismo de protección denominado 1+1 bidireccional, con conmutación en los selectores de ambos extremos, lo que requiere un control ejercido por los bytes K1/K2 que se transmiten.

7.3.3 Conmutación de protección MS-SPRing

En la figura 7-8 se muestra el diagrama de red.

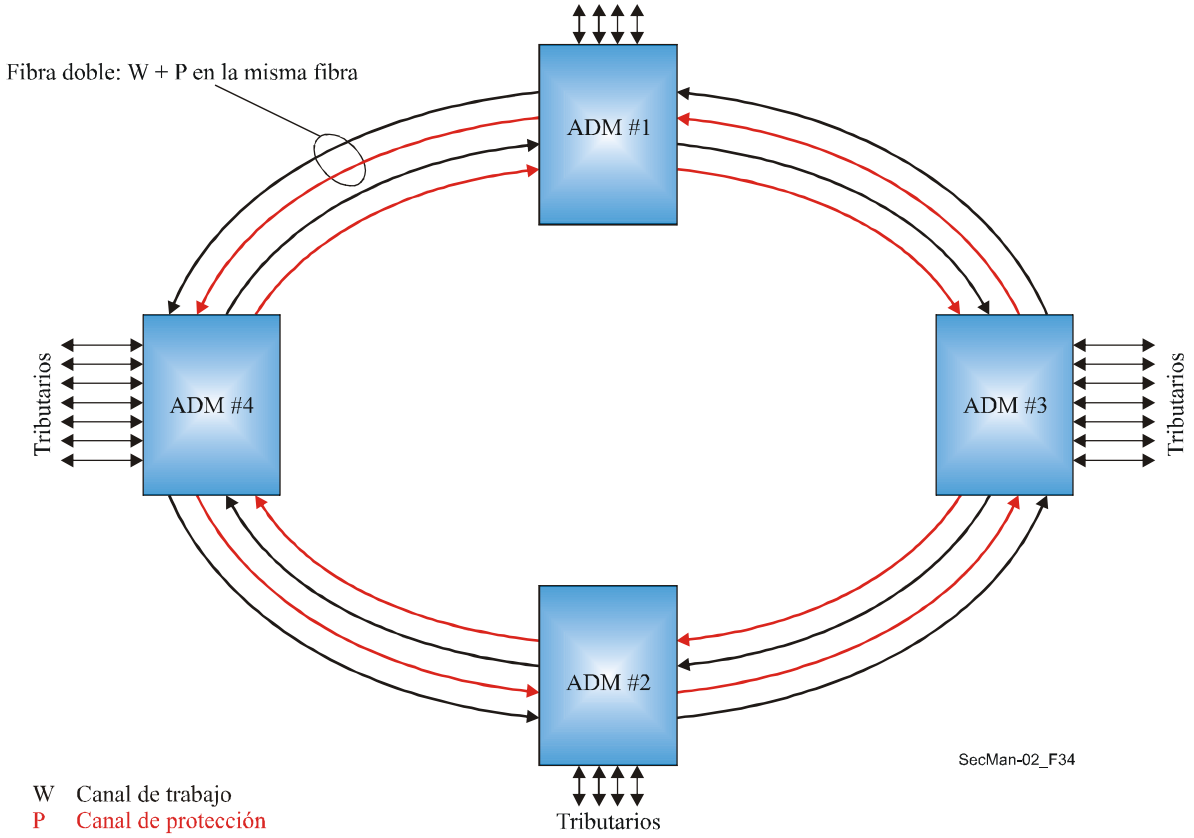


Figura 7-8 – Diagrama de red para la conmutación de protección MS-SPRing

En la red SDH suele haber mayoritariamente una configuración MS-SPRing de fibra doble. Hay 2 fibras para cada tramo del anillo, y cada una de ellas transporta la mitad de la anchura de banda de los canales de trabajo y protección (por ejemplo, una línea STM-64 con unidades administrativas (AU, *administrative units*) AU-4 de 1 a 32 para el canal de trabajo y AU-4 de 33 a 64 para la protección). El tráfico normal transportado por los canales de trabajo en una fibra está protegido por los canales de protección en el sentido opuesto.

En la figura 7-9 se muestra la función MS-SPRing de dos fibras.

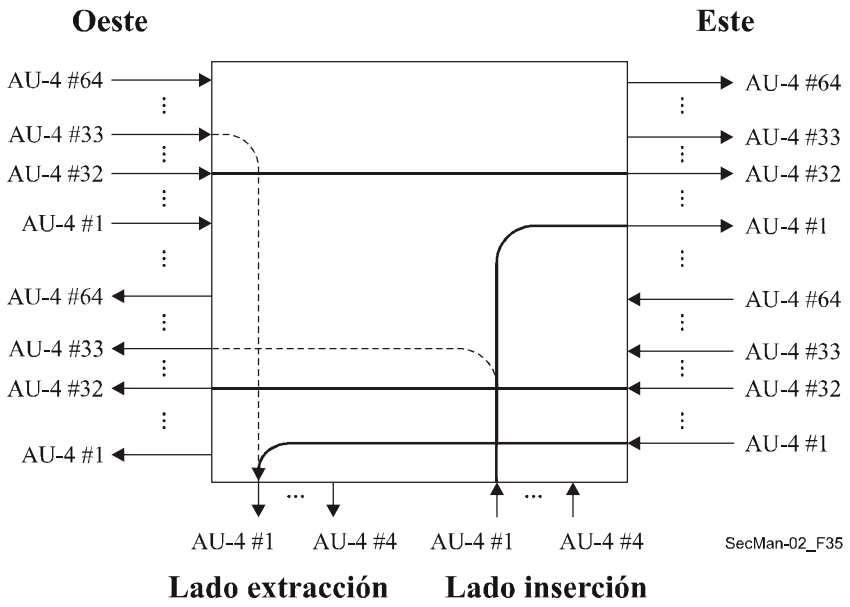


Figura 7-9 – Anillo STM-64 con inserción-extracción STM-4

En la figura 7-9, la señal constituyente "Insertar AU-4 #1" se transfiere a la señal " "Transmisión Este AU-4 #1. La señal "Recepción Este AU-4 #1" se extrae en "Extraer AU-4#1". También hay una conexión directa en AU-4 #32 representada en la figura 7-9.

De haber una interrupción en la fibra Este, hay que transmitir la señal "Insertar Add AU-4 #1" por el lado de protección Oeste ("Transmitir Oeste AU-4 #33") y extraer la señal recibida por el lado de protección Oeste ("Recepción Oeste AU-4 #33") en "Extraer AU-4#1". La señal AU-4 #32 del lado Oeste se devolverá a AU-4 #64. La señal AU-4 #32 del lado Este se habría devuelto al canal de protección (AU-4 #64) en el otro lado del paso, lo que obliga a devolver al canal de trabajo la protección ("Recepción Oeste AU-4 #64") en este nodo (AU-4 #32).

La conmutación de protección se realiza con una granularidad AU-4 o AU-3 en todas las señales de la fibra. Las peticiones y acuses de recibo se transmiten utilizando los bytes K1 y K2 de conmutación de protección automática (APS) de la tara de la sección múltiplex (MSOH). K1 y K2 se transmiten en la línea que transporta los canales de protección. Se transmiten en ambas direcciones (Este y Oeste) siendo uno el trayecto corto y el otro el trayecto largo.

Se aplica el silenciamiento para evitar la transmisión de tráfico al cliente erróneo en caso de aislamiento o fallo del nodo donde se realiza inserción/extracción de tráfico (servicios del mismo intervalo de tiempo pero en distintos tramos). Puede encontrarse una descripción del silenciamiento en el apéndice II/G.841.

Las condiciones de fallo en caso de fallo de señal o degradación de la señal son idénticos al de la conmutación de protección lineal (véase 7.3.1).

Hay tres configuraciones de conmutación que considerar:

- Normal (no hay fallos).
- Fallo en el lado Este (hay que devolver Oeste y sólo insertar/extraer en Oeste).
- Fallo en el lado Oeste (hay que devolver Este y sólo insertar/extraer en Este).
- Conmutación de tramo para MS-SPRing de 4 fibras (conmutación de protección, sin devolución).

7.3.4 Conmutación de protección SNCP

En la figura 7-10 se muestra el diagrama de la red.

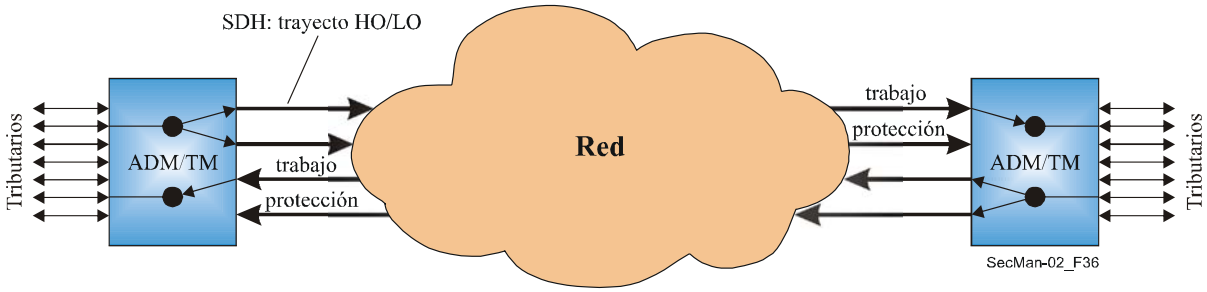


Figura 7-10 – Conmutación de protección SNCP

La protección de conexión de subred (SNCP) se basa en el trayecto, por lo que sólo se conmuta una señal (AU-3, AU-4, etc.) cada vez. También puede considerarse como un 1+1 unidireccional para trayectos individuales. La conmutación de protección se hace a nivel de trayecto.

- SDH: Contenedor Virtual de Orden Superior HO – VC-4/3.
  Unidad Tributaria de Orden Inferior LO – TU-3/2/11/12.

No se utiliza ningún protocolo (excepto para la conmutación forzada). La decisión de conmutar entre un canal de trabajo y uno de protección depende de las condiciones locales, al supervisarse ambos canales.

- Es necesario que la conmutación de protección se realice en menos de 50 ms. En caso de corte en una fibra con gran anchura de banda, por ejemplo, 10 Gbit/s o 40 Gbit/s, y estando todos los trayectos con protecciones SNCP, generalmente este objetivo de tiempo no puede lograrse si la conmutación de protección se realiza en un software que incluye un procesamiento de defectos en una máquina de estados y hay intercambio de mensajes entre la placa y el controlador central.

7.4 Restauración

En la Rec. UIT-T G.805 se describen las técnicas de mejora de disponibilidad de la red de transporte. Se utilizan para clasificar estas técnicas los términos "protección" (sustitución de un recurso en fallo por otro preasignado en espera) y "restablecimiento" (sustitución de un recurso en fallo mediante reencaminamiento utilizando la capacidad sobrante). En general, las acciones de protección se realizan en decenas de milisegundos, mientras que el tiempo de restablecimiento está entre cientos de milisegundos y algunos segundos.

El plano de control de una red óptica con conmutación automática (ASON, *automatic switched optical network*) proporciona al operador de red la capacidad de ofrecer a un usuario llamadas con clase de servicio (CoS, *class of service*) seleccionable, (por ejemplo, disponibilidad, duración de la interrupción, segundos con errores, etc.). La protección y el restablecimiento son mecanismos (de la red) para soportar la CoS que solicita el usuario. La selección del mecanismo de supervivencia (protección, restablecimiento o ninguno) para una conexión concreta que soporta una llamada se basará en la política del operador de red, la topología de la red y la capacidad del equipo instalado. Pueden utilizarse distintos mecanismos de supervivencia en las conexiones que se concatenan para realizar una llamada. Si la llamada transita por las redes de más de un operador, cada una de ellas es responsable de la supervivencia de las conexiones del tránsito. Las peticiones de conexión en la UNI o la E-NNI contendrán únicamente la CoS solicitada, sin indicar ningún tipo de protección o restablecimiento.

La protección o el restablecimiento de una conexión puede invocarse o inhabilitarse temporalmente mediante una instrucción del plano de gestión. Esas instrucciones permiten realizar las actividades de mantenimiento previstas, y también anular las operaciones automáticas si se dan condiciones de fallo excepcionales.

Véase la Rec. UIT-T G.8080/Y.1304.

7.5 Planta exterior

La cuestión de la seguridad de los sistemas de telecomunicaciones comprende muchos aspectos. Los relacionados con la seguridad física de la planta exterior también forman parte del mandato del UIT-T. Se estudian soluciones para que el hardware de un sistema resista a incendios, catástrofes naturales o intrusiones intencionales o accidentales. Las dos cuestiones de seguridad más importantes son la manera de hacer que los componentes de sistemas, cables, recintos, armarios, etc., sean físicamente resistentes a los daños, los sistemas de supervisión para prevenir daños siempre que sea posible o responder ante los problemas que surjan y restaurar la funcionalidad del sistema de la manera más rápida posible.

En general, los principales factores que han de considerarse en este ámbito son:

- causa de daño/pérdida de datos:
  - mantenimiento de red;
  - accidentes y calamidades (no intencionales);
  - vandalismo (intencional; aleatorio);
  - acceso de personal no cualificado (por ejemplo, civiles, técnicos de otros operadores);
  - criminalidad (por ejemplo, daño de un terminal o cortocircuito para robo; robo de cables; escuchas ilegales en un cable); e
  - intencionales; fuerza concentrada o violencia;
- situaciones del entorno de la planta:
  - interiores (central, locales del cliente);
  - exterior aérea (exposición a acciones humanas/naturales);
  - exterior a nivel del suelo (posibilidad de daños por obras); y
  - exterior subterráneo (en conductos o enterrado directamente).

En general, se recomienda adoptar las siguientes precauciones en lo que concierne a la capa física. La mayor parte de estas precauciones forman parte de las prácticas y normas de cada operador:

- evitar la utilización de nodos a nivel del suelo (armarios, pedestales, cajas): quedan expuestos a los accidentes, vandalismo, acciones violentas, incendios y curiosidad en general y es más seguro utilizar nodos y cables subterráneos;
- los armarios (y otras cajas) a nivel del suelo deben ser robustos "contra intrusiones";
- todos los recintos se podrán cerrar con llave o precintar para evitar cualquier acceso no deseado;
- los cables de plantas por conductos son menos vulnerables que los directamente enterrados: piénsese en la degradación accidental por operaciones de cavado;
- los puntos de terminación o demarcación pueden tener una separación (que se pueda bloquear) entre la red y el lado del cliente, o entre circuitos utilizados por distintos operadores;
- los terminales de clientes en interiores son menos vulnerables que las terminaciones exteriores (en paredes) (por ejemplo, en caso de robo);
- puede ser recomendable almacenar remanentes de cable en ubicaciones seguras de la red para facilitar la reparación de un daño accidental (tanto en ubicaciones aéreas como subterráneas);
- en una planta de fibra óptica, se recomienda una separación de circuitos por niveles adecuada además de una estabilidad óptica dinámica para evitar la pérdida de datos/perturbaciones de tráfico durante el mantenimiento de la red; y
- para las líneas indispensables, puede recomendarse la redundancia (líneas de reserva) mediante cables y redes físicamente separados (por ejemplo, estructuras en anillo para bancos, hospitales).

Otras medidas que pueden adoptarse son:

- establecimiento de procedimientos de seguridad en las instalaciones en exteriores;
- instalación de sistemas de detección antiincendios, supervisión y control de la planta exterior;
- definición de criterios para evaluar la coexistencia segura en la misma parte de la red de varios operadores que proporcionan varios servicios, como POTS, RDSI, xDSL, etc., sin interacciones perjudiciales;
- utilización de soluciones técnicas que faciliten la implementación del principio de desagregación, manteniendo al mismo tiempo la integridad, la fiabilidad y la interoperabilidad de las topologías de red que se utilizan comúnmente en todo el mundo;
- instalación de dispositivos de señalización a lo largo de los cables subterráneos;
- supervisión, mantenimiento de soporte y sistemas de prueba para la planta exterior;
- definir correctamente las características de los cables, cuya función primaria es la protección de la integridad física del medio de transmisión (las fibras ópticas); y
- tener en cuenta los aspectos atinentes a la construcción de cables, división de fibras, organización y recintos, unidades de derivación, planificación de rutas, las características de los buques que tienden los cables, actividades de carga y descarga, métodos de reparación, métodos de protección y prueba para los cables de fibra óptica terrenales y marinizados.

8 Organización de incidentes y tratamiento de incidentes de seguridad (directrices) en las organizaciones de telecomunicaciones

La gestión de la seguridad conlleva una serie de procesos entre los que se cuenta la definición de estructuras y los procedimientos para tratar y divulgar la información relacionada con incidentes de seguridad. También en esta esfera los expertos del UIT-T se han involucrado, reconociendo las necesidades y elaborando la Rec. UIT-T E.409. El objetivo de la Rec. UIT-T E.409, *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones*, es analizar como estructurar y sugerir un método de creación de un sistema de gestión de incidencias dentro de una organización de telecomunicaciones que presta servicios de telecomunicaciones internacionales, y los aspectos fundamentales son el flujo en caso de incidente y la estructura del incidente. El flujo y el tratamiento son útiles a la hora de determinar si un evento ha de clasificarse como evento, incidente, incidente de seguridad o crisis. El flujo en caso de incidente incluye las primeras decisiones críticas que han de tomarse.

En esta Recomendación se presenta un panorama general y un marco que orienta a la hora de planificar la organización de incidentes y el tratamiento de incidentes de seguridad.

Se trata de una Recomendación genérica que no identifica ni establece requisitos para determinadas redes.

Si bien el objetivo de esta Recomendación es facilitar el desarrollo internacional de la seguridad de las redes de telecomunicaciones, será más eficaz si los requisitos también pueden aplicarse a las redes de información y comunicaciones (ICN, *information and communication networks*) nacionales.

Con el uso cada vez mayor de computadoras para las telecomunicaciones internacionales ha aparecido la ciberdelincuencia. En los últimos años es un fenómeno que crece exponencialmente, como confirman diversas investigaciones nacionales e internacionales. La mayoría de países no disponen de cifras exactas sobre el número de intrusiones e incidentes de seguridad informáticos, especialmente en lo que atañe a las telecomunicaciones internacionales.

La mayor parte de empresas u organizaciones de telecomunicaciones no disponen de un sistema especializado para el tratamiento de los incidentes de seguridad en las redes de información y comunicaciones (ICN) (aunque algunos disponen de un equipo encargado de crisis de cualquier tipo). En caso de incidente de seguridad en una ICN, las personas que lo detectan tratan de solucionarlo de la mejor manera posible. En algunas organizaciones puede intentarse olvidar el incidente o cubrirlo ya que puede afectar a la producción, disponibilidad e ingresos.

