Unión Internacional de Telecomunicaciones

Seguridad de las telecomunicaciones y las tecnologías de la información

Exposición general de asuntos relacionados con la seguridad de las telecomunicaciones y la aplicación de las Recomendaciones vigentes del UIT-T

UIT-T

Sector de Normalización de las Telecomunicaciones de la UIT

2009

Unión Internacional de Telecomunicaciones

UIT-T

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

Seguridad
de las telecomunicaciones y
las tecnologías de la información

Exposición general de asuntos relacionados con la seguridad
de las telecomunicaciones y la aplicación
de las Recomendaciones vigentes del UIT-T

Septiembre de 2009

Prefacio

Malcolm Johnson
Director
Oficina de Normalización de las
Telecomunicaciones de la UIT

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.

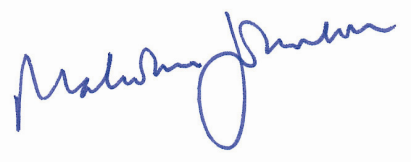
Es posible que la importancia cada día mayor de la seguridad de las tecnologías de la información y la comunicación (TIC) se deba al gran número de incidentes debidos a virus, gusanos, piratas y amenazas a la privacidad de las personas. Pero lo cierto es que en este momento la informática y la interconexión de redes son tan importantes para la vida de todos, que resulta 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 dispone hoy en día de una legislación de protección de datos que requiere el cumplimiento de normas reconocidas de confidencialidad e integridad de datos.

Actualmente casi todos reconocen que la seguridad debe estar incorporada en los sistemas, en lugar de añadirse a posteriori y que, para ser realmente eficaz, la seguridad se ha de tener en cuenta en todas las fases de la vida útil del sistema, desde la concepción y el diseño hasta la implementación e instalación y, por último, el desmantelamiento. De no considerarse adecuadamente estos aspectos de la seguridad durante la fase de diseño de los proyectos y el desarrollo de los sistemas se pueden crear muy fácilmente vulnerabilidades a la hora de su aplicación. Los comités de normalización deben desempeñar un papel esencial en la protección de las telecomunicaciones y de los sistemas de tecnologías de la información manteniendo presentes las cuestiones de seguridad, velando por que ésta sea una parte fundamental de las especificaciones y proporcionando normas técnicas y orientaciones para ayudar a los implementadores y usuarios a mantener la fortaleza de los sistemas y servicios de comunicación a fin de que puedan resistir a ciberataques.

El UIT-T ha participado activamente durante muchos años en los trabajos sobre seguridad de las telecomunicaciones y las tecnologías de la información, pero, al aumentar la utilización de la red, ha crecido espectacularmente la carga de trabajo a causa de la aparición y evolución de amenazas y de las solicitudes de normas por parte de nuestros Miembros para ayudar a contrarrestar esas amenazas. El presente Manual contiene un resumen de algunos elementos clave de ese trabajo y presenta los amplios recursos de que dispone el UIT-T para ayudar a todos los usuarios a afrontar los ataques contra la seguridad de las redes.

La normalización es un elemento fundamental de la creación de una cultura mundial de la ciberseguridad. Podemos ganar la guerra contra las ciberamenazas y la ganaremos si aprovechamos el trabajo de los miles de personas en las administraciones públicas, el sector privado y el sector docente que se reúnen en organizaciones como la UIT con el fin de elaborar normas de seguridad y directrices para prácticas idóneas. El trabajo no tiene mayor encanto ni es llamativo, pero no deja de ser esencial para proteger nuestro futuro digital. Deseo manifestar mi agradecimiento a los ingenieros de la Oficina de Normalización de las Telecomunicaciones de la UIT que, junto con expertos de los Estados Miembros de la Unión, han trabajado y siguen trabajando para desarrollar sin descanso estas normas y directrices.

Este Manual es una guía para altos ejecutivos y administradores que sean responsables de la seguridad de la información y las telecomunicaciones, o se interesen por ella, así como técnicos, reguladores y otros interesados que deseen comprender mejor las cuestiones de seguridad de las TIC y las correspondientes Recomendaciones del UIT-T que tratan de esos temas. Confío en que el presente Manual resulte útil para los que pretenden abordar cuestiones de seguridad de las TIC y acogeré con agrado comentarios de los lectores para utilizarlos en futuras ediciones.