A menudo, cuando se detecta un incidente de seguridad en una ICN, la persona que lo detecta no sabe a quién remitirlo, lo que puede dar como resultado que el administrador del sistema o la red evite el problema o lo solucione rápidamente para quitárselo de en medio. No tienen la suficiente autoridad, tiempo o experiencia para corregir el sistema de manera que el incidente de seguridad no vuelva a ocurrir. Por eso es conveniente disponer de una unidad o grupo formado para tratar los incidentes de seguridad de manera rápida y correcta. Además, muchos problemas pueden darse en esferas tan diversas como la relación con los medios, asuntos jurídicos, cumplimiento con la ley, participación en el mercado o finanzas.

Cuando se trata un incidente, o se informa de él, la utilización de diversas taxonomías puede crear problemas de comprensión y por este motivo es probable que el incidente de seguridad no reciba la atención adecuada ni se trate con suficiente rapidez para solucionarlo y evitar que vuelva a ocurrir. Las consecuencias para la organización afectada (víctima) pueden ser graves.

Para tratar satisfactoriamente un incidente y dar buena cuenta de él, es necesario entender cómo se detectan, tratan y resuelven los incidentes. Una estructura general para incidentes (físicos, administrativos o de organización y lógicos) permite definir un panorama general de la estructura y el flujo en caso de incidente. Para que haya un entendimiento común es básico contar con una terminología uniforme.

8.1 Definiciones

El término incidente de seguridad puede definirse como "una infracción de seguridad, amenaza, punto débil y disfuncionamiento que puede tener repercusión sobre la seguridad de los activos de la organización". En esta Recomendación, incidente es menos grave que incidente de seguridad. Un incidente de seguridad de la información es un tipo concreto de incidente de seguridad.

En la figura 8-1 se muestra la pirámide de eventos. En su base se encuentra el evento, seguido del incidente, el incidente de seguridad y en la cúspide la crisis y la catástrofe. Cuanto más cerca de la cúspide se encuentre el evento, más grave es. Para utilizar un vocabulario común y claro sobre el tratamiento de los incidentes en las ICN, se recomienda utilizar las siguientes definiciones.

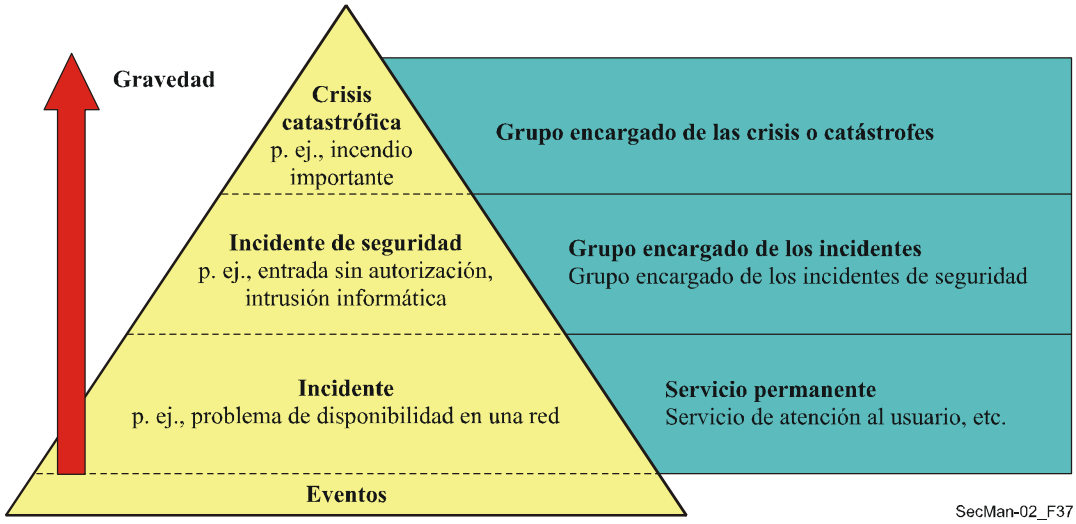


Figura 8-1 – La pirámide de eventos de la Rec. UIT-T E.409

8.1.1 **Evento**: Suceso perceptible que no se puede predecir o controlar (completamente).

8.1.2 **Incidente**: Un evento cuyas consecuencias no son graves.

8.1.3 **Incidente de seguridad**: Cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

8.1.4 **Incidente de seguridad en las redes de información y la comunicación (ICN)**: Cualquier evento adverso, real o potencial, relacionado con la seguridad de las ICN. Por ejemplo:

- intrusión en los sistemas de computación de las ICN a través de la red;
- aparición de virus informáticos;
- sondeos de vulnerabilidad de distintos sistemas de computación a través de la red;
- filtración a través de una central automática privada conectada a la red pública (PABX);
- cualquier otro evento no deseado que surge de acciones internas o externas no autorizadas, incluidos los ataques de denegación de servicio, catástrofes y otras situaciones de emergencia, etc.

8.1.5 Crisis: Estado causado por un evento, o por el hecho de saber que un evento es inminente, que puede tener consecuencias negativas graves. Durante una crisis se puede, en el mejor de los casos, tomar medidas para evitar que ésta se convierta en una catástrofe. En general, se dispone de un plan de previsión de accidentes (BCP, *business contingency plan*) y de un equipo encargado de la gestión de crisis para que se ocupe de la situación.

8.2 Bases

Se recomienda a las organizaciones de telecomunicaciones que creen grupos encargados de los incidentes (de seguridad informática) empiecen por especificar la taxonomía de incidentes a fin de evitar malentendidos. La colaboración es más fácil cuando se utiliza el mismo "idioma".

Se recomienda utilizar las expresiones incidente e incidente de seguridad en una ICN, y establecer subcategorías basándose en la gravedad de este último. En esencia, un incidente de seguridad en una ICN podría ser cualquier evento no deseado y no autorizado, lo que significa que un incidente de seguridad en una ICN incluye una intrusión informática, un ataque por denegación de servicio o un virus dependiendo de la motivación, la experiencia y los recursos de que dispone la organización. En las organizaciones que ya disponen de un equipo eficaz antivirus, los virus pueden considerarse como simples incidentes y no como incidentes de seguridad en una ICN.

Un ejemplo modelo de esta subdivisión es:

– Incidentes

  - Violación de las normas de conducta de Internet (*Internet netiquette)* (correo no deseado, contenido ofensivo, etc.)
  - Violación de las políticas de seguridad
  - Virus particulares

– Incidentes de seguridad en una ICN

  - Exploraciones y sondeos de la vulnerabilidad
  - Intrusiones informáticas
  - Sabotaje y daño a los computadores (ataques contra la disponibilidad, como por ejemplo "programa bombas" o ataques de denegación de servicio)
  - Programas informáticos dolosos (virus, caballos de troya, gusanos, etc.)
  - Robo de información y espionaje
  - Suplantación de identidad

La utilización de la misma granularidad y precisión en la terminología puede permitir ganar experiencia acerca de:

- las directrices relativas a la gravedad y alcance;
- los indicios sobre la rapidez de reacción (por ejemplo, para restablecer el nivel requerido de seguridad);
- las posibles contramedidas; y
- los posibles costos que entrañan.

9 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 sección 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 tecnologías de información. 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 y con la colaboración de otras organizaciones de normalización (por ejemplo, ISO/CEI JTC1/SC27).

Referencias

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

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

[Chadwick] CHADWICK (D.W.), "*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] EUCHNER (M.), PROBST (P.-A.), "*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] CHADWICK (D.W.), MUNDY (D.), "*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 Telecommunication Security" www.itu.int/ITU-T/studygroups/com17/tel-security.html (Catalogue of Approved Recommendations related to Telecommunication Security; Approved ITU-T Security Definitions)

[Shannon] SHANNON (G.), "*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] MANDIL (S.), DARBELLAY (J.), "*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

ISO/CEI 18033-1:2005, *Information technology – Security techniques – Encryption algorithms – Part 1: General*

ISO/CEI 18033-2:2006, *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*

ISO/CEI 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*

ISO/CEI 18033-4:2005, *Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers*

Anexo A

Catálogo de Recomendaciones del UIT-T relacionadas con la seguridad

Recopilado por la Comisión de Estudio 17 del UIT-T, Comisión de Estudio Rectora sobre Seguridad de las Telecomunicaciones

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
E.408	Requisitos de seguridad para las redes de telecomunicaciones	Presenta un panorama general de los requisitos de seguridad y un marco que identifica las amenazas de seguridad en las redes de telecomunicaciones en general (tanto fijas como móviles, de voz y datos) y sirve de orientación para la planificación de contramedidas que pueden adoptarse para reducir estos riesgos.	CE 2
E.409	Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones	Analiza, estructura y sugiere un método para la creación de un sistema de gestión de incidentes dentro de una organización de telecomunicaciones que presta servicios de telecomunicaciones internacionales, tratando en particular del flujo en caso de incidente y de la estructura de los incidentes. El flujo y el tratamiento de los incidentes, sirven para determinar si un evento ha de clasificarse como evento, incidente, incidente de seguridad o crisis. El flujo en caso de incidente incluye las primeras decisiones fundamentales que han de adoptarse. Para poder tratar adecuadamente un incidente y dar informe de ello, debe entenderse adecuadamente cómo se detectan, tratan y resuelven los incidentes. Una estructura general de incidentes (físicos, administrativos u organizativos, y lógicos), permite obtener un panorama general de la estructura y el flujo de un incidente. Para entenderse es necesario tener una terminología uniforme.	CE 17
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 (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 mensajería de intercambio electrónico de datos (EDI, *electronic data interchange*) (F.435 + X.435) y el servicio de mensajería 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 sección 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.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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.	CE 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 sección 4.4 se explican con detalle los requisitos de seguridad.	CE 2
G.808.1	Conmutación de protección genérica – Protección lineal de camino y de subred	Esta Recomendación es una presentación general de la conmutación de protección lineal, y abarca los planes de protección para las redes ópticas de transporte (OTN, *optical transport networks*), las redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*) y las redes del modo de transferencia síncrono (ATM, *asynchronous transfer mode*). En otras Recomendaciones se presentarán los planes de protección en anillo y los principios de interconexión de subredes de nodo dual (por ejemplo, anillo).	CE 15
G.827	Parámetros y objetivos de disponibilidad para trayectos digitales internacionales de extremo a extremo de velocidad binaria constante	Se definen en esta Recomendación los parámetros y objetivos de calidad de funcionamiento de la red para los elementos del trayecto y la disponibilidad de extremo a extremo de los trayectos digitales con velocidad binaria constante. Estos parámetros son independientes del tipo de red física que soporta el trayecto de extremo a extremo, por ejemplo, fibra óptica, radiotransmisión o satélite. Se incluyen directrices sobre los métodos para mejorar la disponibilidad y calcular la disponibilidad de extremo a extremo de una combinación de elementos de red.	CE 12

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
G.841	Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona	En esta Recomendación se describen distintos mecanismos de protección para las redes de la jerarquía digital síncrona (SDH), sus objetivos y aplicaciones. Se presenta un principio de protección de camino SDH (en la capa de sección o trayecto) y un principio de protección de conexión de subredes SDH (con supervisión inherente, supervisión no intrusiva y supervisión de subcapa).	CE 15
G.842	Interfuncionamiento de las arquitecturas de protección para redes de la jerarquía digital síncrona	En esta Recomendación se describen mecanismos para el interfuncionamiento entre las arquitecturas de protección de redes, tanto para la interconexión de un nodo único como de nodo dual para el intercambio del tráfico entre anillos. Cada anillo puede configurarse con protección compartida de sección de multiplexión (MS) y protección de conexión de subred (SNCP).	CE 15
G.873.1	Red óptica de transporte: Protección lineal	Se define el protocolo de conmutación de protección automática (APS) y el funcionamiento de la conmutación de protección para los planes protección lineal de la red óptica de transporte al nivel de la unidad K de datos del canal óptico (ODUk, *optical channel data unit*). En esta Recomendación se especifican varios planes de protección: la protección de camino ODUk, la protección de conexión de subred ODUk con supervisión inherente, la protección de conexión de subred ODUk con supervisión no intrusiva, y la protección de conexión de subred ODUk con supervisión de subcapa.	CE 15
G.911	Parámetros y metodología de cálculo de la fiabilidad y la disponibilidad de los sistemas de fibra óptica	En esta Recomendación se identifica un conjunto mínimo de parámetros necesarios para caracterizar la fiabilidad y disponibilidad de los sistemas de fibra óptica. Se presentan distintos parámetros para la fiabilidad y mantenimiento del sistema, la fiabilidad del dispositivo óptico activo, la fiabilidad del dispositivo óptico pasivo y la fiabilidad de fibra óptica y cables. También presenta directrices y métodos para el cálculo de predicción de fiabilidad de los dispositivos, unidades y sistemas. Se incluyen ejemplos.	CE 15
H.233	Sistema con 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.	CE 16
H.234	Sistema de autenticación 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 descriptan 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*.	CE 16

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
H.235	Seguridad y criptado para terminales multimedias de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)	En esta Recomendación se describen las mejoras del marco de las Recomendaciones de la serie H.3xx que permiten ofrecer *servicios de seguridad* como la *autenticación* y la *privacidad (criptado de datos*). El esquema propuesto es aplicable a conferencias punto a punto y multipunto para cualquier tipo de terminales que utilicen el protocolo de control de la Rec. UIT-T H.245. Por ejemplo, los sistemas H.323 en redes de paquetes sin garantía de calidad de servicio. Por los mismos motivos técnicos, como la red básica no garantiza la calidad de servicio, tampoco proporciona un *servicio de seguridad*. La comunicación segura en tiempo real por redes no seguras presenta dos problemas principales: *la autenticación y la privacidad.* Se describe la infraestructura de seguridad y las *técnicas de privacidad* específicas que han de emplearse en los terminales multimedias de la serie H.3xx. Esta Recomendación abarca los principales problemas de la conferencia interactiva, entre los que se cuentan, aunque no únicamente, la *autenticación y la privacidad* de todos los trenes de medios en tiempo real que se intercambian durante una conferencia. Se proporciona el protocolo y los algoritmos necesarios entre entidades H.323. Esta Recomendación utiliza las características generales que se soportan en la Rec. UIT-T H.245 y, por ello, cualquier norma que se utilice junto con este protocolo de control puede utilizar este marco de seguridad. Se supone que, siempre que sea posible, otros terminales de la serie H serán compatibles y podrán utilizar directamente los métodos descritos en esta Recomendación. Esta Recomendación no proporciona desde un principio lo necesario para una implementación completa en todas las esferas, resaltando específicamente los aspectos de *autenticación de punto extremo y privacidad de medios.* Incluye la capacidad de negociar servicios y funcionalidades de manera genérica y de seleccionar las técnicas criptográficas y capacidades utilizadas. La manera específica en que se utilicen tiene relación con las capacidades del sistema, los requisitos de aplicación y las restricciones de política de seguridad específicas. Se soportan diversos algoritmos criptográficos, con diversas opciones adecuadas a distintos fines: por ejemplo, longitud de claves. Algunos *algoritmos criptográficos* pueden asignarse a servicios de seguridad específicos (por ejemplo, uno para la criptación rápida de tren de medios y otro para la criptación de señalización). También hay que señalar que algunos de los algoritmos o mecanismos criptográficos disponibles pueden estar reservados para exportación o para otros fines nacionales (por ejemplo, con longitud de clave restringida). Esta Recomendación soporta la señalización de algoritmos bien conocidos, además de la señalización de algoritmos criptográficos no normalizados o privados. No hay algoritmos obligatorios, aunque se recomienda vivamente que los puntos extremos soporten el mayor número de algoritmos aplicables posibles para lograr la interoperabilidad. Recuérdese que la conformidad con la Rec. UIT-T H.245 no garantiza la interoperabilidad entre los códecs de dos entidades. La versión 2 de la Rec. UIT-T H.235 sustituye a la versión 1 y añade diversas mejoras, como la criptografía de curva elíptica, los perfiles de seguridad (de contraseña simple y de firma digital sofisticada), nuevas contramedidas de seguridad (contra el correo no deseado), admisión del algoritmo de criptación avanzada (AES, *advanced encryption algorithm*), admisión del servicio de reserva, identificadores de objetos definidos y cambios incorporados de la guía de los implementadores H.323. La versión 3 de H.235 sustituye a la versión 2 y añade un procedimiento para señales DTMF criptadas, identificadores de objeto para el algoritmo de criptación AES para la criptación de la cabida útil de los medios, un modo de criptación de trenes de medios OFB mejorado (EOFB), una opción de sólo autenticación en el anexo D para un paso simple por un punto de traducción de direcciones de red (NAT) o un cortafuegos, un procedimiento de distribución de claves en el canal RAS, procedimientos para el transporte de claves de sesión más seguras y procedimientos más robustos de distribución y actualización de claves de sesión, procedimientos para la seguridad de múltiples trenes de cabida útil, mayor garantía de seguridad para llamadas con encaminamiento directo en el nuevo anexo I, medios de señalización para información de errores más flexible, aclaraciones y mejoras para la seguridad de arranque rápido y señalización Diffie-Hellman, así como parámetros Diffie-Hellman más largos y modificaciones originadas en la guía para implementadores H.323.	

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
		Anexo F/H.235: *Perfil de seguridad híbrido.* En este anexo se describe un *perfil de seguridad híbrido basado en la infraestructura de clave pública*, eficiente y escalable, que utiliza las *firmas digitales* del anexo E/H.235 y 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 del anexo E/H.235 se aplican realmente en un sentido ligero; las firmas digitales son aún conformes con los procedimientos RSA. Las *firmas digitales* se aplican sólo cuando es absolutamente necesario; de lo contrario, se utilizan *técnicas de seguridad simétricas* sumamente eficientes del perfil de seguridad básico descrito en el anexo D/H.235. 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/H.235 y, además, resuelve ciertos inconvenientes del anexo E/H.235 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. Incluye mecanismos de 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 necesita el modelo con encaminamiento por pasarela y se basa en las técnicas de tunelización H.245. La posibilidad de utilizar modelos con encaminamiento que no es pasarela queda en estudio. Anexo G/H.235: *Utilización del protocolo de gestión de claves MIKEY para SRTP en H.235*. Este anexo permite la implantación del protocolo de transporte en tiempo real seguro (SRTP, *secure real time transport protocol*) de IETF para la seguridad de medios, con un sistema de gestión de claves MIKEY que proporciona las claves necesarias y los parámetros de seguridad entre puntos extremos que participan en una comunicación de extremo a extremo. El anexo G puede utilizarse en un dominio H.323 entre sistemas H.323 conformes a la especificación del anexo G/H.235. Este anexo define extensiones del protocolo de seguridad para registro, admisión y estado (RAS) y señalización de llamada H.225.0, así como H.245, con sus correspondientes procedimientos. Además, este anexo proporciona las capacidades necesarias para el interfuncionamiento con entidades SIP IETF que aplican a la gestión de claves MIKEY y SRTP. Hay que señalar que este anexo es un perfil de seguridad de H.235, que se presenta como opción, y puede complementar otras características de seguridad de medios H.235 (véanse los anexos B y D.7). NOTA – H.235 se ha reestructurado de la siguiente manera: • H.235.0, Marco de seguridad H.323: Marco de seguridad para sistemas multimedias de la serie H (H.323 y otros basados en H.245). • H.235.1, Marco de seguridad H.323: Perfil de seguridad básico • H.235.2, Marco de seguridad H.323: Perfil de seguridad de firma • H.235.3, Marco de seguridad H.323: Perfil de seguridad híbrido • H.235.4, Marco de seguridad H.323: Seguridad de llamada con encaminamiento directo y selectivo • H.235.5, Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles • H.235.6, Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa H.235.7, Marco de seguridad H.323: Utilización del protocolo de gestión de claves MIKEY para el protocolo de transporte en tiempo real seguro en H.235 • H.235.8, Marco de seguridad H.323: Intercambio de claves para el protocolo de transporte en tiempo real seguro utilizando canales de señalización seguros • H.235.9, Marco de seguridad H.323: Soporte de pasarela de seguridad para H.323.	

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
H.323	Sistemas de comunicación multimedias basados en paquetes	La presente Recomendación describe terminales y otras entidades que proporcionan servicios de comunicaciones de audio, de video, de datos y multimedias en tiempo real por redes por paquetes (PBN, *packet based networks*) 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 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. Anexo J: Seguridad para tipos de punto a extremo simples.	CE 16
H.350.2	Arquitectura de servicios de directorio para H.235	Describe un esquema LDAP para representar los elementos H.235. Se trata de una clase auxiliar relacionada con H.350 y muchas de sus funcionalidades se derivan de esa arquitectura. Los implementadores deben revisar detalladamente H.350 antes de aplicar esta Recomendación. Sus atributos incluyen los elementos identidad, contraseña y certificado H.235. Estos elementos pueden descargarse en un punto extremo para configuración automática o el controlador de acceso puede obtenerlos para la señalización de llamada y la autenticación. El alcance de esta Recomendación no incluye métodos normativos para la utilización del directorio LDAP ni de los datos que contiene. El objetivo de este esquema no es representar todos los elementos de datos posibles del protocolo H.235, sino representar el conjunto mínimo requerido para alcanzar los objetivos de diseño de H.350.	CE 16
H.530	Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación 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 multimedias de H.323. Proporciona detalles sobre los procedimientos de seguridad para H.510. Hasta el presente, las capacidades de señalización de 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 multimedias pueden lograr cierta movilidad limitada dentro de zonas de controladores de acceso; H.323 en general y 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 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.	CE 16

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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	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.	CE 9
J.112	Sistemas de transmisión para servicios interactivos de televisión por cable	En muchos países se han implantado los servicios de televisión digital y se reconocen los beneficios de ampliarlos a la prestación de servicios interactivos. Los sistemas de distribución de televisión por cable están especialmente adaptados a la aplicación de servicios de datos bidireccionales. Esta Recomendación complementa y amplía el alcance de J.83, "Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable", para la prestación de datos bidireccionales por cables coaxiales e híbridos fibra-coaxial para servicios interactivos. También contiene diversos anexos para los distintos entornos de medios existentes. Se recomienda utilizar estos sistemas para la introducción de un acceso rápido a Internet y/o servicios de televisión por cable interactivos, para aprovechar las ventajas de las economías de escala y facilitar la interoperabilidad. Se establecen requisitos de seguridad, la utilización del sistema de seguridad de datos por cable SP-DOCSS (DOCSS), la especificación del módulo de seguridad extraíble (SP-RSM) y la especificación de seguridad de datos por cable básico (SP-BDS).	CE 9
J.160	Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable	En esta Recomendación se establece un marco de arquitectura que permite a los operadores de televisión por cable proporcionar servicios dependientes del tiempo en sus redes mejoradas para soportar los módems de cable. Los servicios de seguridad disponibles a través de la capa de servicio básica IPCablecom son la autenticación, el control de acceso, la integridad, la confidencialidad y el no repudio. Una interfaz de protocolo IPCablecom puede emplear uno o más de estos servicios, o ninguno, para cumplir con sus requisitos de seguridad particulares. La seguridad IPCablecom cumple los requisitos de seguridad de cada interfaz de protocolo mediante: • identificación del modelo de amenaza específico a cada interfaz de protocolo; • identificación de los servicios de seguridad (autenticación, autorización, confidencialidad, integridad y no repudio) necesarios para contrarrestar las amenazas identificadas; • especificación de un mecanismo de seguridad concreto adaptado a los servicios de seguridad requeridos. Los mecanismos de seguridad incluyen tanto el protocolo de seguridad (por ejemplo, IPsec, seguridad de capa RTP y seguridad de SNMPv3) y el protocolo de gestión de claves correspondiente (por ejemplo, IKE, PKINIT/Kerberos).	CE 9
J.170	Especificación de la seguridad de IPCablecom	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

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
J.191	Lote de características basadas en el protocolo Internet para mejorar los módems de cable	Esta Recomendación especifica un conjunto de características IP que pueden añadirse a los módems de cable de manera que los operadores de cable puedan proporcionar servicios adicionales mejorados a sus clientes: calidad de servicio IPCablecom, seguridad mejorada, características de gestión y configuración adicionales y un mejor direccionamiento y tratamiento de paquetes. Estas características IP residen en el servicio Portal de elemento lógico (PS o sólo Portal). Un módem de cable que contiene estas características mejoradas es un "módem de cable adaptado a IP" (IPCM) y constituye la implementación de una clase de dispositivo HA J.190. Como se describe en la Rec. UIT-T J.190, la clase de dispositivo HA incluye tanto la funcionalidad de módem de cable como la funcionalidad de servicios Portal. En el capítulo 11, Seguridad, se definen las interfaces, protocolos y requisitos funcionales de seguridad necesarios para proporcionar servicios IP fiables por cable en un entorno seguro al PS. El objetivo de cualquier tecnología de seguridad es proteger el valor, sea una fuente de ingresos o un activo de información que tiene valor comercial. Estas fuentes de ingresos están amenazadas cuando cualquier usuario de una red percibe el valor, invierte en esfuerzo y dinero e inventa una técnica para evitar los pagos necesarios. Anexo C: Amenazas de seguridad y medidas preventivas.	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 secciones. Asimismo, se presenta un modelo de referencia lógico para la partición de la funcionalidad de gestión denominado arquitectura lógica por capas (LLA, *logical layered architecture*). 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.	CE 4
M.3016	Seguridad en el plano de gestión	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. NOTA – La Rec. UIT-T M.3016 se ha reestructurado en la siguiente manera: • M.3016.0 – Seguridad en el plano de gestión: Visión general • M.3016.1 – Seguridad en el plano de gestión: Requisitos de seguridad • M.3016.2 – Seguridad en el plano de gestión: Servicios de seguridad • M.3016.3 – Seguridad en el plano de gestión: Mecanismos de seguridad • M.3016.4 – Seguridad en el plano de gestión: Formulario de características	CE 4

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
M.3210.1	Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000)	Esta Recomendación pertenece a la serie de Recomendaciones 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). 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. Se basa en un conjunto de funciones identificadas en la Rec. UIT-T M.3400 y añade nuevos conjuntos, funciones y parámetros, nuevas expresiones de semántica y restricciones adicionales.	CE 4
M.3320	Marco de los requisitos de gestión para la interfaz X de la RGT	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. Incluye especificaciones de los requisitos de seguridad en la interfaz X de la RGT.	CE 4
M.3400	Funciones de gestión de la red de gestión de las telecomunicaciones	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 soporte 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. Incluye descripciones de la función de gestión de la seguridad que soporta la RGT.	CE 4
Q.293	Periodos en los que conviene tomar medidas de seguridad	Es un extracto del Libro Azul y contiene solamente las secciones 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, *protocol data unit*) del elemento de servicio de operaciones a distancia (ROSE, *remote operations service element*) 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. Esta Recomendación mejora la seguridad en la RGT introduciendo transformaciones de seguridad para las PDU ROSE y el intercambio de la información de seguridad conexa.	CE 4

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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 soporta *no repudio de origen y de recibo*, así como *integridad del mensaje* completo.	CE 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, *public key infrastructure*) 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 soporte 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* (M.3016). Sin embargo, la presente Recomendación no especifica si deben implementarse esas funciones, con o sin PKI.	CE 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 11
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 del acceso radioeléctrico del sistema de telecomunicaciones móviles universales	En esta Recomendación se incluyen referencias a las siguientes especificaciones de seguridad 3GPP: *TS 21.133:Amenazas y requisitos relativos a la seguridad, 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*	CE 19
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:Amenazas y requisitos relativos a la seguridad, TS 22.048: Mecanismos de seguridad para el juego de herramientas de aplicaciones (U)SIM, TS 22.101: Principios de servicio, TS 33.102: Arquitectura de seguridad, TS 33.103: Directrices de integración, TS 33.105: Requisitos de algoritmos criptográficos, TS 33.106: Requisitos de intercepción lícita, TS 33.107: 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: Especificación del conjunto de algoritmos MILENAGE*	CE 19

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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	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: Arquitectura de seguridad, TS 33.106: Requisitos de intercepción lícita, TS 33.107: Arquitectura y funciones de la intercepción lícita, TS 33.108: Interfaz de traspaso para la interceptación legal (LI), TS 33.200: Seguridad en el dominio de red; MAP, TS 33.203: Seguridad de acceso para servicios basados en IP, TS 33.210: Seguridad del dominio de red (NDS); Seguridad de la capa de red IP, TS 35.205, .206, .207, .208 y .909: Especificación del conjunto de algoritmos MILENAGE*	CE 19
Q.1742.1	Referencias 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 Recomendación 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 Rec. UIT-R M.1457. Las asociaciones para otros miembros de la familia IMT-2000 se identifican en la serie de Rec. 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.	CE 19
Q.1742.2	Referencias IMT-2000 (aprobadas el 11 de julio de 2002) a la red medular desarrollada ANSI-41 con red de acceso a cdma2000	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 Rec. 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 Rec. 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 Rec. UIT-R M.1457. Las asociaciones para otros miembros de la familia IMT-2000 se identifican en la serie de Recs. 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.	CE 19
Q.1742.3	Referencias IMT-2000 (aprobadas el 30 de junio de 2003) a la red medular desarrollada ANSI-41 con red de acceso a cdma2000	Especificaciones técnicas referenciadas en Q.1742.3 con aspectos de seguridad *Especificaciones entre sistemas:* N.S0003-0 – Módulo de identidad de usuario (Versión 1.0; abril de 2001) N.S0005-0 – Operaciones entre sistemas de radiocomunicaciones celulares (Versión 1.0; sin fecha) N.S0009-0 – IMSI (Versión 1.0; sin fecha) N.S0010-0 – Prestaciones avanzadas en sistemas de espectro ensanchado de banda ancha (Versión 1.0; sin fecha) N.S0011-0 – OTASP y OTAPA (Versión 1.0; sin fecha) N.S0014-0 – Mejoras de autenticación (Versión 1.0; sin fecha) N.S0018 – TIA/EIA-41-D Tasación preabonada (Versión 1.0.0; 14 de julio de 2000) N.S0028 – Interfuncionamiento de red entre la MAP GSM y la MAP ANSI-41 Rev. B Revisión: 0 (Versión 1.0.0; abril de 2002) *Especificaciones relativas a redes de datos en paquetes:* P.S0001-A – Norma de red IP inalámbrica (Versión 3.0.0; 16 de julio de 2001) P.S0001-B – Norma de red IP inalámbrica (Versión 1.0.0; 25 de octubre de 2002)	CE 19

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
		Especificaciones de aspectos de servicios y de sistemas: S.R0005-B – Modelo de referencia de red para sistemas de espectro ensanchado cdma2000 Revisión: B (Versión 1.0; 16 de abril de 2001) S.R0006 – Revisión de la descripción de características inalámbricas Revisión: 0 (Versión 1.0.0; 13 de diciembre de 1999) S.R0009-0 – Módulo de identidad de usuario (Etapa 1) Revisión: 0 (Versión 1.0; 13 de diciembre de 1999) S.R0018 – Tasación preabonada (Etapa 1) Revisión: 0 (Versión 1.0.0; 13 de diciembre de 1999) S.R0019 – Sistema de servicios basados en la posición (LBSS) Descripción de la Etapa 1 (Versión 1.0.0; 22 de septiembre de 2000) S.R0032 – Autenticación de abonado mejorada (ESA) y privacidad de abonado mejorada (ESP) (Versión 1.0; 6 de diciembre de 2000) S.R0037-0 – Modelo de arquitectura de la red IP para los sistemas de espectro ensanchado cdma2000 (Versión 2.0; 14 de mayo de 2002) S.R0048 – Identificador de equipo móvil 3G (MEID) (Versión 1.0; 10 de mayo de 2001) S.S0053 – Algoritmos criptográficos comunes (Versión 1.0; 21 de enero de 2002) S.S0054 – Especificación de interfaz para algoritmos criptográficos comunes (Versión 1.0; 21 de enero de 2002) S.S0055 – Algoritmos criptográficos mejorados (Versión 1.0; 21 de enero de 2002) S.R0058 – Requisitos del sistema del dominio multimedios IP (Versión 1.0; 17 de abril de 2003) S.R0059 – Dominio MS anterior – Requisitos del sistema, Etapa 1 (Versión 1.0; 16 de mayo de 2002) S.R0066-0 – Requisitos de la Etapa 1 de los servicios IP basados en la posición (Versión 1.0; 17 de abril de 2003) S.R0071 – Requisitos de vigilancia de los datos en paquetes del sistema anterior – Requisitos de la Etapa 1 (Versión 1.0; 18 de abril de 2002) S.R0072 – Requisitos de vigilancia de datos en paquetes exclusivamente IP – Requisitos de la Etapa 1 (Versión 1.0; 18 de abril de 2002) S.R0073 – Gestión de la configuración de dispositivos durante la comunicación Internet (Versión 1.0; IOTA) Etapa 1 (11 de julio de 2002) S.S0078-0 – Algoritmos de seguridad común (Versión 1.0; 12 de diciembre de 2002)	
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 *algoritmo 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.123 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 de claves* manual, X.274/ ISO TLSP y GSS-API.	CE 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