Malcolm Johnson

Director
Oficina de Normalización de las Telecomunicaciones, UIT

Índice

Página

Prefacio i

Agradecimientos vii

Resumen de conclusiones ix

Introducción a la 4ª edición xi

1 Introducción 1
- 1.1 Objeto y alcance del presente Manual 1
- 1.2 Cómo utilizar el presente Manual 1

2 Resumen de las actividades del UIT-T en materia de seguridad 5
- 2.1 Introducción 5
- 2.2 Documentación de referencia y exteriores 5
- 2.3 Resumen de los principales asuntos y Recomendaciones relativos a la seguridad 5

3 Requisitos de seguridad 9
- 3.1 Introducción 9
- 3.2 Amenazas, riesgos y vulnerabilidades 9
- 3.3 Objetivos generales de seguridad para las redes TIC 11
- 3.4 Antecedentes de las normas de seguridad 12
- 3.5 Evolución de las normas de seguridad del UIT-T 12
- 3.6 Requisitos de seguridad personal y física 14

4 Arquitecturas de seguridad 17
- 4.1 Arquitectura de seguridad de sistemas abiertos y normas relacionadas 17
- 4.2 Servicios de seguridad 18
- 4.3 Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo 19
  - 4.3.1 Elementos de la arquitectura UIT-T X.805 19
  - 4.3.2 Disponibilidad de la red y de sus componentes 22
- 4.4 Directrices de implementación 22
- 4.5 Algunas arquitecturas específicas de la aplicación 23
  - 4.5.1 Comunicaciones entre pares 23
  - 4.5.2 Arquitectura de seguridad para la seguridad de mensajes en los servicios móviles por Internet 25
- 4.6 Otras arquitecturas y modelos de seguridad de red 26

Página

5 Aspectos de la gestión de seguridad ... 29
5.1 Gestión de seguridad de la información ... 29
5.2 Gestión de riesgos ... 30
5.3 Tratamiento de incidentes ... 31
6 El directorio, autenticación y gestión de identidad ... 37
6.1 Protección de la información de directorio ... 37
6.1.1 Objetivos de la protección del directorio ... 37
6.1.2 Autenticación de los usuarios de directorio ... 38
6.1.3 Control de acceso al directorio ... 38
6.1.4 Protección de privacidad ... 39
6.2 Autenticación robusta: mecanismos de seguridad de clave pública ... 39
6.2.1 Clave secreta y criptografía de clave pública ... 40
6.2.2 Certificados de clave pública ... 42
6.2.3 Infraestructuras de clave pública ... 43
6.2.4 Infraestructura de gestión de privilegios ... 43
6.3 Directrices de autenticación ... 45
6.3.1 Protocolo de autenticación basado en contraseña segura con intercambio de clave ... 45
6.3.2 Protocolo de autenticación extensible ... 46
6.4 Gestión de identidad ... 47
6.4.1 Visión general de la gestión de identidades ... 47
6.4.2 Tareas del UIT-T en la gestión de identidades ... 48
6.5 Telebiometría ... 49
6.5.1 Autenticación telebiométrica ... 49
6.5.2 Generación y protección de claves digitales telebiométricas ... 49
6.5.3 Aspectos de seguridad de la telebiometría ... 50
6.5.4 Telebiometría relacionada con la fisiología humana ... 50
6.5.5 Elaboración de otras normas sobre telebiometría ... 51
7 Seguridad de la infraestructura de red ... 55
7.1 Red de gestión de las telecomunicaciones ... 55
7.2 Arquitectura de gestión de red ... 55
7.3 Seguridad de los elementos de infraestructura de una red ... 57
7.4 Seguridad de las actividades de supervisión y control ... 58
7.5 Seguridad de las aplicaciones basadas en la red ... 59

Página

7.6 Servicios comunes de gestión de seguridad ... 60
7.6.1 Función de informe de alarmas de seguridad ... 60
7.6.2 Función de pista de auditoría de seguridad ... 60
7.6.3 Control de acceso para entidades gestionadas ... 61
7.6.4 Servicios de seguridad basados en CORBA ... 61

8 Planteamientos específicos a la seguridad de la red ... 65
8.1 Seguridad para las redes de la próxima generación (NGN) ... 65
8.1.1 Objetivos y requisitos de seguridad de las NGN ... 65
8.2 Seguridad de las comunicaciones móviles ... 67
8.2.1 Comunicaciones de datos móviles seguras de extremo a extremo ... 68
8.3 Seguridad para redes domésticas ... 72
8.3.1 Marco de seguridad para las redes domésticas ... 72
8.3.2 Certificación y autenticación de dispositivos en redes domésticas ... 73
8.3.3 Autenticación de usuario humano para servicios de red doméstica ... 75
8.4 IPCablecom ... 76
8.4.1 Arquitectura IPCablecom ... 76
8.4.2 Requisitos de seguridad para IPCablecom ... 77
8.4.3 Servicios y mecanismos de seguridad en IPCablecom ... 78
8.5 IPCablecom2 ... 78
8.5.1 Arquitectura de IPCablecom2 ... 78
8.5.2 Requisitos de seguridad para IPCablecom2 ... 78
8.5.3 Servicios y mecanismos de seguridad en IPCablecom2 ... 79
8.6 Seguridad para redes de sensores ubicuos ... 80