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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 entre la aplicación local (LA, *local application*) y aplicación de comunicación (CA, *communication application*). 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 16
X.217	Tecnología de la información – Interconexión de sistemas abiertos – Definición de servicios para el elemento de servicio de control de asociación	En esta Recomendación se especifica el control de asociaciones de aplicación en entornos de interconexión de sistemas abiertos (OSI) mediante un elemento de servicio de control de asociación (ACSE, *association control service element*). 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*. La enmienda 1 proporciona el soporte del mecanismo de autenticación para el modo sin conexión.	CE 17
X.227	Tecnología de la información – Interconexión de sistemas abiertos – Protocolo con conexión para el elemento de servicio de control y 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".	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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.	CE 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 especifican las condiciones de conformidad de la implementación de protocolo (PICS, *protocol implementation conformance statement*). Para el caso del protocolo sin conexión en un entorno de interconexión de sistemas abiertos (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.	CE 17
X.272	Compresión y privacidad de datos por redes de transmisión 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 en 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. Se especifican mecanismos de compresión y privacidad de datos en conexiones virtuales permanentes (PVC, *permanent virtual connections*) y conexiones virtuales conmutadas (SVC, *switched virtual connections*).	CE 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 soporta 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 soporta estos servicios mediante el empleo de *mecanismos criptográficos*, *etiquetas de seguridad* y *atributos de seguridad asignados*, tales como *claves criptográficas*.	CE 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*.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.400/ F.400	Visión de conjunto del sistema y del servicio de tratamiento de mensajes	Esta Recomendación define los elementos de servicios de seguridad del sistema de tratamiento de mensajes (MHS, *message handling system*) para 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).	CE 17
X.402	Tecnología de la información – Sistema 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.	CE 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 que soportan 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 *técnicas de criptografía simétricas*.	CE 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 soportar 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).	CE 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 que garantizan la seguridad de acceso de entidades MHS y usuarios distantes, mediante los servicios de *autenticación* y *control de acceso*, en lo que concierne a la capa de aplicación.	CE 17
X.420	Tecnología 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.	CE 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.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.440	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.	CE 17
X.500	Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Visión de conjunto de conceptos, modelos y servicios	Esta Recomendación, junto con otras, se ha elaborado para facilitar la interconexión de los sistemas de procesamiento de la información que proporcionan servicios de directorio. El conjunto de estos sistemas y la información de directorio que contienen puede considerarse como un todo, denominado directorio. La información que contiene el directorio conocido como la base de información del directorio (DIB, *directory information base*) se utiliza normalmente para facilitar la comunicación entre, con o sobre objetos: entidades de aplicación, personas, terminales y listas de distribución. El directorio desempeña una función significativa en la interconexión de sistemas abiertos, cuyo objetivo es permitir, con un mínimo de acuerdo técnico fuera de las normas de interconexión, la interconexión de los sistemas de procesamiento de la información. Esta Recomendación presenta los conceptos de directorio y de la DIB, con modelos, y describe someramente los servicios y capacidades de estos conceptos. Otras Recomendaciones utilizan estos modelos para definir el servicio abstracto proporcionado por el directorio y para especificar los protocolos que permiten obtener o difundir este servicio. En esta Recomendación se especifican el directorio y sus características de seguridad.	CE 17
X.501	Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos	En esta Recomendación se presenta una serie de modelos para el directorio como marco para otras Recomendaciones UIT-T de la serie X.500: modelo (funcional) general, modelo de autoridad administrativa, modelos de información de directorio genéricos que permiten conocer la información del directorio desde el punto de vista del usuario del directorio y del usuario administrativo, el agente del sistema de directorio genérico (DSA, *directory system agent*) y los modelos de información DSA y el marco operativo y de seguridad. En esta Recomendación se especifica la utilización del certificado de atributo y la clave pública X.509 en el directorio.	CE 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 para certificados de claves públicas y atributos (edición de 2000, cuarta edición/versión) – Marcos para certificados de claves públicas y atributos (edición de 2005, quinta 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, *privilege management infrastructures*). 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.	CE 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 formas seguras de acceso durante la vinculación de entidades de directorio.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.680	Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de la notación básica	Esta Recomendación especifica la norma de notación denominada notación de sintaxis abstracta uno (ASN.1, *asbract syntax notation one*) para la definición de las sintaxis de datos. Se definen varios tipos de datos simples y se especifica una notación para la referenciación de estos tipos y la especificación de los valores de estos tipos. La notación ASN.1 puede aplicarse siempre que sea necesario para definir la sintaxis abstracta de la información sin limitar de manera alguna la codificación de la información para la transmisión. ASN.1 se utiliza para definir tipos de datos, valores y restricciones de tipos de datos, es decir, define un número de tipos simples, con sus etiquetas, y especifica una notación para la referenciación de estos tipos y la especificación de los valores de estos tipos; se definen mecanismos para la construcción de nuevos tipos a partir de tipos más básicos y se especifica una notación para la definición de estos tipos y la asignación de etiquetas y la especificación de sus valores; se define un conjunto de caracteres (por referencia a otras Recomendaciones) para su utilización dentro de ASN.1. Un tipo de datos (o tipo) es una categoría de información (por ejemplo, numérica, textual, de imagen fija o de vídeo). Un valor de datos (o valor) es un ejemplar de un tipo. La presente Recomendación define diversos tipos básicos y sus correspondientes valores, y normas para su combinación en tipos y valores más complejos. En algunas arquitecturas de protocolo, cada mensaje se especifica como un valor binario de una secuencia de octetos. No obstante, los normalizadores necesitan definir tipos de datos bastante complejos para transportar sus mensajes sin preocuparse de su representación binaria. Para especificar estos tipos de datos se requiere una notación que no determina necesariamente a la representación de cada valor. Esta notación es ASN.1. La completa una especificación de uno o más algoritmos denominados normas de codificación que determinan el valor de los octetos que transportan la semántica de aplicación (denominada sintaxis de transferencia). NOTA – Las series de Recomendaciones sobre ASN.1 (y en concreto las normas de codificación de ASN.1 distinguidas y canónicas) se han utilizado ampliamente en muchas normas relacionadas con la seguridad y otras Recomendaciones. En concreto, H.323 y las series X.400 y X.500 dependen en gran medida de ASN.1. Estas Recomendaciones han constituido, y siguen constituyendo los principales elementos utilizados en la labor relativa a la seguridad.	CE 17
X.681	Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de objetos de información	En esta Recomendación se presenta la notación ASN.1 que permite definir y dar nombres de referencia a las clases de objetos de información así como a los objetos de información individuales y sus conjuntos, es decir, presenta la notación para especificar las clases de objetos de información, los objetos de información y los conjuntos de objetos de información. Una clase de objetos de información constituye un cuadro conceptual (un conjunto de objetos de información) con una columna para cada campo de la clase de objeto de información y en el que cada fila define un objeto de información. Los diseñadores de aplicaciones con frecuencia necesitan diseñar un protocolo que funcione con cualquier número de instancias de una determinada clase de objetos de información, sabiendo que estas instancias las pueden definir otros organismos y que pueden aparecer nuevas instancias con el tiempo. Ejemplos de estas clases de objetos de información son las "operaciones" del servicio de operaciones remoto (ROS, *remote operations service*) y los "atributos" del directorio OSI. Esta Recomendación especifica una notación que permite definir y dar nombres de referencia a las clases de objetos de información así como a los objetos de información individuales y sus conjuntos. Véase la nota *supra* (X.680).	CE 17
X.682	Tecnología de la información – Notación de sintaxis abstracta uno: Especificación de constricciones	Esta Recomendación forma parte de la notación de sintaxis abstracta uno (ASN.1) y especifica una notación para especificar las restricciones (del usuario, tabla y de contenido). Presenta la notación ASN.1 para el caso general de especificación de restricciones y excepciones que limitan los valores de datos de un tipo de datos estructurado. Esta notación también se utiliza para señalización de violaciones. Los diseñadores de aplicaciones necesitan una notación que defina un tipo de dato estructurado para transportar su semántica y para restringir los valores que puedan aparecer. Por ejemplo, restringir la gama de algunos componentes o utilizar un conjunto de objetos de información específico para restringir un componente "ObjectClassFieldType" o la utilización "AtNotation" para especificar la relación entre componentes. Véase la nota *supra* (X.680).	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.683	Tecnología de la información – Notación de sintaxis abstracta uno: Parametrización de especificaciones de notación de sintaxis abstracta uno	Esta Recomendación forma parte de la notación de sintaxis abstracta uno (ASN.1) y define la notación para la parametrización de las especificaciones ASN.1, es decir, para los nombres de referencia y las asignaciones a los tipos de datos, que son de utilidad para los diseñadores al escribir especificaciones, cuando algunos aspectos se dejan sin definir en determinadas etapas del desarrollo para completarlos más adelante y obtener una definición completa de una sintaxis abstracta. Los diseñadores de aplicaciones han de escribir especificaciones en las cuales algunos aspectos se dejan sin definir. Estos aspectos los definirán más adelante uno o más grupos (cada uno según le convenga) para obtener una especificación plenamente definida que pueda utilizarse en la definición de una sintaxis abstracta (una para cada grupo). En algunos casos, pueden quedar sin definir algunos aspectos de especificación (por ejemplo, límites), incluso en el momento de definir la sintaxis abstracta. Se completará mediante especificación de perfiles normalizados internacionales o perfiles funcionales procedentes de otro organismo. Véase la Nota *supra* (X.680).	CE 17
X.690	Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida	En esta Recomendación se especifica un conjunto de reglas de codificación básicas (BER, *basic encoding rules*) que pueden aplicarse a los valores de tipos definidos utilizando la notación ASN.1, es decir, para especificar una sintaxis de transferencia para valores de tipos definidos utilizando la notación especificada en la serie de Recs. UIT-T X.680, que se denominan notación de sintaxis abstracta uno o ASN.1. La aplicación de estas reglas de codificación produce una sintaxis de transferencia para estos valores. Está implícito en la especificación que estas reglas de codificación también se utilizan para la decodificación, es decir, para decodificar la sintaxis de transferencia a fin de identificar los valores de datos que se han transferido. También se especifica un conjunto de reglas de codificación canónicas y distinguidas que restringen la codificación de los valores a sólo una de las alternativas que ofrecen las reglas de codificación básicas: un conjunto de reglas de codificación distinguida (DER, *distinguished encoding rules*) y un conjunto de reglas de codificación canónica (CER, *canonical encoding rules*) que limitan las reglas de codificación básicas (BER). La principal diferencia entre ellas es que la DER utiliza una longitud definida para la codificación mientras que CER utiliza una longitud indefinida. Las reglas DER se adaptan mejor a los valores de codificación pequeños, mientras que las reglas CER son más apropiadas para valores grandes. Está implícito en la especificación que estas reglas de codificación también se utilizan para la decodificación. Véase la Nota *supra* (X.680).	CE 17
X.691	Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de la reglas de codificación compactada	En la serie de Recs. UIT-T X.680 se describe la notación de sintaxis abstracta uno (ASN.1), una notación para la definición de mensajes que van a intercambiar las aplicaciones pares. Esta Recomendación describe un conjunto de reglas de codificación que puede aplicarse a los valores de todos los tipos ASN.1 para obtener una representación mucho más compacta que la que se puede lograr con las reglas de codificación básica y sus derivados (descritas en X.690). Se especifica un conjunto de reglas de codificación compactada que pueden utilizarse para escribir una sintaxis de transferencia de los valores de los tipos definidos en la Rec. UIT T X.680. Las reglas de codificación compactada también se aplican para la decodificación de esta sintaxis de transferencia con el objetivo de identificar los valores de datos que se han transferido. Hay varias reglas de codificación que pueden aplicarse a los valores de los tipos ASN.1. Estas reglas de codificación compactada (PER, *packed encoding rules*) se denominan así porque se logra una representación mucho más compacta de la que puede lograrse con las reglas de codificación básica (BER) y sus derivados descritos en la Rec. UIT T X.690. Véase la nota *supra* (X.680).	CE 17
X.692	Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de la notación de control de codificación + anexo E: Soporte de la codificación Huffman	En esta Recomendación se define la notación de control de codificación (ECN, *encoding central notation*) utilizada para especificar las codificaciones de los tipos ASN.1 o de partes de los tipos que son distintas de las que se consiguen con las reglas de codificación normalizadas, como las reglas de codificación básica (BER) y las reglas de codificación compactada (PER). Se presentan diversos mecanismos para esta especificación, así como los medios para vincular la especificación de las codificaciones a las definiciones de los tipos a que se aplican. La ECN puede utilizarse para codificar todos los tipos de una especificación ASN.1, pero también con las normas de codificación normalizadas, como BER o PER, para especificar únicamente la codificación de los tipos que tienen requisitos especiales. Un tipo ASN.1 especifica un conjunto de valores abstractos. Las reglas de codificación especifican la representación de estos valores abstractos como una serie de bits. Véase la Nota *supra* (X.680).	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.693	Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Reglas de codificación de lenguaje de marcaje extensible	La notación de sintaxis abstracta uno (ASN.1) es la que se utiliza generalmente para la definición de mensajes que han de intercambiar aplicaciones pares. Esta Recomendación especifica las reglas de codificación que pueden aplicarse a los valores codificados de tipo ASN.1 utilizando el lenguaje de marcaje extensible (XML, *extensible markup language*): un conjunto de reglas de codificación XML básicas (XER, *XML encoding rules*) que puede utilizarse para escribir una sintaxis de transferencia para los valores de tipos definidos en la serie de Recs. UIT-T X.680. Esta Recomendación especifica un conjunto de reglas de codificación XML canónicas que restringe las reglas de codificación XML básicas y produce una codificación única para cada valor ASN.1. Está implícito en la especificación que estas reglas de codificación también se utilizan para la decodificación. Hay varios conjuntos de reglas de codificación que pueden aplicarse a los valores de los tipos ASN.1. En esta Recomendación se definen dos conjuntos de reglas de codificación que utilizan el lenguaje de marcaje extensible (XML): son las reglas de codificación XML (XER) para ASN.1 y ambas producen un documento XML conforme a la norma W3C XML 1.0. El primer conjunto son las denominadas reglas de codificación XML básicas. El segundo conjunto se denomina reglas de codificación XML canónicas, porque sólo hay una manera de codificar un valor ASN.1 utilizando estas reglas de codificación (las reglas de codificación canónicas se utilizan generalmente para aplicaciones con características de seguridad, como las firmas digitales).	CE 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.	CE 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.	CE 4
X.736	Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad	Define 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. Está situada en la capa de aplicación. 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.	CE 4
X.740	Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pista de auditoría de seguridad	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. Está posicionada en la capa de aplicación.	CE 4

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.741	Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso	Contiene las especificaciones para el control de acceso para aplicaciones que utilizan servicios de gestión y protocolos OSI. La información de control de acceso identificada por esta Recomendación puede utilizarse para planes basados en listas de control de acceso, en capacidades, en etiquetas de seguridad y en restricciones de contexto.	CE 4
X.790	Función de gestión de dificultades para aplicaciones del UIT-T	Esta Recomendación trata de la gestión de los disfuncionamientos en sistemas y redes de comunicaciones desde la perspectiva del proveedor de servicio y del usuario del mismo servicio. Las disfunciones ("dificultades") son problemas que afectan negativamente a la calidad de servicio que perciben los usuarios de la red. Cuando se detecta una dificultad, posiblemente como resultado de un informe de alarma, el usuario puede enviar un informe de dificultades o el sistema generarlo automáticamente. La gestión de un informe de dificultades es necesaria para garantizar que esta dificultad recibe la atención que merece y que se elimina para restablecer el servicio en su anterior nivel de capacidad. Se define un formato de informes de dificultades por parte del usuario, que el proveedor utilizará para resolver el problema. Durante la fase de resolución por parte del proveedor de servicios, el usuario puede enviar una petición para saber si está o no resuelto. Una vez solucionado el problema, el proveedor puede notificarlo al usuario. Se incluyen tipos concretos de dificultades y mecanismos para definir otros, puesto que la utilización de esta Recomendación por parte de una aplicación en concreto puede requerir tipos específicos de dificultades. En el momento en que aparece el problema, la red puede estar interfuncionando con otra red para proporcionar un servicio y el problema de disfuncionamiento puede provenir de esa otra red, por lo que puede ser necesario intercambiar información de gestión de dificultades entre los sistemas de gestión a través de interfaces, entre el cliente y el proveedor de servicios, o entre dos proveedores de servicios. Estas interfaces pueden representar fronteras interjurisdiccionales o intrajurisdiccionales. Además de intercambiar información sobre la dificultad detectada, también es posible que sea necesario intercambiar información sobre la inaccesibilidad del servicio. Probablemente un proveedor de servicios deberá informar a los clientes de la futura inaccesibilidad del servicio (por mantenimiento planificado, por ejemplo). En el alcance de esta Recomendación se incluyen todos los procesos expuestos para el intercambio de información de gestión.	CE 4
X.800	Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT	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.	CE 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.	CE 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).	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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.	CE 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.	CE 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*.	CE 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*.	CE 17
X.813	Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad en sistemas abiertos: Marco de no rechazo	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*.	CE 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.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.815	Tecnología de la información – Interconexión de sistemas abierto – 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.	CE 17
X.816	Tecnología de la información – Interconexión de sistemas abierto – 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.	CE 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 soportan 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 soportar la especificación de requisitos de protección selectiva de los campos en una especificación de sintaxis abstracta y para soportar 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.	CE 17
X.831	Tecnología de la información – Interconexión de sistemas abiertos – Seguridad genérica de las capas superiores: Definición del servicio basado en el elemento 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 soportan la prestación de servicios de seguridad. Se define el servicio proporcionado por el elemento de servicio de intercambio de seguridad (SESE, *security exchange service element*), 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.	CE 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 soportan la prestación de servicios de seguridad. Esta Recomendación *especifica 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 soportar la prestación de *servicios de seguridad* dentro de la capa de aplicación de OSI.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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 soportan la prestación de servicios de seguridad. En esta Recomendación 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.	CE 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, *protocol implementation conformance statement*) 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 la Rec. UIT-T X.830. En el anexo C se presentan las capacidades y opciones normalizadas de una manera que permite evaluar la conformidad de una implementación determinada.	CE 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). 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 describe las capacidades y opciones normalizadas de una manera que permite evaluar la conformidad de una implementación determinada.	CE 17
X.841	Tecnología de la información – Técnicas de seguridad – Objetos de información de seguridad para control de acceso	Esta Recomendación contiene definiciones de objetos habitualmente necesarias en las normas de seguridad para evitar la existencia de múltiples definiciones diferentes de la misma funcionalidad. La precisión de estas definiciones se logran utilizando la rotación de sintasis abstracta uno (ASN.1). Esta Recomendación trata solamente los aspectos estáticos de los objetos de información de seguridad (SIO, *security information objects)*.	CE 17
X.842	Tecnología de la información – Técnicas de seguridad – Directrices sobre el uso y gestión de servicios a tercera parte confiable	En esta Recomendación se proporcionan una orientación para el uso y gestión de los servicios de tercera parte confiable (TTP, *trusted third party*), 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 hora*, el *no repudio*, la *gestión de claves*, la *gestión de certificados* y la *notaría pública electrónica*.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
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 que impiden 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*.	CE 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 y determina una arquitectura de distribución, interfuncionamiento y portabilidad integrada. 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, los escritores de normas y arquitectos de sistemas ODP. Contiene también una agrupación en categorías de las áreas de normalización requeridas, según los puntos de referencia para conformidad identificados en la Rec. UIT-T X.903. Los sistemas ODP han de ser seguros, es decir, la construcción y el mantenimiento deben garantizar 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*.	CE 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. El nivel de detalle de la especificación se limita a lo que es necesario para determinar qué *nuevas técnicas de especificación habrá que utilizar*.	CE 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. Son las restricciones aplicables a las normas de procesamiento distribuido abierto (ODP). Se emplean las técnicas descriptivas de la Rec. UIT-T X.902.	CE 17
X.904	Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia: Semántica arquitectural	Esta Recomendación contiene una normalización de los conceptos de modelado del ODP definidos en las secciones 8 y 9 de la Rec. UIT-T X.902. La normalización consiste en interpretar cada concepto según los elementos constitutivos de las diferentes técnicas de descripción formal normalizada.	CE 17

N.º	TÍTULO	OBJETIVO PRINCIPAL Y ASPECTOS DE SEGURIDAD	Comisión de Estudio
X.1051	Sistemas de gestión de seguridad de la información – Requisitos para telecomunicaciones	Para las organizaciones de telecomunicaciones, la información y los procesos conexos, las instalaciones de telecomunicaciones, redes y líneas son activos comerciales importantes. Para que estas organizaciones puedan gestionar adecuadamente estos activos y proseguir sus actividades de manera correcta y satisfactoria, es fundamental una gestión en la seguridad de la información. Esta Recomendación expone los requisitos de gestión de seguridad de la información para las organizaciones de telecomunicaciones. En esta Recomendación se especifican los requisitos para establecer, implementar, explotar, supervisar, revisar, mantener y mejorar un sistema de gestión de seguridad de la información (ISMS) documentado en el contexto de los riesgos comerciales generales de las telecomunicaciones. Se especifican los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de las telecomunicaciones individuales o partes de las mismas.	CE 17
X.1081	El modelo telebiométrico multimodal – Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad	Esta Recomendación define un modelo telebiométrico multimodal que establece el marco común para la especificación de cuatro cuestiones de seguridad interconectadas: privacidad, autenticación, seguridad y seguridad personal. Este modelo telebiométrico multimodal cubre todas las posibilidades de interacción hombre-máquina multimodales seguras y está parcialmente basado en las normas ISO 31 y CEI 60027-1. En el campo de las telecomunicaciones también son relevantes los aspectos cognitivos, perceptuales y comportamentales del ser humano, que probablemente serán utilizados por un sensor o lector biométrico en el futuro con fines de autenticación. Estos aspectos se han incluido en el modelo telebiométrico multimodal. La Recomendación presenta una taxonomía de las interacciones que tienen lugar en la capa multimodal del cuerpo humano con dispositivos electrónicos, fotónicos, químicos o materiales que capturan parámetros biométricos o que producen algún efecto en el cuerpo. La autenticación del ser humano, preservando su privacidad y seguridad, puede especificarse en términos de interacción entre los dispositivos y la esfera de la privacidad personal, que modeliza y encapsula las interacciones del ser humano con su entorno, con descripciones explícitas y modificables. Esta Recomendación incluye la especificación de la esfera de la privacidad personal, una indicación de categorías de modalidades de interacción en esta esfera, las unidades básicas y derivadas para la medición y especificación (de manera cuantitativa) de estas interacciones y una escala jerárquica de proximidad relativa.	CE 17
X.1121	Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo	Esta Recomendación describe las amenazas de seguridad para la comunicación de datos móviles de extremo a extremo y los requisitos de seguridad para los usuarios móviles y los proveedores de servicios de aplicación (ASP) en la capa superior del modelo de referencia OSI para comunicaciones de datos móviles de extremo a extremo entre un terminal móvil en una red móvil y un servidor de aplicación en una red abierta. Además, muestra la ubicación de las tecnologías de seguridad que desempeñan determinadas funciones en el modelo de comunicaciones de datos móviles de extremo a extremo. Se establece un marco de tecnologías de seguridad para las comunicaciones de datos móviles de extremo a extremo.	CE 17
X.1122	Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas	La infraestructura de claves públicas (PKI) es una tecnología de seguridad que se aplica a la relación entre un terminal móvil y un servidor de aplicación en el modelo general de comunicaciones de datos móviles de extremo a extremo entre un usuario móvil y un ASP, o a la relación entre un terminal móvil y una pasarela de seguridad móvil y entre la pasarela de seguridad móvil y un servidor en el modelo de pasarela de las comunicaciones de datos móviles de extremo a extremo entre un usuario móvil y un ASP. Aunque la tecnología PKI resulta muy útil para proteger las comunicaciones de datos móviles de extremo a extremo, algunas características específicas a este tipo de comunicaciones pueden requerir una adaptación de la tecnología PKI al crear sistemas móviles seguros (cifrado, firmas digitales, integridad de datos, etc.). Dado que no se han establecido métodos para construir y gestionar sistemas móviles seguros con la tecnología PKI, esta Recomendación ofrece directrices para la construcción de sistemas móviles seguros utilizando esta tecnología.	CE 17

Anexo B

Terminología relativa a la seguridad

Las siguientes definiciones y abreviaturas relacionadas con la seguridad en el marco de los trabajos del UIT-T se han extraído de las Recomendaciones UIT-T pertinentes.

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. Existe igualmente una versión en CD-ROM que se actualiza regularmente. Todos los términos y definiciones citados en esta sección se pueden encontrar en SANCHO junto con la lista de Recomendaciones del UIT-T donde se los define.

La CE 17 del UIT-T publicó 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/tel-security.html.

B.1 Lista de términos y definiciones relacionados con la seguridad

A continuación se incluye una lista de los términos relativos a la seguridad más comúnmente utilizados que se definen en las Recomendaciones del UIT-T en vigor. En el compendio elaborado por la Comisión de Estudio 17 figura una lista más completa de definiciones en materia de seguridad (véase el enlace arriba).

Término	Definición	Referencia
control de acceso	1. Prevención del uso no autorizado de un recurso, incluida la prevención del uso de un recurso de una manera no autorizada. 2. 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.800 J.170
lista de control de acceso	Lista de entidades, con sus derechos de acceso, que están autorizadas a tener acceso a un recurso.	X.800
política de control de acceso	Conjunto de normas que definen las condiciones de acceso.	X.812
servicio de control de acceso	El servicio de control de acceso proporciona los medios necesarios para acceder a los recursos únicamente a las personas autorizadas. Dichos recursos pueden ser, entre otros, el sistema físico, los programas informáticos del sistema, las aplicaciones y los datos. El servicio de control de acceso puede definirse y aplicarse a distintas escalas en la RGT: personas, objetos o atributos. Las limitaciones de acceso se especifican en la información de control de acceso: los medios que determinan las entidades autorizadas y el tipo de acceso permitido (lectura, escritura, modificación, creación, supresión).	M.3016.2
amenazas fortuitas	Las amenazas que existen sin intención premeditada. Entre otras amenazas fortuitas cabe señalar las disfunciones del sistema, los errores operativos y los problemas que plantean los programas informáticos.	X.800
imputabilidad	Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.	X.800
amenaza activa	Amenaza de una alteración deliberada y no autorizada de la información que figura en el sistema, o del estado del sistema. *Nota* – Ejemplos de amenazas activas relativas a la seguridad: la modificación de mensajes, la reproducción de mensajes, la inserción de mensajes espurios, la usurpación de identidad (o impostura) de una entidad autorizada, la de negación de servicio, la modificación malintencionada de los cuadros de encaminamiento de un sistema por un usuario no autorizado.	X.800
árbitro	Entidad que arbitra conflictos que puedan surgir como resultado de eventos o acciones de repudio, es decir, la entidad que evalúa las pruebas y determina si ha ocurrido la acción o el evento dudosos. El *fallo* sólo será eficaz si las partes en conflicto aceptan la *autoridad* del árbitro.	X.813
algoritmo	Proceso matemático que puede utilizarse para criptar y descriptar flujos de datos.	J.93
método de autenticación asimétrica	Método de autenticación en el que las dos entidades no comparten toda la información de autenticación.	X.811

algoritmo criptográfico asimétrico	Algoritmo para ejecutar el cifrado o el correspondiente descifrado con claves diferentes en cada caso. *Nota* – Con algunos algoritmos criptográficos asimétricos, el descifrado del texto o la generación de una firma digital requieren la utilización de más de una clave privada.	X.810
ataque	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.	H.235
atributo	En el contexto de la gestión de mensajes, un elemento de información, un componente de una lista de usuarios o de distribución. Permite la ubicación por referencia a la estructura física u organizativa del sistema de gestión de mensajes (o la red conexa).	X.400
autoridad de atributo	1. Autoridad que asigna privilegios expidiendo certificados de atributo. 2. Entidad en la que depositan su confianza una o más entidades para crear y firmar certificados de atributo. *Nota* – Una CA también puede ser una AA.	X.509 X.842
certificado de atributo	Estructura de datos, firmada digitalmente por una autoridad de atributo, que vincula algunos valores de atributo con información de identificación de su titular.	X.509
tipo de atributo	Identificador que indica una clase de información (por ejemplo, nombres personales). Forma parte de un atributo.	X.400
valor de atributo	Ejemplar de la clase de información designada por un tipo de atributo (por ejemplo, un determinado nombre personal). Forma parte de un atributo.	X.400
auditoría	Véase auditoría de seguridad.	X.800
registro de auditoría	Véase registro de auditoría de seguridad.	X.800
identidad autenticada	El identificador diferenciador de una entidad principal que se ha verificado en el proceso de autenticación.	X.811
autenticación	1. El proceso de verificación de una identidad. *Nota* – Véase entidad principal y verificador y las dos formas de autenticación distintas (autenticación de origen de datos y autenticación de entidad). La autenticación puede ser unilateral o mutua. La autenticación unilateral garantiza la identidad de una sola entidad principal. La autenticación mutua garantiza las identidades de ambas entidades principales. 2. Confirmación de la identidad con que se presenta una entidad. 3. Véase autenticación del origen de datos y autenticación de entidad par. El término autenticación no se emplea en relación con la integridad de los datos; para ello se emplea el término integridad de datos. 4. La confirmación de la identidad de objetos cuando se va a crear una asociación. Por ejemplo, las AE, AP, y los usuarios humanos de aplicaciones. *Nota* – Este término se ha definido así para establecer que se trata de un marco de autenticación más amplio que la autenticación de entidades pares de la Rec. CCITT X.800. 5. Proceso de verificación de la identidad que presenta de una entidad ante otra entidad. 6. Proceso destinado a permitir al sistema asegurar la identificación de una parte.	X.811 X.811 X.800 X.217 J.170 J.93

certificado de autenticación	Certificado de seguridad garantizado por una autoridad de autenticación, que puede usarse para garantizar la identidad de una entidad.	X.811
intercambio de autenticación	1. Mecanismo destinado a garantizar la identidad de una entidad mediante intercambio de información. 2. Secuencia de una o más transferencias de información de autenticación para autenticar algo.	X.800 X.811
servicio de autenticación	El servicio de autenticación aporta las pruebas de que la identidad de un objeto o sujeto es la que ha presentado. En función del tipo de parte y del fin de la identificación, pueden solicitarse los siguientes tipos de autenticación: autenticación de usuario, autenticación de entidad par, autenticación de origen de datos. Entre otros mecanismos, la autenticación se realiza mediante contraseñas, números de identificación personal (PIN, *personal identification numbers*) (autenticación simple) y métodos criptográficos (autenticación de mayor seguridad).	M.3016.2
testigo de autenticación	Información transportada durante un intercambio de autenticación robusta, que se puede utilizar para autenticar a quien la envió.	X.509
autenticidad	1. Se garantiza que determinada información no ha sido modificada o falsificada, y además que proviene de la entidad que se presenta como autor. 2. La fuente de datos presentada puede comprobarse a satisfacción del receptor.	J.170 T.411
autoridad	Entidad responsable de la expedición de certificados. Se definen dos tipos; la autoridad de certificación que expide certificados de clave pública y la autoridad de atributo que expide certificados de atributo.	X.509
certificado de autoridad	Certificado expedido a una autoridad (autoridad de certificación o autoridad de atributo).	X.509
autorización	1. Atribución de derechos, incluido el acceso basado en los correspondientes derechos. *Nota* – Esta definición implica la concesión de permisos para realizar determinadas actividades (por ejemplo, acceder a datos) y su relación con determinados procesos, entidades o agentes humanos. 2. Concesión de permisos sobre la base de identificación autenticada. 3. Concesión de acceso a un servicio o dispositivo cuando se tiene el permiso para utilizarlo.	X.800 H.235 J.170
disponibilidad	Propiedad de ser accesible y utilizable a petición por una entidad autorizada.	X.800
portal de seguridad por cable (CSP)	Elemento funcional que proporciona funciones de gestión y traducción de seguridad entre el HFC y la Base.	J.191
servidor de gestión de llamadas (CMS)	IPCablecom. Controla las conexiones de audio. También denominado Agente de Llamadas en la terminología MGCP/SGCP.	J.191
capacidad	Testigo utilizado como identificador de un recurso de modo que la posesión del testigo confiera derechos de acceso a ese recurso.	X.800
certificado	Conjunto de datos relativos a la seguridad emitidos por una autoridad de seguridad o un tercero de confianza, junto con información de seguridad que se utiliza para proporcionar los servicios de integridad y autenticación de origen de los datos (Recomendación UIT-T X.810). En la presente Recomendación el término se refiere a los 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.	H.235

política de certificado	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.	X.509
lista de revocación de certificados (CRL)	1. 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. 2. Lista que incluye los números de serie de los certificados revocados (por ejemplo, hay dudas sobre la seguridad de la clave o el sujeto ya no trabaja en la empresa) y cuyo periodo de validez aún no ha caducado.	X.509 Q.817
autoridad de certificación (CA)	1. 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. 2. 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.	X.509 X.810
trayecto de certificación	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.	X.509
código de puesta a prueba o comprobación	Parámetro de variante temporal generado por un verificador.	X.811
cifrado	1. Algoritmo criptográfico, una transformada matemática. 2. Algoritmo que transforma los datos entre el texto descifrado y el texto cifrado.	H.235 J.170
criptograma (o texto cifrado)	Datos producidos mediante cifrado. El contenido semántico de los datos resultantes no está disponible. *Nota* – Un criptograma puede someterse a cifrado a su vez para obtener un criptograma super cifrado.	X.800
declarante	La entidad *principal* o su representante para los fines de autenticación. El declarante tiene las funciones necesarias para llevar a cabo intercambios de autenticación en nombre de una entidad principal.	X.811
texto no cifrado	Datos inteligibles, cuyo contenido semántico está disponible.	X.800
pruebas comprometidas	Pruebas que en su día fueron satisfactorias, pero que ya no son consideradas fiables por las terceras partes fiables o los árbitros.	X.813
confidencialidad	Propiedad que garantiza que la información no se pone a disposición ni se divulga a personas, entidades o procesos no autorizados.	X.800
servicio de confidencialidad	Servicio que proporciona protección contra la divulgación no autorizada de datos intercambiados. Se distinguen los distintos tipos de servicios de confidencialidad siguientes: confidencialidad de campos selectiva; confidencialidad de conexión y confidencialidad del flujo de datos.	M.3016.2
integridad de contenidos	1. Permite al destinatario comprobar que no se ha modificado el contenido original del mensaje. 2. Este elemento de servicio permite al creador del mensaje proporcionar al destinatario un modo de comprobar que no se ha modificado el contenido del mensaje. La integridad del contenido se realiza para cada destinatario y puede utilizarse una técnica de criptación asimétrica o simétrica.	X.400 X.400

contra firma	Firma digital anexa a una unidad de datos que ya ha sido firmada por una entidad distinta (por ejemplo una tercera parte fiable).	X.813
credenciales	Datos que se transfieren para establecer la identidad alegada de una entidad.	X.800
criptoanálisis (o análisis criptográfico)	1. Análisis de un sistema criptográfico y/o sus entradas y salidas para deducir variables confidenciales y/o datos sensibles, incluido texto sin cifrar. 2. Proceso de recuperar el texto no cifrado de un mensaje o la clave de criptación, sin acceso a la clave. 3. Procedimiento que permite recuperar el texto no cifrado de un mensaje sin acceso a la clave (a la clave electrónica en los sistemas criptográficos electrónicos).	X.800 J.170 J.93
algoritmo criptográfico	Función matemática que calcula un resultado a partir de uno o varios valores de entrada.	H.235
encadenamiento criptográfico	Modo de utilización de un algoritmo criptográfico en el cual la transformación realizada por el algoritmo depende de los valores anteriores de entradas o salidas.	X.810
valor de comprobación criptográfico	Información que se obtiene realizando una transformación criptográfica (véase criptografía) sobre una unidad de datos. *Nota* – El valor de comprobación puede obtenerse en uno o más pasos y es el resultado de una función matemática de la clave y una unidad de datos. Suele utilizarse para verificar la integridad de una unidad de datos.	X.800
sistema criptográfico, criptosistema	1. Colección de transformaciones de texto no cifrado en texto cifrado 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. 2. Un criptosistema es simplemente un algoritmo capaz de convertir los datos de entrada en algo irreconocible (criptación) y volver a convertir los datos irreconocibles en su forma original (descriptación). Las técnicas de criptación RSA se describen en X.509.	X.509 Q.815
criptografía	Disciplina que abarca los principios, medios y métodos para la transformación de los datos con el fin de esconder su contenido de información, impedir su modificación no detectada y/o su uso no autorizado. *Nota* – La criptografía determina los métodos utilizados para cifrar y descifrar. El criptoanálisis es un ataque destinado a vencer los principios, medios y métodos criptográficos.	X.800
confidencialidad de datos	Este servicio se puede utilizar para impedir la divulgación no autorizada. El servicio de confidencialidad de datos está soportado por el marco de autenticación. Se puede utilizar para la protección contra la interceptación de datos.	X.509
integridad de los datos	Confirmación de que los datos no han sido modificados o destruidos por personas no autorizadas.	X.800
autenticación del origen de los datos	1. Confirmación de que la fuente de los datos recibidos es la alegada. 2. Confirmación de la identidad de la entidad principal, como responsable de una unidad de datos específica.	X.800 X.811
descifrado	Operación inversa al cifrado reversible correspondiente.	X.800
descriptación	Véase descifrado.	X.800
delegación	Cesión de un privilegio de una entidad a otra.	X.509
denegación de servicio	Prevención de acceso autorizado a los recursos o retardo deliberado de operaciones que tienen plazos críticos.	X.800

traducción de aleatorización	1. Restauración de las características de una señal de imagen/audio/datos a fin de permitir la recepción de forma clara. Esta restauración es un proceso específico bajo el control del sistema de acceso condicional (extremo receptor). 2. Inversión de la función de codificación aleatoria (véase "aleatorización") que permite obtener servicios utilizables de imágenes, sonido y datos.	J.96 J.93
huella dactilar digital	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.	X.810
firma digital	1. Datos añadidos a una unidad de datos, o transformación criptográfica (véase criptografía) de esta última que permite al destinatario comprobar la fuente y la integridad de la unidad de datos y proteger contra la falsificación (por ejemplo, por el destinatario). 2. Transformación criptográfica de una unidad de datos que permite al destinatario comprobar el origen y la integridad de la unidad de datos, y que protege al remitente y al destinatario de la unidad de datos contra la falsificación por parte de terceros, y al remitente contra la falsificación por parte del destinatario.	X.800 X.843
ataque directo	Ataque a un sistema basado en deficiencias existentes en los algoritmos, principios o propiedades subyacentes de un mecanismo de seguridad.	X.814
servicio de directorio	Servicio de búsqueda y recuperación de información de un catálogo de objetos bien definidos, que puede contener información sobre certificados, números de teléfono, condiciones de acceso, direcciones, etc. Cabe señalar el ejemplo de un servicio de directorio según X.500.	X.843
técnica de doble cobertura	Se puede dar protección adicional a un mensaje completo, incluidos parámetros de cobertura, especificando que el contenido del mensaje es, en sí mismo, un mensaje completo. Esta técnica de doble cobertura consiste en utilizar el argumento "tipo de contenido", que permite especificar que el contenido del mensaje es una cobertura interna.	X.402
escucha clandestina	Violación de la confidencialidad mediante la supervisión de las comunicaciones.	M.3016.0
clave electrónica	Señales de datos que se utilizan para controlar el proceso de lectura del código aleatorizado en los decodificadores del abonado. *Nota* – Existen al menos tres tipos de claves electrónicas: las que se utilizan para los trenes de señales de televisión, las que se utilizan para proteger las operaciones del sistema de control y las que se utilizan para la distribución de claves electrónicas en el sistema por cable.	J.93
cifrado	1. Transformación criptográfica de datos (véase criptografía) para producir un criptograma o texto encriptado. *Nota* – El cifrado puede ser irreversible, en cuyo caso no puede realizarse el proceso de descriptado correspondiente. 2. El cifrado (criptación) es el proceso que hace que los datos sean ilegibles para entidades no autorizadas aplicando un algoritmo criptográfico (un algoritmo de criptación). El descriptado es la operación inversa por la cual el texto cifrado se transforma en texto legible.	X.800 H.235
criptación	1. Método utilizado para traducir información en texto legible a texto cifrado (criptograma). 2. Proceso de aleatorización de señales con el fin de evitar el acceso no autorizado. (Véase también cifrado.)	J.170 J.93
entidad final	Sujeto del certificado que utiliza su clave privada para otros fines distintos que firmar certificados, o entidad que es una parte confiante.	X.509

cifrado de extremo a extremo	Cifrado de datos en el interior o en el sistema extremo fuente, cuando el descifrado correspondiente se produce sólo en el interior o en el sistema extremo de destino. (Véase también cifrado enlace por enlace.)	X.800
entidad	1. Ser humano, organización, elemento de equipos informáticos o un programa informático. 2. Cualquier cosa de interés concreta o abstracta. Si bien en general el término entidad puede emplearse para referirse a cualquier cosa, en el contexto de la modelización se utiliza para referirse a algo que forma parte del proceso modelizado.	X.842 X.902
autenticación de la entidad	Comprobación de la identidad de una entidad principal, en el contexto de una relación de una relación de comunicación. *Nota* – La identidad autenticada de la entidad principal está garantizada únicamente cuando se recurre a este servicio. La garantía de continuidad de la autenticación puede obtenerse mediante métodos que se describen en 5.2.7/X.811.	X.811
discriminador de eventos	Función que permite efectuar un análisis inicial de un evento relativo a la seguridad y, en su caso, genera una auditoría de seguridad y/o una alarma.	X.816
pruebas	Información que, ya sea por sí misma o utilizada conjuntamente con otra información, puede utilizarse para resolver un litigio. *Nota* – Son pruebas las firmas digitales, los sobres de seguridad y los testigos de seguridad. Las firmas digitales se utilizan con las técnicas de clave pública, mientras que los sobres y los testigos de seguridad se utilizan con las técnicas de claves secretas.	X.813
generador de pruebas	Entidad que genera pruebas para la función de no repudio. *Nota* – Puede tratarse del solicitante de servicios de no repudio, el originador, el destinatario o varias partes que colaboran entre sí (por ejemplo, un firmante o cofirmante).	X.813
falsificación	Una entidad fabrica información y alega que la recibió de otra entidad o la envió a otra entidad.	M.3016.0
función *hash* ("de troceo" o función de cálculo de clave)	Función (matemática) que refleja valores de un dominio grande (posiblemente muy grande) en una gama más pequeña.	X.810
esconder	Operación por la que se aplica protección de confidencialidad a datos no protegidos, o protección de confidencialidad adicional a datos ya protegidos.	X.814
política de seguridad basada en la identidad	Política de seguridad basada en las identidades y/o atributos de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios y de los recursos/objetos a que se accede.	X.800
ataque indirecto	Ataque a un sistema que no está basado en las deficiencias de un determinado mecanismo de seguridad (por ejemplo, ataques que evitan el mecanismo o que dependen en la utilización incorrecta del mecanismo por el sistema).	X.814
integridad	Propiedad de que los datos no han sido alterados de una manera no autorizada. (Véase también integridad de datos)	H.235
servicio de integridad	Este servicio proporciona los medios para garantizar la exactitud de los datos intercambiados, protegiéndolos contra la modificación, la supresión, la creación (inserción) y la reproducción. Se distinguen los siguientes tipos de servicios de integridad: integridad de campos selectiva, integridad de conexión sin recuperación, integridad de conexión con recuperación.	M.3016.2
canal con protección de integridad	Un canal de comunicaciones en el que se ha aplicado un servicio de integridad (véase integridad de conexión e integridad sin conexión).	X.815