9 Seguridad de aplicación ... 85
9.1 Voz sobre IP (VoIP) y multimedios ... 85
9.1.1 Aspectos de seguridad en multimedios y VoIP ... 86
9.1.2 Recomendaciones de la subserie H.235.x ... 88
9.1.3 Dispositivos de traducción de dirección de red y cortafuegos ... 90
9.2 IPTV ... 92
9.2.1 Mecanismos para proteger el contenido IPTV ... 93
9.2.2 Mecanismos para proteger el servicio IPTV ... 94
9.2.3 Protección de la información de abonado ... 94
9.3 Transmisión segura de facsímil ... 94

Página

9.4 Servicios web ... 95
9.4.1 Lenguaje de marcaje de asertos de seguridad ... 96
9.4.2 Lenguaje de marcaje de control de acceso extensible ... 97
9.5 Servicios basados en marcadores ... 97
10 Contrarrestar amenazas comunes en las redes ... 103
10.1 Contrarrestar el bombardeo electrónico ... 103
10.1.1 Estrategias técnicas para contrarrestar el bombardeo electrónico ... 103
10.1.2 Correo electrónico no solicitado ... 104
10.1.3 Correo basura en aplicaciones multimedios IP ... 105
10.1.4 Correo basura en servicios de mensajes cortos (SMS) ... 106
10.2 Código malicioso, programas espía y software engañoso ... 106
10.3 Notificación y difusión de actualizaciones de software ... 107
11 El futuro de la normalización de seguridad de las TIC ... 111
12 Fuentes de información adicional ... 115
Anexo A – Definiciones relativas a la seguridad ... 117
Anexo B – Acrónimos y abreviaturas utilizados en este Manual ... 127
Anexo C – Resumen de las Comisiones de Estudio del UIT-T relacionadas con la seguridad ... 133
Anexo D – Recomendaciones de seguridad referenciadas en este Manual ... 137

Agradecimientos

El presente Manual se ha preparado gracias a la contribución de numerosos autores, ya sea elaborando las Recomendaciones del UIT-T pertinentes o participando en reuniones, talleres y seminarios de las Comisiones de Estudio del UIT-T. Se ha de reconocer la labor de los Relatores, editores y coordinadores de seguridad de las Comisiones de Estudio de la UIT, de los consejeros de la UIT/TSB que participan en estudios sobre seguridad y, en particular, de Herb Bertine, antiguo Presidente de la Comisión de Estudio rectora del UIT-T para los trabajos sobre seguridad de las telecomunicaciones, y Mike Harrop, antiguo Relator para el proyecto de seguridad.

Resumen de conclusiones

El presente Manual tiene por objeto presentar una introducción de carácter general a los trabajos que realiza el UIT-T en materia de seguridad. Está destinado a quienes tienen responsabilidades en la seguridad de la información y las comunicaciones y las normas conexas, y se interesan por ellas, y a los que necesitan sencillamente comprender mejor cuestiones de seguridad de las TIC y las correspondientes Recomendaciones del UIT-T.

El texto comienza con un resumen de las actividades del UIT-T en materia de seguridad. En esa sección figuran enlaces a algunos de los recursos esenciales del UIT-T sobre seguridad y a información exterior. Además, esa introducción al Manual contiene un cuadro resumido en el cual se indica cómo lo pueden utilizar distintos tipos de lectores.

A continuación, los requisitos básicos de protección de aplicaciones, servicios e información TIC se presentan en una sección en la cual se explican las correspondientes amenazas y vulnerabilidades, se examina la función de las normas y se describen algunas de las características necesarias para proteger a los muy interesados por la utilización y explotación de instalaciones TIC. Además, en esa sección se justifican las normas de seguridad de las TIC y se resume la evolución de los trabajos del UIT-T al respecto.

Luego se introducen las arquitecturas de seguridad genéricas para sistemas abiertos y comunicaciones de extremo a extremo, junto con algunas arquitecturas específicas de la aplicación. Cada una de esas arquitecturas establece un marco en el cual se pueden aplicar las múltiples facetas de la seguridad de manera coherente. También se normalizan los conceptos subyacentes de los servicios y mecanismos de seguridad y se indica un vocabulario normalizado de términos y conceptos básicos de seguridad de las TIC. Los principios generales presentados en esas arquitecturas constituyen la base de muchas de las otras normas sobre servicios, mecanismos y protocolos de seguridad. Esa sección también contiene un enlace a directrices de seguridad relacionadas con actividades críticas asociadas con la vida útil de la seguridad de la red.