datos con protección de integridad	Datos y demás atributos en el marco de un entorno con protección de integridad.	X.815
entorno con protección de la integridad	Entorno en el que se evitan o detectan alteraciones de datos no autorizadas (incluidas las creación y la supresión).	X.815
amenazas intencionadas	Amenazas que abarcan desde un examen somero mediante la utilización de instrumentos de control fácilmente disponibles, hasta ataques sofisticados mediante la aplicación de conocimientos especiales sobre el sistema. Las amenazas intencionadas efectivas son "ataques".	X.800
resistencia a la intrusión	Capacidad de un objeto informático de denegar el acceso (físico, eléctrico o por radiación) de partes no autorizadas a las funciones internas.	J.93
IPCablecom	Proyecto del UIT-T que incluye una arquitectura y varias Recomendaciones que permiten la prestación de servicios en tiempo real en redes de televisión por cable utilizando módems de cable.	J.160
Kerberos	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.	J.170
clave	1. Secuencia de símbolos que controla las operaciones de cifrado y descifrado. 2. Valor matemático introducido en el algoritmo criptográfico seleccionado.	X.800 J.170
servicio de distribución de claves	Servicio que distribuye claves de manera segura a entidades autorizadas a través de un centro de distribución de claves que se describe en ISO/CEI 11770-1.	X.843
intercambio de claves	Trueque de claves públicas entre entidades que serán utilizadas para criptar las comunicaciones entre las entidades.	J.170
gestión de claves	Generación, almacenamiento, distribución, supresión, archivo y aplicación de claves de acuerdo con una política de seguridad.	X.800
fuga de información	Información adquirida por una parte no autorizada mediante la supervisión de las transmisiones, el acceso no autorizado a la información almacenada en cualquier entidad MHS o mediante la escucha clandestina, haciéndose pasar por otra persona o utilizando indebidamente, o haciendo que un MTA funcione incorrectamente. La fuga de información puede provocar: la pérdida de confidencialidad, la pérdida del anonimato, la apropiación indebida de mensajes y el análisis del tráfico.	X.402
cifrado enlace por enlace	Aplicación individual del cifrado de datos en cada enlace de un sistema de comunicación. (Véase también cifrado extremo a extremo.) *Nota* – En este caso los datos están en forma de texto legible en las entidades relevadoras.	X.800
pérdida o degradación de información	La integridad de los datos transferidos es dudosa por posibles acciones de supresión, inserción, o modificación, reordenamiento, respuesta o demora no autorizadas.	M.3016.0
detección de manipulación	Mecanismo que se utiliza para detectar si una unidad de datos ha sido modificada, sea accidental o intencionalmente.	X.800
usurpación de identidad (o impostura)	Cuando una entidad pretende ser una entidad diferente.	X.800
código de autenticación de mensaje (MAC)	Valor de comprobación criptográfico utilizado para autenticar el origen de los datos y garantizar su integridad.	X.813

autenticación de origen del mensaje	El destinatario o un MTA de paso pueden autenticar la identidad del originador del mensaje.	X.400
integridad de la secuencia de mensajes	1. Permite al originador demostrar al destinatario que se ha preservado la secuencia de mensajes. 2. Este elemento de servicio permite al originador ofrecer al destinatario del mensaje un modo de comprobar que se ha preservado la secuencia de mensajes del originador al destinatario (sin pérdida, reordenación o repetición de mensajes). La integridad de secuencia de mensajes es un mecanismo que se utiliza para cada destinatario y para el que se puede utilizar una técnica criptográfica asimétrica o simétrica.	X.400
secuenciación de mensajes	Parte o la totalidad de un mensaje se repite, se difiere o se reordena para, por ejemplo, explotar la información de autenticación de un mensaje válido y modificar la secuencia o diferir mensajes válidos. Si bien es imposible impedir la reproducción con los servicios de seguridad MHS, se puede detectar y se pueden eliminar los efectos de la amenaza. Este proceso de secuenciación de mensajes incluye la reproducción, el reordenamiento, la preemisión y el retraso de mensajes.	X.402
función de supervisión	Cuando una TTP tiene la función de supervisión de la acción o el evento y se encarga de proporcionar pruebas sobre el objeto supervisado.	X.813
autenticación mutua	La confirmación de la identidad de ambas entidades principales.	X.811
no repudio	1. Capacidad de evitar que un remitente niegue más tarde haber enviado un mensaje o ejecutado una acción. 2. Impedir que una de las entidades que participa en una comunicación niegue que ha participado en toda la comunicación niegue parte de ésta. 3. Proceso por el que el remitente de un mensaje (por ejemplo una solicitud sobre un elemento de consulta previo pago) no puede negar que ha enviado el mensaje.	J.170 H.235 J.93
atestación	Registro de los datos ante un tercero de confianza que permite la ulterior confirmación de la exactitud de sus características, tales como contenido, origen, fecha, entrega.	X.800
atestador	Una tercera parte confiable ante la cual se registran los datos para que más adelante pueda garantizarse la exactitud de sus características.	X.813
amenaza pasiva	Amenaza de revelación de la información no autorizada sin modificar el estado del sistema.	X.800
contraseña	1. Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres. 2. Cuando es una cadena de contraseña introducida por el usuario: una clave de seguridad asignada que el usuario móvil comparte con su dominio propio. Esta contraseña de usuario y el secreto compartido del usuario deberán aplicarse para los fines de la autenticación del usuario	X.800 H.530
autenticación de entidad par	1. Corroboración de la identidad de una entidad par en una asociación. 2. Establecimiento de la prueba de la identidad de la entidad par durante una relación de comunicación.	X.800 M.3016.0
entorno de seguridad personal (PSE)	Almacenamiento local seguro para la clave privada de una entidad, la clave de la CA confiada directamente y posiblemente otros datos. Dependiendo de la política de seguridad de la entidad o los requisitos del sistema, se puede tratar, por ejemplo, de un archivo criptográficamente protegido o un testigo resistente a las manipulaciones en los equipos informáticos.	X.843

seguridad física	Medidas adoptadas para proporcionar la protección física de los recursos contra amenazas deliberadas o accidentales.	X.800
entidad principal	Entidad cuya identidad puede autenticarse.	X.811
privacidad	1. 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 una justificación de la seguridad. 2. 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 cifrado.	X.800 H.235
clave privada; clave secreta (término desaconsejado)	1. (En un criptosistema de claves públicas) clave de un par de claves de usuario que sólo es conocida por ese usuario. 2. Clave que se utiliza con un algoritmo criptográfico asimétrico y cuya posesión está restringida (usualmente a una sola entidad). 3. Clave utilizada en la criptografía de claves públicas que pertenece a una entidad y se debe mantener secreta.	X.509 X.810 J.170
privilegio	Atributo o propiedad asignado a una entidad por una autoridad.	X.509
infraestructura de gestión de privilegios (PMI)	Infraestructura capaz de soportar la gestión de privilegios, que permite un servicio de autorización completo y en relación con una infraestructura de claves públicas.	X.509
clave pública	1. (En un criptosistema de claves públicas) clave de un par de claves del usuario conocida públicamente. 2. Clave que se utiliza con un algoritmo criptográfico asimétrico y que se puede divulgar. 3. Clave utilizada en la criptografía de claves públicas que pertenece a una entidad particular y es distribuida públicamente. Otras entidades utilizan esta clave para encriptar datos que han de ser enviados al propietario de la clave.	X.509 X.810 J.170
certificado de clave pública	1. La clave pública de un usuario, junto con otras informaciones, que es infalsificable porque está cifrada con la clave privada de la autoridad de certificación que la emitió. 2. Valores que representan la clave pública de un propietario (u otra información opcional) verificada y firmada por una autoridad fiable en un formato infalsificable. 3. Vinculación entre la clave pública de una entidad y uno o más atributos relacionados con su identidad; se denomina también certificado digital.	X.509 H.235 J.170
criptografía de clave pública	Técnica criptográfica basada en un algoritmo de dos claves (privada y pública). El mensaje se encripta con la clave pública, pero puede descriptarse únicamente con la clave privada. También se conoce como sistema de clave privada-pública (PPK). *Nota* – El hecho de conocer la clave pública no permite conocer la clave privada. Ejemplo: A crea una clave privada y una pública, y envía la clave pública a todos sus posibles interlocutores, pero mantiene secreta la clave privada. De esta forma, todos los que poseen la clave pública pueden criptar un mensaje destinado a A, pero sólo A puede descriptar los mensajes con la clave privada.	J.93
infraestructura de claves públicas (PKI)	Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio.	X.509

autoridad de registro (RA)	1. Entidad responsable de la identificación y autenticación de sujetos de certificados. Como no es una CA ni una AA, no firma ni emite certificados. *Nota* – Una RA puede ayudar en el proceso de aplicación de certificados, en el proceso de revocación o en ambos. 2. Entidad fiable encargada de las actividades de registro.	X.842 X.843
ataque por retransmisión	Ataque a la autenticación que consiste en interceptar el intercambio de información de autenticación retransmitiendo inmediatamente.	X.811
parte confiante	Usuario o agente que se fía de los datos de un certificado al tomar decisiones.	X.509
reproducción no autorizada	Mensaje o parte de un mensaje que se repite para producir un efecto no autorizado. Por ejemplo, una entidad puede reproducir un mensaje válido con información de autenticación con el fin de autenticarse a sí mismo (por algo que no es).	X.800
repudio	1. Una de las entidades implicadas en una comunicación niega haber participado en toda la comunicación o en parte de ella. 2. Una entidad que participa en un intercambio de comunicación posteriormente, lo niega. 3. (En un caso de MHS): un usuario del servicio de transferencia de mensajes (MTS) o el MTS pueden negar haber presentado, recibido o creado un mensaje. Incluye: negación de origen, negación de presentación y negación de transmisión.	X.800 M.3016.0 X.402
revelación	Operación en la que se suprime parte o la totalidad de la protección de confidencialidad previamente aplicada.	X.814
certificado de revocación	Certificado de seguridad expedido por una autoridad de seguridad para indicar que un determinado certificado de seguridad ha sido revocado.	X.810
certificado de lista de revocaciones	Certificado de seguridad que contiene una lista de certificados de seguridad que han sido revocados.	X.810
control de encaminamiento	Aplicación de reglas durante el proceso de encaminamiento con el fin de elegir o evitar redes, enlaces o relevadores específicos.	X.800
política de seguridad basada en reglas	Política de seguridad basada en reglas globales impuestas a todos los usuarios. Estas reglas suelen depender de una comparación de la sensibilidad de los recursos a los que se accede y la posesión de los atributos correspondientes por parte de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios.	X.800
sello	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.	X.810
clave secreta	Clave que se utiliza con un algoritmo criptográfico simétrico. La posesión de una clave secreta está restringida (usualmente a dos entidades).	X.810
seguridad	El término "*seguridad*" se emplea en el sentido de reducir al mínimo las vulnerabilidades de los activos y los recursos. Un activo es cualquier cosa de valor. La *vulnerabilidad* es cualquier debilidad que puede explotarse para entrar en un sistema o consultar la información que tiene. Una *amenaza* es una posible violación de la seguridad.	X.800
administrador de seguridad	Persona que es responsable de la definición o aplicación de una o más partes de una política de seguridad.	X.810
alarma de seguridad	Mensaje generado cuando se detecta un evento relativo a la seguridad definido por la política de seguridad como una condición de alarma. Las alarmas de seguridad tienen por objeto llamar la atención de las entidades adecuadas oportunamente.	X.816

asociación de seguridad	Relación entre dos o más entidades para las que existen atributos (información y normas de estado para regir la prestación de servicios de seguridad en los que participan dichas entidades. Relación existente entre entidades comunicantes de la capa inferior, que tiene los atributos de asociación de seguridad correspondientes.	X.803 X.802
auditoría de seguridad	Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.	X.800
registro de auditoría de seguridad	Datos recogidos que posiblemente pueden usarse para efectuar una auditoría de seguridad.	X.800
auditor de seguridad	Persona o proceso a los que se permite acceder al registro de auditoría de seguridad y elaborar informes de auditoría.	X.816
autoridad de seguridad	1. Entidad que es responsable de la definición, aplicación o cumplimiento de la política de seguridad. 2. Entidad responsable de la administración de una política de seguridad en el marco de un dominio de seguridad. 3. Administrador responsable de la implementación de una política de seguridad.	X.810 X.841 X.903
certificado de seguridad	Conjunto de datos pertinentes a la seguridad expedido 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. En la serie X.800 se adopta el término certificado de seguridad para evitar conflictos de terminología con X.509.	X.810
dominio de seguridad	1. Conjunto de usuarios y sistemas sujetos a una política de seguridad común. 2. Conjunto de recursos sujetos a una única política de seguridad.	X.841 X.411
intercambio de seguridad	Transferencia o secuencia de transferencias de información de control del protocolo de aplicación entre sistemas abiertos, que se inscriben en los procesos de uno o más mecanismos de seguridad.	X.803
información de seguridad (SI)	Información necesaria para implementar los servicios de seguridad.	X.810
etiqueta de seguridad	Marca vinculada a un recurso (puede ser una unidad de datos) que denomina o designa los atributos de seguridad de dicho recurso.	X.800
gestión de seguridad	Abarca todas las actividades necesarias para crear, mantener e interrumpir los aspectos relativos a la seguridad de un sistema: gestión de los servicios de seguridad, instalación de mecanismos de seguridad, gestión de claves (parte de gestión), creación de identidades, claves, información de control de acceso, gestión del registro de auditoría de seguridad y alarmas de seguridad entre otros.	M.3016.0
modelo de seguridad	Marco de descripción de los servicios de seguridad que contrarrestan las posibles amenazas al MTS y los elementos de seguridad que permiten dichos servicios.	X.402

política de seguridad	1. Conjunto de reglas establecidas por la autoridad de seguridad que rigen la utilización y prestación de servicios y facilidades de seguridad. 2. Conjunto de criterios para la prestación de servicios de seguridad. *Nota* – Véanse también política de seguridad basada en la identidad y política de seguridad basada en reglas. Una política de seguridad completa tratará necesariamente muchos aspectos que están fuera del ámbito de OSI.	X.509 X.800
reglas de seguridad	Información local que, en función de los servicios de seguridad seleccionados, especifica los mecanismos de seguridad que han de emplearse, incluidos los parámetros necesarios para explotar dicho mecanismo. *Nota* – Las reglas de seguridad constituyen reglas de interacción seguras tal y como se definen en el modelo de seguridad de capas superiores.	X.802
servicio de seguridad	Servicio proporcionado por una capa de sistemas abiertos comunicantes, que garantiza la seguridad adecuada de los sistemas o de la transferencia de datos.	X.800
estado de seguridad	Información de estado que se almacena en un sistema abierto y que se precisa para prestar servicios de seguridad.	X.803
testigo de seguridad	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.	X.810
transformación de seguridad	Conjunto de funciones (funciones de seguridad del sistema y funciones de comunicación de seguridad) que, combinadas, modifican de alguna forma los elementos de datos de usuario para protegerlos durante la comunicación o el almacenamiento.	X.803
protección selectiva de los campos	Protección de ciertos campos específicos dentro de un mensaje que ha de transmitirse.	X.800
sensibilidad	Característica de un recurso que presupone su valor o importancia.	X.509
secreto compartido	Clave de seguridad para los algoritmos criptográficos; se puede deducir de una contraseña.	H.530
blindar/blindaje	Crear una protección de integridad de los datos.	X.815
firma	Véase firma digital.	X.800
autenticación simple	Autenticación por medio de medidas de contraseñas simples.	X.509
fuente de autoridad (SOA)	Autoridad de atributo en la que confía un verificador de privilegios para un recurso determinado como la autoridad definitiva para asignar un conjunto de privilegios.	X.509
inundación (*spamming*)	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.	H.235
autenticación robusta	Autenticación por medio de credenciales derivadas criptográficamente.	X.509
método de autenticación simétrica	Método de autenticación en el que ambas entidades comparten información de autenticación común.	X.811

algoritmo criptográfico simétrico	Algoritmo de cifrado, o el correspondiente algoritmo de descifrado, que requieren la misma clave para estas dos operaciones.	X.810
amenaza	Violación potencial de la seguridad.	X.800
servicio de indicación de hora	Servicio que certifica la existencia de datos electrónicos en un determinado momento. *Nota* – Los servicios de indicación de hora son útiles y probablemente indispensables para respaldar la validez a largo plazo de las firmas.	X.842
análisis del tráfico	Información deducida de la observación de flujos de tráfico (presencia, ausencia, cantidad, sentido y frecuencia).	X.800
confidencialidad del flujo de tráfico	Servicio de confidencialidad que ofrece protección contra el análisis de tráfico, es decir, que protege la información que puede derivarse de la observación de los flujos de tráfico.	X.800
relleno de tráfico	Generación de ejemplares de comunicación espurias, unidades de datos y/o datos espurios en las unidades de datos.	X.800
trampilla	Cuando se altera una entidad de un sistema con el fin de permitir que un agresor produzca efectos no autorizados a petición o en el curso de un evento o secuencia de eventos predeterminados. Por ejemplo, se podría modificar la validación de una contraseña para validar, no sólo su efecto normal, sino también la contraseña del agresor.	X.800
caballo de troya	El caballo de troya introducido en el sistema tiene una función no autorizada, además de su función autorizada. Un relevador que también copia mensajes destinados a un canal no autorizado es un caballo de troya.	X.800
fiduciario (de confianza)	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.	X.810
entidad fiable	Entidad que puede infringir una política de seguridad, ya sea porque ejecuta acciones indebidas o porque no ejecuta las acciones debidas.	X.810
funcionalidad fiable	Funcionalidad percibida como correcta con respecto a algunos criterios, por ejemplo, los establecidos por una política de seguridad.	X.800
tercera parte fiable (TTP)	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).	X.810
acceso no autorizado	Cuando una entidad intenta acceder a datos, violando la política de seguridad en vigor.	M.3016.0
desblindar/desblindaje	Conversión de datos con protección de integridad en su formato inicial.	X.815
autenticación del usuario	Comprobar la identidad del usuario o el proceso de aplicación.	M.3016.0
validar	Comprobar los datos con protección de integridad a fin de detectar la pérdida de integridad.	X.815
verificador	Entidad o representante de la entidad que necesita autenticar una identidad. Sus funciones son las necesarias para establecer intercambios de autenticación.	X.811
vulnerabilidad	Cualquier debilidad que podría explotarse con el fin de violar un sistema o la información que contiene.	X.800
certificado X.509	Especificación de certificado de una clave pública que forma parte de las normas de la Rec. UIT-T X.500.	J.170