Después se abordan varios asuntos sobre gestión de seguridad en una sección en la cual se examina la gestión de la seguridad de la información, la gestión del riesgo y la respuesta y el tratamiento de incidentes.

Posteriormente se examina el Directorio y su función en los servicios de seguridad, junto con temas conexos de autenticación y gestión de la identidad. Se examinan temas tales como las infraestructuras de clave pública, la telebiometría (es decir, identificación y autenticación personal mediante aparatos biométricos en entornos de telecomunicaciones) y la privacidad, y también se aborda la importancia de la protección de la base de información del directorio.

Más adelante se analiza la seguridad de la infraestructura de red en relación con la gestión de red y los servicios comunes de gestión de seguridad.

A continuación se dan varios ejemplos y planteamientos específicos de la seguridad de las redes. La sección comienza con un estudio de los requisitos de seguridad de las redes de la próxima generación, seguido por un estudio de las redes de comunicaciones móviles que se encuentran en transición de la movilidad basada en una sola tecnología (tal como CDMA o GSM) a la movilidad a través de plataformas heterogéneas que utilizan el protocolo Internet. Esto va seguido por un examen de las disposiciones de seguridad de las redes domésticas y la televisión por cable. Por último, se resumen las dificultades de la seguridad para las redes de sensores ubicuas.

Si bien los desarrolladores de aplicaciones prestan hoy más atención a la necesidad de incorporar la seguridad en sus productos, en lugar de incorporarla a posteriori cuando la aplicación se encuentre en producción, las aplicaciones siguen estando en peligro por un entorno de amenazas en constante evolución y por sus vulnerabilidades inherentes. En la sección sobre la seguridad de las aplicaciones se estudian varias aplicaciones TIC tales como voz por IP, IPTV y fax seguro, insistiendo en particular en las características de seguridad definidas en Recomendaciones del UIT-T.

En la sección siguiente se examina cómo contrarrestar algunas amenazas comunes en las redes, tales como correos indeseados, códigos maliciosos y programas espía. También se estudia la importancia de una notificación y divulgación oportuna de actualizaciones y la necesidad de ser organizado y coherente en el tratamiento de incidentes de seguridad.

Por último, una breve sección trata de las posibles orientaciones futuras de la normalización de la seguridad de las TIC, seguida por un resumen de las fuentes de información adicional.

En los anexos se indican definiciones y siglas utilizadas en el Manual, se indican las Comisiones de Estudio que tratan asuntos de seguridad y se da una lista completa de las Recomendaciones mencionadas en el presente Manual.

Introducción a la 4ª edición

La estructura y el contenido de esta cuarta edición del Manual han sido objeto de una revisión sustancial. Desde que se publicó la primera edición en 2003, el UIT-T ha emprendido estudios sobre numerosos nuevos temas. Además, desde la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) de 2008 se han terminado y publicado numerosas nuevas Recomendaciones y se han reestructurado las Comisiones de Estudio propiamente dichas. Cualquier intento de abarcar todos estos trabajos de manera pormenorizada habría resultado en un documento demasiado largo, complejo e inmanejable. Tras consultar a los Miembros de la UIT se han determinado varios principios orientadores para esta edición, a saber:

- la publicación debería interesar a una amplia audiencia y tratar de evitar terminología y términos complejos que probablemente sólo se comprenden en ámbitos especializados;
- el texto debería completar y no duplicar el material existente disponible en otros formatos (por ejemplo, Recomendaciones);
- debería estar redactado para poderse publicar en formato impreso y electrónico;
- el texto debería contener en la medida de lo posible enlaces web a Recomendaciones y otras fuentes de material públicamente disponible. Debería indicarse mediante enlaces web información detallada adicional a la necesaria para alcanzar los objetivos básicos;
- en la medida de lo posible, el texto debería tratar sobre todo de los trabajos terminados y publicados, y no de los trabajos planificados o en curso.

Con arreglo a esos objetivos, en este Manual no se trata de abarcar todos los trabajos del UIT-T en materia de seguridad que ya han sido completados o están en curso. En cambio, se abordan temas concretos y se indican enlaces web a información adicional.

El Manual se publica en formato impreso y electrónico. Los lectores que utilicen una versión electrónica del texto disponen de hiperenlaces directos a las Recomendaciones indicadas y a documentación adicional en línea. Los lectores que utilizan los ejemplares impresos del texto pueden consultar la lista de Recomendaciones mencionadas en el Anexo D. Esas Recomendaciones se pueden consultar en línea en la dirección www.itu.int/rec/T-REC/es.

1. Introducción

1 Introducción

1.1 Objeto y alcance del presente Manual

El presente Manual se ha elaborado para presentar los trabajos sobre seguridad de las telecomunicaciones realizados por el UIT-T a altos ejecutivos y administradores con responsabilidades o interesados en la seguridad de las TIC y en las correspondientes normas. Además, el Manual puede interesar a los que deseen comprender mejor las cuestiones de seguridad de las TIC y las correspondientes Recomendaciones del UIT-T que tratan de esos temas.

En este Manual se da una perspectiva general de la seguridad de las tecnologías de telecomunicaciones y de la información, se examinan algunas de las cuestiones prácticas asociadas y se indica cómo diversos aspectos de la seguridad de las TIC se abordan en los trabajos de normalización del UIT-T. El Manual contiene material didáctico con enlaces a consejos más detallados y a material de referencia adicional. En particular, contiene enlaces directos a Recomendaciones y a documentos de referencia y divulgación. Reúne material relacionado con la seguridad extraído de las Recomendaciones del UIT-T en una sola publicación y contiene explicaciones sobre las relaciones entre diversos aspectos de los trabajos. Se indican los resultados logrados por el UIT-T en materia de normalización relacionada con la seguridad desde la segunda edición del Manual. En su mayoría, el Manual trata de trabajos ya terminados. Los resultados de los trabajos en curso actualmente se abordarán en futuras ediciones del presente Manual.

Además de los trabajos del UIT-T, también la Secretaría General y varios otros Sectores de la UIT han iniciado trabajos sobre seguridad, tales como trabajos sobre ciberseguridad (www.itu.int/cybersecurity) y el Informe del UIT-D sobre prácticas idóneas.

1.2 Cómo utilizar el presente Manual

El presente Manual tiene por objeto dar una visión global detallada de las actividades de normalización de seguridad realizadas por el UIT-T. Los lectores que necesiten información más detallada sobre las Recomendaciones publicadas y documentaciones conexas pueden utilizar los enlaces directos. El Manual se puede utilizar de varias maneras, y en el cuadro 1 se indica cómo atender a las necesidades de los distintos lectores.

Cuadro 1 – Cómo atiende el Manual a las necesidades de los lectores

Organización	Lectores	Necesidades	Cómo atiende el Manual a sus necesidades
Proveedores de servicios de telecomunicaciones	Altos ejecutivos/ administradores	Resumen general del alcance de las actividades de normalización Hoja de ruta de alto nivel para las normas pertinentes	El Manual atiende directamente a esas necesidades
	Ingenieros de diseño e instalación	Hoja de ruta para normas pertinentes Detalles técnicos asociados con ámbitos específicos	El Manual contiene una hoja de ruta y enlaces a explicaciones detalladas Las Recomendaciones contienen detalles técnicos
Vendedores de servicios de telecomunicaciones	Altos ejecutivos/ administradores	Resumen general del alcance de las actividades de normalización Hoja de ruta de alto nivel para las normas pertinentes	El Manual atiende directamente a esas necesidades
	Administradores de producto	Hoja de ruta para normas pertinentes	El Manual contiene una hoja de ruta y enlaces a explicaciones detalladas
	Diseño de productos	Detalles técnicos asociados con ámbitos específicos	El Manual contiene enlaces a explicaciones detalladas sobre ámbitos específicos Las Recomendaciones contienen detalles técnicos
Usuarios	Técnicos	Pueden interesarse por detalles técnicos asociados con ámbitos específicos	El Manual contiene una hoja de ruta y enlaces a explicaciones detalladas
	No técnicos	Pueden interesarse por un resumen global del alcance de las actividades de normalización	El Manual atiende directamente a esas necesidades
Sector académico	Estudiantes/ profesores	Hoja de ruta para normas pertinentes Detalles técnicos asociados con ámbitos específicos Sensibilización sobre actividades de normalización nuevas y futuras	El Manual contiene una hoja de ruta y enlaces a explicaciones detalladas sobre ámbitos específicos
Gobierno	Altos ejecutivos y administradores	Resumen general del alcance de las actividades de normalización Hoja de ruta de alto nivel para las normas pertinentes	El Manual atiende directamente a esas necesidades
	Reguladores		
	Poderes públicos		
Organizaciones no gubernamentales	Altos ejecutivos y administradores	Resumen general del alcance de las actividades de normalización Hoja de ruta de alto nivel para las normas pertinentes	El Manual atiende directamente a esas necesidades
	Desarrollo y creación de capacidades	Hoja de ruta para normas pertinentes Detalles técnicos asociados con ámbitos específicos	El Manual contiene una hoja de ruta y enlaces a explicaciones detalladas Las Recomendaciones contienen detalles técnicos

2. Resumen de las actividades del UIT-T en materia de seguridad

2 Resumen de las actividades del UIT-T en materia de seguridad

2.1 Introducción

Los trabajos del UIT-T sobre seguridad de las TIC están en curso desde hace más de dos décadas, periodo durante el cual diversas Comisiones de Estudio han elaborado Recomendaciones y directrices en algunos ámbitos fundamentales. La Comisión de Estudio 17 (CE 17) tiene actualmente la principal responsabilidad para los trabajos del UIT-T en materia de seguridad y también ha sido designada como la Comisión de Estudio rectora en seguridad. Sin embargo, los aspectos de seguridad conciernen a la mayoría de los ámbitos del trabajo del UIT-T y muchas Comisiones de Estudio están llevando a cabo tareas de seguridad relacionadas con su propio ámbito de responsabilidad.