B.2 Acrónimos relacionados con la seguridad

Acrónimos	Definición
AA	[X.509] Autoridad de atributo (*attribute authority*)
ACI	[SANCHO] Información de control de acceso (*access control information*)
AE	[M.3010] Entidad de aplicación (*application entity*)
AES	[H.235] [J.170] Algoritmo de criptación avanzada (*advanced encryption standard algorithm*)
APS	[SANCHO] Conmutación automática de protección (*automatic protection switching*)
ASN.1	[H.680] Notación de sintaxis abstracta uno (*abstract syntax notation one*)
ASON	[SANCHO] Red óptica con conmutación automática (*automatically switched optical network*)
ASP	[X.805] [X.1121] Proveedor de servicio de aplicación (*application service provider*)
CA	[H.234] [H.235] [J.170] [X.509] Autoridad de certificación (*certification authority*). Organización de confianza que acepta las solicitudes de certificación de las entidades, autentica las solicitudes, emite certificados y mantiene información del estado sobre 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
CME	[X.790] Entidad de gestión conforme (*conformant management entity*)
CMIP	[M.3010] Protocolo común de información de gestión (*common management information protocol*)
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 (es un ejemplo de servidor de aplicación)
CORBA	[SANCHO] Arquitectura de intermediario de petición de objeto común (*common object request broker architecture*)
COS	[SANCHO] Clase de servicio (*class of service*)
CP	Política de certificado (*certificate policy*)
CPS	[SANCHO: X.842] Declaración de ejecución práctica de la certificación (*certification practice statement*) [SANCHO: Q.817] Declaración de política de certificación (*certification policy statement*)
CRL	[H.235] [X.509] Lista de revocación de certificados (*certificate revocation list*)
DCN	[SANCHO] Red de comunicación de datos (*data communication network*)
DES	[SANCHO] Norma de criptación de datos (*data encryption standard*). Norma de criptación digital (*digital encryption standard*)
DHCP	[SANCHO] Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)
DOCSIS	[SANCHO] Especificación de interfaz del servicio de datos por cable (*data-over-cable service interface specification*)
DSA	[X.509] Agente de sistema de directorio (*directory system agent*) [SANCHO] Algoritmo de firma digital (*digital signature algorithm*)
DSL	[SANCHO] Bucle de abonado digital (*digital subscriber loop*)
DSP	[SANCHO] Procesador de señales digitales (*digital signal processor*) [SANCHO] Protocolo de servicio de directorio (*directory service protocol*)
FDS	[SANCHO] Sistema de detección de fraude (*fraud detection system*)
FEAL	[T.36] Familia de algoritmos para el cifrado rápido de datos (*fast data encipherment algorithm*). Refleja bloques de 64 bits de texto sin cifrar en 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. Como es más rápida y simple, es más adecuada para microprocesadores de baja complejidad (tarjetas con microprocesador, por ejemplo). (A. Menezes et al., Handbook of Applied Cryptography, CRC Press, 1997).
FIGS	[M.3210.1] Sistema de registro de información de fraude (*fraud information gathering system*)
GK	[H.235] [H.510] [H.530] Controlador de acceso (*gatekeeper*)
GW	[H.235] Pasarela (*gateway*)

Acrónimos	Definición
HFC	[SANCHO] Cable híbrido fibra/coaxial (*hybrid fibre-coaxial cable*)
HFX	[T.30] [T.36] Cifrado de facsímil Hawthorne (*Hawthorne facsimile cipher*)
HKM	[T.30] [T.36] Algoritmo de gestión de claves de Hawthorne (*Hawthorne key management algorithm*)
ICN	Redes de información y comunicación (*information and communication network*)
ICT	Tecnologías de la información y la comunicación (*information and communication technology*)
ID	[H.235] Identificador (*identifier*)
IDEA	[T.36] Algoritmo internacional de criptación 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. Es uno de los algoritmos más conocidos. Desde su aparición, no se conocen ataques efectivos, aunque se ha intentado definirlos (http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci213675,00.html)
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
IKE+	[J.170] Señala una utilización de IKE que requiere certificados de clave pública
IMT-2000	[M.3210.1] Telecomunicaciones móviles internacionales-2000 (*international mobile telecommunications 2000*)
IP	[X.805] Protocolo Internet (*Internet protocol*)
IPSec	[H.235] [H.530] [J.170] [X.805] Seguridad del protocolo Internet (*Internet protocol security*)
IVR	[J.170] Sistema de respuesta vocal interactiva (*interactive voice response system*)
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*). Una subcapa de la capa de enlace de datos que suele funcionar directamente sobre la capa física.
MCU	[H.235] Unidad multidifusión (*multicast unit*) [H.323] Unidad de control multipunto (*multipoint control unit*)
MD5	[H.235] [J.170] Sumario 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*)
MS	[M.3210.1] Sistema de gestión (*management system*) Memoria de mensajes (*message store*) Sección multiplex (*multiplex section*)
MSP	[SANCHO] Protección de sección de multiplexación (*multiplex section protection*)
MS-SPRing	Anillo de protección compartida de sección múltiplex (*multiplex section shared protection ring*)
MTA	[J.170] Adaptador de terminal de medios (*media terminal adapter*) Adaptador de terminal multimedios (*multimedia terminal adapter*) Agente de transferencia de mensajes (*message transfer agent*)
NAT	[H.235] Traducción de direcciones de red (*network address translation*)
OAM&P	[SANCHO] Operaciones, administración, mantenimiento y aprovisionamiento (*operations, administration, maintenance & provisioning*)

Acrónimos	Definición
OS	[M.3010] [X.790] Sistema de operaciones (*operations system*)
OSF	[M.3010] Función de sistema de operaciones (*operations systems function*)
OSI	[SANCHO] 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
PDA	Agenda digital personal (*personal data assistant*)
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
PKINIT	[J.160] Autenticación inicial mediante criptografía de clave pública (*public key cryptography initial authentication*) [J.191] Criptografía de clave pública para la autenticación inicial (*public-key cryptography for initial authentication*)
PMI	[X.509] Infraestructura de gestión de privilegios (*privilege management infrastructure*)
QoS	[SANCHO] Calidad de servicio (*quality of service*)
RA	Autoridad de registro (*registration authority*)
RADIUS	[J.170] Servicio de usuario de marcación para autenticación a distancia (*remote authentication dial-in user service*)
RAS	[SANCHO] Registro, admisión y situación (*registration, admission and status*) [SANCHO] Protocolo de registro, admisión y estado (*registration, admission and status protocol*)
RBAC	[X.509] Control de acceso basado en los cometidos (*role-based access control*)
RKS	[J.170] Servidor de mantenimiento de registros (*record keeping server*). Dispositivo que recopila y correlaciona los diversos mensajes de evento
RSA	[H.235] [T.30] [T.36] Rivest, Shamir y Adleman (algoritmo de clave pública)
RTP	[H.225.0] [H.235] [J.170] Protocolo en tiempo real (*real time protocol*)
SHA1	[H.235] Algoritmo de generación numérica seguro N.º 1 (*secure hash algorithm No. 1*)
SG	Pasarela de señalización (*signalling gateway*)
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
SNC	[SANCHO] Conexión de subred (*sub-network connection*)
SNMP	[J.170] [X.805] Protocolo simple de gestión de red (*simple network management protocol*)
SoA	[X.509] Fuente de autoridad (*source of authority*)
SRTP	[H.225.0] [H.235] Protocolo de transporte en tiempo real seguro (*secure real time protocol*)
SS7	[J.170] [X.805] Sistema de señalización N.º 7. Arquitectura y conjunto de protocolos para la señalización de llamada fuera de banda en una red telefónica
SSL	[H.235] [X.805] Capa de zócalo segura (*secure socket layer*)
TFTP	[SANCHO] Protocolo de transferencia de ficheros trivial (*trivial file transfer protocol*)
TGS	[J.160] Servidor que concede tique (*ticket granting server*)
TLS	[H.235] Seguridad de capa de transporte (*transport level security*)
RGT	[M.3010] [M.3210.1] [X.790] Red de gestión de las telecomunicaciones
TTP	[X.810] Tercera parte confiable (*trusted third party*)
UDP	[J.170] Protocolo de datagrama de usuario (*user datagram protocol*)
VA	Autoridad de validación (*validation authority*)
VoIP	[X.805] Voz por IP (*voice over IP*)
VPN	[X.805] Red privada virtual (*virtual private network*)

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 Comisiones de Estudio (CE), en las que los representantes de los miembros del Sector preparan Recomendaciones (normas) relativas a los diferentes campos de las telecomunicaciones internacionales. El trabajo de las CE está organizado en Cuestiones de estudio, que tratan cada una un aspecto determinado de la normalización de las telecomunicaciones. A continuación se enumeran las Comisiones de Estudio del UIT-T para el periodo de estudios 2005-2008, 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 para la definición de servicios, la numeración y el encaminamiento*
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 relacionadas con la seguridad:	
– **C.1/2** – Aplicación de los planes de numeración, denominación y direccionamiento para los servicios de telecomunicaciones, y aspectos de la explotación y del servicio de la numeración, incluida la definición de servicio (F.851)	
– **C.4/2** – Aspectos de la explotación de la calidad de servicio de las redes de telecomunicaciones (E.408, E.409 (en colaboración con la CE 17)).	

CE 3	Principios de tarificación y contabilidad, incluidos los temas relativos a economía y política de las telecomunicaciones
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 relacionadas con la seguridad: Ninguna	

CE 4	Gestión de las telecomunicaciones *Comisión de Estudio Rectora sobre la gestión de las telecomunicaciones.*

Se encarga de los estudios relativos a la gestión de los servicios, las redes y los equipos de telecomunicaciones, incluidos los de las redes de la próxima generación (NGN) y la aplicación y evolución del marco de la red de gestión de las telecomunicaciones (RGT). Además, se encarga de otros estudios de gestión de las telecomunicaciones relativos a las designaciones, los procedimientos operativos relacionados con el transporte, y las técnicas y la instrumentación de pruebas y mediciones.

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.

La serie de Recomendaciones M.3016 aprobada recientemente sustituye a la serie original de la Rec. UIT-T M.3016 (1998). En ella se describe la importancia y la aplicabilidad de la seguridad en lo referente al lenguaje de la RGT. En lugar de imponer la prestación de un conjunto de servicios como medida de protección ante las amenazas, se especifica un marco en que las distintas organizaciones pueden especificar la utilización de los mecanismos disponibles.

En la serie M.3016 se tratan las siguientes amenazas en la RGT: la usurpación de identidad, la escucha clandestina, el acceso no autorizado, la pérdida o la alteración de información, el repudio, la falsificación, y la denegación de servicio. En ella también se abordan los siguientes aspectos de la seguridad: la confidencialidad, la integridad de datos, la imputabilidad y la disponibilidad.

Cuestiones relacionadas con la seguridad:

– **C.6/4** – Arquitectura y principios de gestión (M.3010, serie M.3016 y M.3400)

– **C.7/4** – Necesidades en materia de interfaces de gestión de empresa a empresa y de cliente a empresa (M.3320)

– **C.10/4** – Modelos de información específicos para una aplicación (M.3210.1)

– **C.11/4** – Protocolos para interfaces de gestión (Q.813, Q.815 y Q.817)

CE 5	Protección contra los efectos del entorno electromagnético

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), con la seguridad y las consecuencias para la salud de los campos electromagnéticos producidos por las instalaciones y los dispositivos de telecomunicaciones, incluidos los teléfonos celulares.

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. 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 premeditados de origen humano. Durante el periodo de estudio actual, los aspectos de seguridad en los trabajos de la CE se examinan en el marco de la nueva Cuestión 15/5, *Seguridad de los sistemas de telecomunicación e información relativa al entorno electromagnético*.

Entre las amenazas electromagnéticas se cuentan los fenómenos transitorios de alta potencia generados por actividades humanas malintencionadas, como los impulsos electromagnéticos a gran altitud (HEMP) y las emisiones de generadores de alta potencia electromagnética (HPEM, *high power electromagnetic*), que incluyen las fuentes de alta potencia de microondas (HPM) y de banda ultraancha (UWB, *ultra-wideband*). La seguridad electromagnética también tiene que ver con la prevención de posibles fugas de información en la red causadas por emisiones radioeléctricas inesperadas de los equipos.

Cuestiones 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 (EMC de los equipos de telecomunicaciones mejora 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.15/5** – Seguridad de los sistemas de telecomunicación e información relativa al entorno electromagnético. (La resistencia de los equipos a los rayos supone mayor resistencia a los impulsos a gran altitud (HEMP).

CE 6	Planta exterior e instalaciones interiores relacionadas

Se encarga de los estudios relativos a la planta exterior, e instalaciones interiores relacionadas: fabricación, instalación, empalme, terminación, protección contra la corrosión y otros daños causados por las condiciones ambientales (no por los procesos electromagnéticos), de todos los tipos de cables terrenales utilizados por las telecomunicaciones públicas y estructuras asociadas.

Cuestiones relacionadas con la seguridad:

– **C.1/6** – Procedimientos ambientales y de seguridad para la planta exterior

– **C.6/6** – Mantenimientos de la red de cables de fibra óptica

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

Se encarga de los estudios relativos a:

a) 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.

b) 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 calidad de Comisión de Estudio Rectora en materia de redes de cable integradas de banda ancha y televisión, evalúa las amenazas y vulnerabilidades de las redes y los servicios de banda ancha, documenta los objetivos de seguridad, estudia las posibles medidas de protección, y define arquitecturas de seguridad.

Las actividades relacionadas con la seguridad se concentran en:

a) *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.

b) *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 vídeo por el IP. Los servicios de seguridad que se ofrecen en el IPCablecom son: autenticación del adaptador de terminal multimedias (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.

c) *Servicios seguros de redes propias (domésticas)*: Gracias a los módem de cable mejorados se pueden ofrecer servicios en redes domésticas del tipo cortafuegos 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.

d) *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 multimedias (MHP, *multimedia home platform*).

Cuestiones relacionadas con la seguridad:
– **C.3/9** – Métodos y prácticas para el acceso condicional y la protección contra las copias no autorizadas y la redistribución no autorizada ("control de redistribución" para la distribución de televisión digital por cable a los hogares) (J.93, J.96)
– **C.8/9** – Distribución de servicios y aplicaciones digitales en la televisión por cable, que utilizan protocolos Internet y/o datos basados en paquetes (J.112)
– **C.9/9** – Aplicaciones de señales vocales y vídeo con protocolos Internet en las redes de televisión por cable (J.160, J.170 y J.191)
– **C.10/9** – Ampliación de los servicios por cable utilizando redes de banda ancha domésticas

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

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 multimedias y la mejora de las Recomendaciones actuales sobre protocolos de señalización de interfuncionamiento y acceso de ATM, RDSI-BE y RTPC.

La mayoría de las Recomendaciones en vigor de la CE 11 se elaboraron para redes confiables basadas en la multiplexación por división temporal (TDM) en las que podían utilizarse conexiones de punto a punto para garantizar la seguridad de las comunicaciones. La CE 11 reconoció que la introducción de la tecnología IP en la red presentaría nuevos problemas de seguridad. Para adaptarse a esta introducción de la tecnología IP y satisfacer la necesidad de información de señalización y de control en esta red en transformación con todas las garantías de seguridad, la CE 11 planteó en 2004 una serie de Cuestiones relativas a los requisitos y protocolos de señalización con estos nuevos retos de seguridad.

Cuestiones relacionadas con la seguridad:
– **C.1/11** – Señalización de red y arquitecturas funcionales de control en entornos emergentes de redes de la próxima generación (NGN)
– **C.7/11** – Requisitos y protocolos de señalización y control para soportar la anexión en entornos NGN

CE 12	Calidad de funcionamiento y calidad del servicio *Comisión Estudio Rectora sobre calidad de servicio y calidad de funcionamiento.*

Se encarga de dar orientación sobre la calidad de transmisión de extremo a extremo de redes y terminales, tomando como referencia la calidad percibida y la aceptación de aplicaciones de texto, voz y multimedias por los usuarios. Si bien esta labor comprende las implicaciones de transmisión para todas las redes (por ejemplo, redes basadas en PDH, SDH, ATM, IP así como las redes NGN) y para todos los terminales de telecomunicaciones (por ejemplo, microteléfonos, terminal de manos libres, auriculares, móviles, audiovisuales y de respuesta interactiva a la voz), se presta especial atención a la calidad de servicio IP, la compatibilidad y las implicaciones para las NGN. En sus labores se incluyen temas de gestión de la calidad de funcionamiento y de los recursos.

Cuestiones relacionadas con la seguridad:

– **C.10/12** – Planificación de la transmisión y consideraciones de calidad de funcionamiento para los servicios en banda vocal, de datos y multimedias

– **C.13/12** – Requisitos en cuanto a la calidad de servicio/calidad de la percepción, así como los métodos de evaluación

– **C.17/12** – Calidad de funcionamiento de las redes basadas en el protocolo Internet (IP)

CE 13	Redes de la próxima generación Comisión de Estudio Rectora para las NGN y temas de satélite.

Se encarga de los estudios relativos a la arquitectura, la evolución y la convergencia de las redes de la próxima generación (NGN), incluidos los marcos y las arquitecturas funcionales, los requisitos de señalización para las NGN, la coordinación de la gestión de proyectos de NGN en las Comisiones de Estudio, la planificación de sistemas, los escenarios de implementación y los modelos de instalación, las capacidades de la red y del servicio, la compatibilidad, la repercusión del IPv6, la movilidad y la convergencia en las NGN y los aspectos de la red pública de datos.

Al reconocer que la seguridad es uno de los elementos fundamentales de las NGN, la CE 13 ha creado una Cuestión dedicada a dicho tema: La Cuestión 15/13, Seguridad de las NGN, está centrada en el estudio de los asuntos de seguridad específicos a las NGN y la definición de soluciones. Uno de los objetivos esenciales de la CE 13 es elaborar un conjunto de normas que garanticen, en la mayor medida posible, la seguridad de la infraestructura de las telecomunicaciones ahora que las redes evolucionan hacia las NGN.

La Comisión de Estudio 13 también ha decidido incorporar en cada una de las Recomendaciones nuevas y revisadas una sección dedicada a la seguridad, en el que se indicarán las secciones de la Recomendación que tratan de los aspectos relativos a la seguridad.

La Comisión de Estudio 13 trabaja en los asuntos relativos a la seguridad de las NGN en colaboración con otras Comisiones de Estudio y con otros organismos de normalización. El IETF (Internet, Seguridad y Transporte), 3GGP, 3GPP2 y el Foro DSL principales son las organizaciones de normalización para los estudios de seguridad realizados por la CE 13.