Entre las responsabilidades como Comisión de Estudio rectora en seguridad, la CE17 ha elaborado diversas publicaciones de referencia y divulgativas. Estas publicaciones, entre las que se incluye el presente Manual, contribuyen al esfuerzo de coordinar las tareas de seguridad del UIT-T internamente, así como a promover el trabajo de una comunidad mucho más amplia y el uso de las Recomendaciones.

Esta sección contiene una visión general de las publicaciones de referencia del UIT-T y facilita un resumen gráfico de los trabajos sobre seguridad en curso.

2.2 Documentación de referencia y exteriores

El UIT-T mantiene algunas publicaciones y sitios web en los que se puede obtener información más detallada sobre las Recomendaciones y los trabajos sobre seguridad del UIT-T.

El sitio web de la CE 17, Comisión de Estudio rectora sobre seguridad, facilita un resumen de sus responsabilidades y actividades. En ese sitio web se encuentran resúmenes y enlaces a documentación y a material orientativo, información sobre anteriores cursillos, presentaciones y actividades de formación y enlaces para orientación en materia de seguridad, incluido un seminario sobre cómo elaborar programas seguros.

En el capítulo 12 se incluye información más detallada sobre diversos aspectos de los trabajos en materia de seguridad junto con enlaces directos a más información.

2.3 Resumen de los principales asuntos y Recomendaciones relativos a la seguridad

El cuadro 2 facilita una referencia rápida de algunos de los principales asuntos y de las Recomendaciones que se consideran en el presente Manual. Para los lectores que utilizan una versión electrónica del texto, se proporcionan hipervínculos directos al texto de cada asunto o subasunto y a las Recomendaciones enumeradas. El Anexo D contiene una lista completa de las Recomendaciones a las que se refiere este Manual. Los hipervínculos se incluyen en el anexo D de forma que los usuarios de la versión electrónica del texto puedan enlazar directamente para descargar las Recomendaciones.

Cuadro 2 – Visión general de algunos de los asuntos y Recomendaciones seleccionados