Cuestiones relacionadas con la seguridad:

- **Q.2/13** – Requisitos y escenarios de implementación de los servicios de reciente aparición en las NGN
- **Q.3/13** – Principios y arquitectura funcional de las NGN
- **Q.4/13** – Requisitos y marco de trabajo para la QoS de las NGN
- **Q.5/13** – Gestión de operaciones, administración y mantenimiento (OAM) para las NGN
- **Q.6/13** – Movilidad de las NGN y convergencia de las redes fija-móvil y de sus servicios
- **Q.7/13** – Interfuncionamiento de redes y servicios en el entorno de las NGN
- **Q.8/13** – Escenarios de servicios y modelos de despliegue de las NGN
- **Q.9/13** – Repercusión del protocolo IPv6 en una NGN
- **Q.10/13** – Interoperabilidad de las redes de satélite con las redes terrenales y de la próxima generación (NGN)
- **Q.12/13** – Retransmisión de tramas (X.272)
- **Q.13/13** – Redes públicas de datos
- **Q.14/13** – Protocolos y mecanismos de servicios para las redes de datos multiservicios (MSDN)
- **Q.15/13** – Seguridad en las NGN

Entre las tareas relativas a la seguridad cabe señalar las siguientes:

- Dirigir los asuntos relativos a los proyectos de seguridad específicos a las NGN en el marco de la CE 13 y en colaboración con otras Comisiones de Estudio. Reconociendo la función global de la CE 17 como Comisión de Estudio Rectora para la seguridad de las telecomunicaciones, asesorar y asistir a esta Comisión en lo tocante a los asuntos de coordinación de la seguridad de las NGN.
- Determinar el modo de aplicación de la Rec. UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo* en el marco de un entorno de NGN.
- Velar por el desarrollo de una arquitectura NGN que se ajuste a los principios de seguridad aceptados.
- Garantizar la debida incorporación de los principios de autenticación, autorización y contabilidad (AAA) en las NGN

CE 15	Infraestructuras de las redes ópticas y de otras redes de transporte *Comisión de Estudio Rectora sobre transporte por redes de acceso* *Comisión de Estudio Rectora sobre tecnología óptica*

La CE 15 es la coordinadora en el UIT-T de las cuestiones relacionadas con la elaboración de normas para las infraestructuras, sistemas, equipos y fibras ópticas de las redes ópticas y otras redes de transporte, fibras ópticas y las tecnologías del plano de control correspondientes que permiten realizar la transición hacia redes de transporte inteligentes. Este trabajo abarca la elaboración de normas relativas a las instalaciones de los clientes, el acceso, y las secciones metropolitanas y de larga distancia de las redes de comunicación.

La CE 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. La Cuestión 14/15 sigue 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 la Cuestión 14/15:

a) 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 y 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.

b) Requisitos y arquitecturas de redes de comunicación de datos: en G.7712/Y.1703 se definen los requisitos de arquitectura para una RCD capaz de soportar las comunicaciones de gestión distribuida relacionadas con la RGT, las comunicaciones de señalización distribuida relacionadas con la red óptica con conmutación automática (ASON, *automatically switched optical 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 ASON 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 G.7712/Y.1703 se hace referencia a la serie 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.

c) 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*). 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, información que permita la autenticación de la petición de llamada, y tal vez la verificación de su integridad).

d) Arquitectura y requisitos para el encaminamiento en la ASON: 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 ASON. Los temas principales cubiertos en esta Recomendación son: arquitectura de encaminamiento ASON, componentes funcionales (selección de trayecto, atributos de encaminamiento, mensajes abstractos y diagramas de estado). En esta Recomendación se hace referencia a la serie de Recs. 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 la serie de Recs. UIT-T M.3016 (confidencialidad, integridad de datos, imputabilidad y disponibilidad), pueden adquirir diversos niveles de importancia. En el análisis de amenazas para un protocolo de encaminamiento deberá incluir, basándose en la Rec. UIT-T X.800: la suplantación de identidad, la escucha clandestina, el acceso no autorizado, la pérdida o degradación de información (incluidos los ataques de reproducción no autorizada), el repudio, la falsificación y la denegación de servicio.

e) Marco de gestión de la ASON: en G.7718/Y.1709 se tratan los aspectos de gestión del plano de control ASON y las interacciones de este plano de control de ASON con el plano de gestión. Se incluirán los requisitos para los distintos tipos de gestión (averías, configuración, contabilidad, calidad de funcionamiento y seguridad) en el plano de control.

Cuestiones relacionadas con la seguridad:

– **C.3/15** – Características generales de las redes ópticas de transporte (G.911)

– **C.9/15** – Equipos de transporte y protección para la recuperación de red (G.808.1, G.841, G.842, G.873.1)

– **C.14/15** – Gestión y control de sistemas y equipos de transporte

CE 16	Terminales, sistemas y aplicaciones multimedias *Comisión de Estudio Rectora sobre terminales, sistemas y aplicaciones multimedias, y sobre aplicaciones ubicuas ("todo electrónico", tales como cibersanidad y empresa electrónica)*

La CE 16 es la Comisión de Estudio Rectora sobre terminales, sistemas y aplicaciones multimedias, y sobre aplicaciones ubicuas ("todo electrónico", tales como cibersanidad y empresa electrónica). La Cuestión 25/16 (del

GT 2/16) trata sobre "Seguridad multimedia en redes de próxima generación", en particular sobre:

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

Se suele aceptar que todas estas aplicaciones tienen las mismas necesidades de seguridad que se pueden satisfacer mediante medidas genéricas, por ejemplo de seguridad de red o de autenticación de toda la 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 25/16 se centra en los aspectos de seguridad de las aplicaciones MM en las redes de la próxima generación (NGN-MM-SEC) y también considera medidas complementarias de seguridad de red cuando conviene. Su objetivo es elaborar Recomendaciones en materia de seguridad para satisfacer las necesidades del mercado a este respecto.

Cuestiones relacionadas con la seguridad:

– **C.1/16** – Sistemas, terminales y conferencias de datos multimedias (H.233, H.234)

– **C.2/16** – Comunicaciones de audio, vídeo y datos en tiempo real a través de redes con conmutación de paquetes (H.323)

– **C.4/16** – Características avanzadas de los servicios de comunicación multimedias sobre las plataformas de los sistemas multimedias definidas por el UIT-T (H.350.2)

– **C.25/16** – Seguridad multimedias en redes de la próxima generación (NGN-MM-SEC) (serie H.235)

– **C.29/16** – Movilidad de los sistemas y servicios multimedias (H.530)

CE 17	Seguridad, lenguajes y soporte lógico de telecomunicaciones *Comisión de Estudio Rectora sobre seguridad de las telecomunicaciones y sobre lenguajes y técnicas de descripción.*

La CE 17 se encarga de los estudios relativos a la seguridad, la aplicación de las comunicaciones de sistemas abiertos (sistemas de intercambios y de directorio), y de los lenguajes técnicos, el modo de utilizarlos y otros temas relacionados con los aspectos del soporte lógico de los sistemas de telecomunicaciones.

La CE 17 del UIT-T es la Comisión de Estudio Rectora sobre seguridad de las telecomunicaciones. Las tareas de normalización en materia de seguridad del UIT-T se coordinan a través de un nuevo proyecto sobre seguridad del Sector dirigido en el marco de la Cuestión 4/17. Una de las iniciativas es la elaboración y actualización de un catálogo de Recomendaciones de la UIT relativas a la seguridad y un compendio de definiciones sobre seguridad extraídas de Recomendaciones del UIT-T aprobadas. Se han celebrado talleres sobre seguridad y simposios sobre ciberseguridad en Seúl (Corea) en mayo de 2002, en Florianópolis (Brasil) en octubre de 2004, en Moscú (Rusia) en marzo de 2005 y en Ginebra (Suiza) en octubre de 2005. Se organizarán otros talleres según sea necesario.

La Rec. UIT-T X.509, *Marcos de clave pública y certificados de atributo*s, definida por el Grupo de Trabajo 1/17 proporciona las bases de las infraestructuras de clave pública (PKI) y las infraestructuras de gestión de privilegios (PMI). La Recomendación X.509 se adapta para satisfacer nuevas necesidades. El Grupo de Trabajo 2/17 se encarga de las Recomendaciones relativas a la arquitectura, el marco y el protocolo fundamentales de seguridad, y en especial de las Recomendaciones pertenecientes a la serie X.800. Durante el último periodo de estudios se elaboró un conjunto de Recomendaciones nuevas relativas a la seguridad, incluida la X.805, en la que se define una arquitectura para proporcionar seguridad en la red de extremo a extremo. Dicha arquitectura puede aplicarse a distintos tipos de redes, independientemente de la tecnología utilizada en la red.

Puede utilizarse como instrumento para garantizar la integridad de las consideraciones de seguridad en la preparación de Recomendaciones y para evaluar la seguridad de las redes. La Recomendación X.1051 es otra Recomendación fundamental, en la que se definen los requisitos para un sistema de gestión de seguridad de la información (ISMS, *information security management system*) en el contexto de las telecomunicaciones. En ella se especifican los requisitos necesarios para establecer, implementar, poner en funcionamiento, supervisar, revisar, mantener y mejorar un ISMS documentado en el marco de los riesgos comerciales globales de una organización de telecomunicaciones. La Recomendación X.1081 es una Recomendación marco en la que se establecen las bases para futuras especificaciones telebiométricas. En las Recomendaciones X.1121 y X.1122 se estudian las comunicaciones móviles de datos de extremo a extremo. En la Recomendación X.1121 se analizan las amenazas de seguridad en un entorno móvil y los métodos de protección desde el punto de vista del usuario móvil y del proveedor de servicios de la aplicación. En la Recomendación X.1122 se ofrecen directrices para construir sistemas móviles seguros basados en la tecnología de infraestructura de claves públicas (PKI). En la página de la CE 17 que se encuentra en el sitio web de la UIT puede consultarse información actualizada al respecto (véase http://www.itu.int/ITU-T/studygroups/com17/tel-security.html).

Cuestiones relacionadas con la seguridad:

GT 1/17 Tecnología de sistemas abiertos

– C.1/17 – Comunicaciones de multidistribución de extremo a extremo con gestión de la calidad de servicio

En esta Cuestión se examinan aspectos relativos a los requisitos, la arquitectura, la gestión de grupo y de sesión, y el protocolo de comunicaciones multidistribución de extremo a extremo. Para lograr una comunicación segura entre los miembros, se están estudiando extensiones de protocolo de seguridad para los protocolos de comunicaciones de multidistribución de extremo a extremo. En la actualidad el trabajo se centra en la aplicación de mecanismos de seguridad pertinentes para los protocolos de comunicaciones de multidistribución y en el establecimiento de procedimientos para entablar comunicaciones seguras.

– C.2/17 – Servicios de directorio, sistemas de directorio y certificados de clave pública y de atributos

El Grupo encargado de esta Cuestión elabora y mantiene la Recomendación X.509, en la que se especifican certificados de clave pública, certificados de atributos, la revocación de certificados y las infraestructuras de soporte (infraestructura de claves públicas e infraestructura de gestión de privilegios). Los certificados de claves públicas y la infraestructura de soporte son fundamentales para proporcionar autenticación y se aplican, en particular, en las firmas digitales.

– C.16/17 – Nombres de dominio internacionales

Los temas de seguridad forman parte de la labor que se realiza en torno a los nombres de dominio internacionales. La Cuestión 16/17 tiene por objeto identificar la documentación técnica existente sobre los nombres de dominio internacionales, incluida la documentación relativa a los riesgos de seguridad que implica la implementación de estos nombres en las redes de telecomunicaciones. Esta tarea se realiza en consulta con organismos como la ISO/CEI, el Consorcio UNICODE, IETF, ICANN y CENTR.

GT 2/17 Seguridad en las telecomunicaciones

– C.4/17 – Proyecto de seguridad de los sistemas de comunicaciones

El objetivo de esta Cuestión es establecer la finalidad, coordinar y organizar las actividades de seguridad en materia de telecomunicaciones en el marco del UIT-T. El tema de la seguridad se abordará adoptando una metodología descendente en colaboración con otras Comisiones de estudio y organizaciones de normalización. Se trata de concentrar los esfuerzos en los ámbitos estratégico y de proyectos.

– C.5/17 – Arquitectura y marco genérico de la seguridad

La seguridad en las redes debería fundamentarse en arquitecturas de seguridad normalizadas y tecnologías de seguridad normalizadas, para definir soluciones de seguridad rentables y globales que puedan aplicarse a distintos tipos de redes, servicios y aplicaciones en un entorno de múltiples vendedores. Habida cuenta de las amenazas de seguridad para un entorno de comunicaciones y el constante progreso de las contramedidas de seguridad que existen para luchar contra dichas amenazas, en el marco de este proyecto se examinan nuevos requisitos de seguridad y soluciones, y la evolución de las arquitecturas y los marcos de seguridad para adaptarse a la nuevas condiciones.

– C.6/17 – Ciberseguridad

En esta Cuestión se examinan los aspectos de las ciberseguridad en el contexto de la normalización internacional, a saber:

- los procesos de distribución, compartición y divulgación de información de vulnerabilidad;
- el procedimiento normalizado en las operaciones de manejo de incidentes en el ciberespacio;
- la estrategia de protección de la infraestructura de red fundamental.

– C.7/17 – Gestión de la seguridad

La finalidad de esta Cuestión es elaborar un conjunto de Recomendaciones sobre gestión de la seguridad para el UIT-T, teniendo en cuenta la necesidad de hacerlo en colaboración con la Comisión Técnica Mixta 1 de ISO/CEI. La prioridad es la identificación y gestión de los riesgos en los sistemas de telecomunicaciones, y armonizar el sistema de gestión de la seguridad de la información (ISMS) para los operadores de telecomunicaciones con las normas ISMS en vigor.

– C.8/17 – Telebiometría

Esta Cuestión, que se basa en los trabajos realizados en torno a la identificación y la autenticación personal por medio de la telebiometría, se estudia en estrecha colaboración con otros organismos de normalización competentes. Se trata de estudiar la utilización de métodos telebiométricos seguros para mejorar la identificación y la autenticación de los usuarios y las particularidades de las tecnologías de autenticación biométricas en el campo de las telecomunicaciones.

– C.9/17 – Servicios de comunicación seguros

Debido a determinadas características específicas de las comunicaciones móviles (por ejemplo, la transmisión por el aire, la capacidad de procesamiento limitada y el tamaño de la memoria de los pequeños dispositivos móviles), la seguridad plantea dificultades particulares y debe ser estudiada con especial atención. En el marco de esta Cuestión se examinan la identificación y definición de los servicios de comunicación seguros en las comunicaciones móviles o en los servicios por Internet, la identificación y la reacción a las amenazas que pesan sobre los servicios de comunicaciones, las tecnologías de soporte de los servicios de comunicaciones seguros, y las soluciones para mantener una interconectividad segura entre los distintos servicios de comunicación.

– C.17/17 – Soluciones técnicas al problema de las comunicaciones indiscriminadas

En esta Cuestión se estudian los requisitos técnicos, los marcos, las directrices y las nuevas tecnologías necesarias para contrarrestar las comunicaciones indiscriminadas. Se está elaborando un conjunto de Recomendaciones destinadas a contrarrestar el problema del correo electrónico basura y las comunicaciones indiscriminadas en las aplicaciones multimedias, tomando en consideración la necesidad de colaborar con otras Comisiones de Estudio del UIT-T y organizaciones de normalización.

GT 32/17 Lenguajes y soporte lógico de telecomunicaciones

– C.10/17 – Notación de sintaxis abstracta uno (ASN.1) y otros lenguajes de datos

Se ocupa de mantener y mejorar la ASN.1 y sus reglas de codificación, incluidas las DER (reglas de codificación distinguidas), que se utilizan en la creación de certificados digitales o firmas digitales según X.509. La ASN.1 es una parte importante de la representación de información de forma que se pueda criptar/descriptar y firmar/verificar de manera fiable. Uno de los objetivos de esta Cuestión es seguir mejorando la ASN.1 con el fin de atender a las necesidades cambiantes de los entornos de comunicación actuales.

CE 19	Red de telecomunicaciones móviles *Comisión de Estudio Rectora sobre redes de telecomunicaciones móviles y movilidad.*
Se encarga de los estudios relativos a las redes para las telecomunicaciones móviles, incluidas las redes de telecomunicaciones móviles internacionales 2000 (IMT-2000) y posteriores, la conexión inalámbrica a Internet, la convergencia de las redes móviles y fijas, la gestión de la movilidad, las funciones multimedias en sistemas móviles, la interconexión, la interoperabilidad y la mejora de las Recomendaciones del UIT-T en vigor sobre las IMT-2000.	
Cuestiones relacionadas con la seguridad:	
– **C.1/19 –** Requisitos de servicio y de capacidad de red y arquitectura de red	
– **C.3/19 –** Identificación de los sistemas IMT-2000 existentes y en curso de evolución (Q.1741.1, Q.1741.2, Q.1741.3, Q.1742.1, Q.1742.2, Q.1742.3)	
– **C.5/19 –** Convergencia de los sistemas del servicio fijo y los sistemas IMT-2000 existentes	

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.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

Seguridad en las telecomunicaciones

X.805 – Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo
X.1051 – Sistemas de gestión de seguridad de la información – Requisitos para telecomunicaciones
X.1081 – Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad
X.1121 – Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo
X.1122 – Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas

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 y privacidad de datos por redes de retransmisión de tramas

Técnicas de seguridad

X.841 – Objetos de información de seguridad para control de acceso
X.842 – Directrices sobre 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 certificados de claves públicas y atributos
X.519 – Especificaciones de protocolo

Seguridad de gestión de redes

M.3010 – Principios para una red de gestión de las telecomunicaciones
M.3016.x – Seguridad en el plano de gestión (subserie de Recomendaciones)
M.3210.1 – Servicios de gestión de la RGT para la gestión de 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

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 la seguridad de IPCablecom

Comunicaciones multimedios

H.233 – Sistemas con confidencialidad para servicios audiovisuales
H.234 – Sistema de gestión de claves de criptación y de autenticación para servicios audiovisuales
H.235.x – Marco de seguridad H.323 (subserie de Recomendaciones)
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

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 tratamiento de mensajes

X.400/F.400 – Visión de conjunto del sistema y del servicio de tratamiento de mensajes
X.402 – Arquitectura global
X.411 – Sistema de transferencia de mensajes: Definición del servicio abstracto y procedimientos
X.413 – Memoria de mensajes – Definición del servicio abstracto
X.419 – Especificaciones de protocolo
X.420 – Sistema de mensajería interpersonal
X.435 – Sistema de mensajería con intercambio electrónico de datos
X.440 – Sistema de mensajería vocal

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, ciberseguridad, seguridad de la red doméstica, seguridad de las redes de próxima generación, lucha contra el correo basura y telecomunicaciones de emergencia

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

Impreso en Suiza
Ginebra, 2006