Tema	Subtema	Ejemplos de las Recomendaciones & publicaciones pertinentes
3. Requisitos de seguridad	3.2 Amenazas, riesgos y vulnerabilidades 3.3 Objetivos de seguridad 3.4 Razones para las normas de seguridad 3.6 Requisitos de seguridad personal y física	X.1205: Aspectos generales de la ciberseguridad E.408: Requisitos de seguridad para las redes de telecomunicaciones X.1051: Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones Tecnologías de planta externa para redes públicas Aplicación de ordenadores y microprocesadores a la construcción, instalación y protección de cables de comunicaciones
4. Arquitecturas de seguridad	4.1 Arquitectura de seguridad de sistemas abiertos 4.2 Servicios de seguridad 4.3 Arquitectura de seguridad para sistemas que proporcionan comunicaciones de extremo a extremo 4.3.2 Disponibilidad de la red y sus componentes 4.4 Directrices de implementación 4.5 Arquitecturas específicas de la aplicación	X.800: Arquitectura de seguridad de sistemas abiertos X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo X.810: Marcos de seguridad: Visión general X.Sup3: Serie ITU-T X.800-X.849 – Suplemento sobre directrices para la implementación de la seguridad entre sistemas y redes X.1162: Arquitectura y operaciones de seguridad para redes entre pares X.1161: Marco para comunicaciones seguras entre pares X.1143: Arquitectura de seguridad para seguridad de mensajes en servicios móviles de la web
5. Gestión de seguridad	5.1 Gestión de seguridad de la información 5.2 Gestión de riesgos 5.3 Tratamiento de incidentes	X.1051: Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones X.1055: Guía para la gestión de riesgos y el perfil de riesgos E.409: Estructura para organizar los incidentes y solucionar los incidentes de seguridad
6. El directorio, autenticación y gestión de identidad	6.1 Protección de la información del directorio 6.1.4 Protección de privacidad 6.2 Mecanismos de seguridad de clave pública 6.2.3 Infraestructuras de clave pública 6.4 Gestión de identidad 6.5 Telebiométrica	X.500: Visión de conjunto de conceptos, modelos y servicios X.509: El directorio: Marcos para certificados de claves públicas y atributos X.1171: Amenazas y requisitos para la protección de información identificable personalmente en las aplicaciones que utilizan la identificación basada en las etiquetas Y.2720: Marco general para la gestión de identidades en las redes de la próxima generación X.1081: Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad X.1089: Infraestructura de autenticación de telebiometría
7. Seguridad de la infraestructura de red	7.1 La red de gestión de las telecomunicaciones 7.2 Arquitectura de gestión de red 7.4 Seguridad de las actividades de supervisión y control 7.5 Seguridad de aplicaciones basadas en la red 7.6 Servicios comunes de gestión de la seguridad 7.6.4 Servicios de seguridad basados en CORBA	M.3010: Principios para una red de gestión de las telecomunicaciones X.790: Función de gestión de dificultades para aplicaciones del UIT-T X.711: Protocolo común de información de gestión X.736: Función señaladora de alarmas de seguridad X.740: Función de pista de auditoría de seguridad X.780: Directrices de la RGT para la definición de objetos gestionados CORBA
8. Algunos planteamientos específicos de la seguridad de red	8.1 Seguridad de las redes de la próxima generación (NGN) 8.2 Seguridad de comunicaciones móviles 8.3 Seguridad para redes domésticas 8.4 Requisitos de seguridad para IPCablecom 8.6 Seguridad para redes de sensores ubicuos	Y.2001: Visión general de las redes de próxima generación Y.2701: Requisitos de seguridad de la versión 1 de la red de próxima generación X.1121: Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo X.1111: Marco de tecnologías de la seguridad para redes domésticas J.170: Especificación de la seguridad de IPCablecom
9. Aplicaciones de seguridad	9.1 Voz sobre IP (VoIP) y multimedios 9.2 IPTV 9.3 Facsímil seguro 9.4 Servicios de la web 9.5 Servicios basados en etiquetas	H.235: Marco de seguridad para sistemas multimedia de la serie H X.1191: Requisitos funcionales y arquitectura de los aspectos relativos a la seguridad de la TVIP T.36: Capacidades de seguridad para su utilización con terminales facsímil del grupo 3 X.1141: Lenguaje de etiquetas de aserción de seguridad (SAML 2.0)
10. Contrarrestar amenazas comunes de red	10.1 Contrarrestar el spam 10.2 Código malicioso, programas espía y software engañoso 10.3 Notificación y diseminación de actualizaciones del software	X.1231: Estrategias técnicas contra el correo basura X.1240: Tecnologías utilizadas contra el correo basura X.1244: Aspectos globales para contrarrestar el correo basura en las aplicaciones multimedios en las redes IP X.1207: Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado X.1206: Marco independiente del proveedor para la notificación automática de información relacionada con la seguridad y para la difusión automática de actualizaciones
Para un conjunto completo de las Recomendaciones UIT-T sobre seguridad véase http://www.itu.int/ITU-T/recommendations/		

3. Requisitos de seguridad

3 Requisitos de seguridad

3.1 Introducción

Al desarrollar cualquier tipo de marco de seguridad, es muy importante tener un conocimiento claro de los requisitos. Un análisis completo de los requisitos de seguridad debe tener en cuenta: las partes implicadas; los elementos que han de protegerse; las amenazas de las que hay que proteger a esos elementos y sus vulnerabilidades; y el riesgo global para ellos debido a esas amenazas y vulnerabilidades.

La presente sección introduce los requisitos básicos para la protección de las aplicaciones, los servicios y la información de las TIC, considera las amenazas y vulnerabilidades que dan lugar a esos requisitos, examina el cometido de las normas necesarias para cumplir los requisitos e identifica alguna de las características que se precisan para proteger a las diversas partes que utilizan y explotan las instalaciones TIC.

Los requisitos de seguridad son genéricos y también dependen del contexto. Además, algunos requisitos están bien establecidos mientras que otros siguen evolucionando mediante nuevas aplicaciones y en un entorno de amenazas cambiante. En su mayor parte, el debate en esta sección es genérico. Los requisitos para aplicaciones y entornos particulares se tratan en otras secciones.

3.2 Amenazas, riesgos y vulnerabilidades

En lo que respecta a la seguridad de las TIC, en términos generales habrá que proteger los dispositivos de las siguientes partes interesadas:

- *clientes/abonados* que necesitan confiar en la red y en los servicios que se ofrecen, incluida la disponibilidad de los servicios (en particular de los servicios de emergencia);
- *comunidad/autoridades públicas* que demandan seguridad mediante directrices y/o leyes, con el fin de garantizar la disponibilidad de los servicios, la libre competencia y la protección privada; y
- *los propios operadores de red/proveedores de servicio* que precisan seguridad para salvaguardar su explotación y sus intereses económicos y para cumplir sus obligaciones con los clientes y el público, en el ámbito nacional e internacional.

Es necesario proteger los elementos siguientes:

- los servicios de comunicaciones y de informática;
- la información y los datos, incluido el soporte lógico y los datos relativos a los servicios de seguridad;
- el personal; y
- los equipos y las instalaciones.

Una *amenaza de seguridad* se define como una posible violación de la seguridad. Son ejemplos de amenaza:

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

Las amenazas pueden ser *accidentales* o *intencionadas* y pueden ser activas o pasivas. Una amenaza accidental es aquella no premeditada, como una disfunción o fallo físico de un sistema o del programa

informático. Una amenaza intencionada es aquella que una persona realiza como un acto deliberado. Las amenazas intencionadas pueden variar entre un examen casual mediante instrumentos de verificación fácilmente disponibles hasta ataques complejos que precisan conocimientos especiales del sistema. Cuando se consuma una amenaza intencionada se denomina *ataque*. Una amenaza activa es la que ocasiona un cambio de estado o de funcionamiento del sistema, por ejemplo, la alteración de los datos o la destrucción de los equipos físicos. Una amenaza pasiva no ocasiona ningún cambio de estado. Las escuchas clandestinas y la interceptación electrónica son ejemplos de amenazas pasivas.

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

Las Recomendaciones UIT-T reconocen cuatro tipos de vulnerabilidades:

- vulnerabilidades por tipo de amenaza debidas a la dificultad de prever posibles amenazas futuras;
- vulnerabilidades por diseño y especificación producidas por errores o descuidos en el diseño de un sistema o del protocolo, que los hacen inherentemente vulnerables;
- vulnerabilidades por implementación, que se producen como resultado de errores en la implementación del sistema o del protocolo; y
- vulnerabilidades por operación y configuración producidas por la utilización errónea de opciones en las implementaciones o de políticas y prácticas insuficientes de instalación (como no utilizar criptación en una red inalámbrica).

Un *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 reducirlo a un nivel aceptable. Para ello, es necesario entender las amenazas y vulnerabilidades correspondientes para aplicar las contramedidas adecuadas. Normalmente se trata de servicios y mecanismos de seguridad que se pueden complementar mediante medidas no técnicas tales como seguridad física y personal.

Aunque las amenazas y los agentes de amenaza cambian, las vulnerabilidades de seguridad perduran durante la vida del sistema o del protocolo, a menos que se tomen medidas específicas para reducirlas. Puesto que los protocolos normalizados están muy extendidos, cualquier vulnerabilidad asociada con los protocolos puede suponer implicaciones muy graves y producirse a escala mundial. Por lo tanto, reviste particular importancia comprender e identificar las vulnerabilidades en los protocolos y tomar las medidas correspondientes 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 las amenazas, los riesgos y las vulnerabilidades asociadas con el tratamiento de la información y las redes de comunicaciones, no se puede lograr una seguridad adecuada a menos que se apliquen sistemáticamente medidas de seguridad de conformidad con las políticas pertinentes, políticas que es necesario examinar y actualizar periódicamente. Además, debe garantizarse una gestión de seguridad y un tratamiento de incidentes adecuados, lo que incluye la asignación de responsabilidades y la especificación de las actuaciones que se deben realizar para prevenir, detectar, investigar y actuar frente a cualquier incidente de seguridad.

Los servicios y mecanismos de seguridad pueden proteger las redes de telecomunicaciones frente a ataques malintencionados como la negación del servicio, la escucha clandestina, la piratería, la manipulación de mensajes (modificación, retardo, supresión, inserción, reproducción, reencaminamiento, encaminamiento erróneo o reordenamiento de mensajes), el repudio o la falsificación. Las técnicas de protección incluyen la prevención, detección y recuperación tras ataques, así como la gestión de información relacionada con la seguridad. La protección también debe comprender medidas para evitar cortes de servicio debido a eventos naturales (como tormentas y terremotos) y ataques malintencionados (acciones deliberadas o violentas). Es necesario prever disposiciones que permitan las escuchas y la supervisión previa autorización de las autoridades correspondientes.

La seguridad de las redes de telecomunicaciones también exige una amplia cooperación entre los proveedores de servicio. La Recomendación UIT-T E.408, *Requisitos de seguridad para las redes de telecomunicaciones*, 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 las contramedidas que pueden adoptarse para reducir los riesgos que suponen tales amenazas. La implementación de los requisitos de la Recomendación UIT-T E.408 facilitará la cooperación internacional en los ámbitos siguientes relacionados con la seguridad de redes de telecomunicaciones:

- 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 infraestructuras y servicios críticos; y
- creación de una legislación adecuada.

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

La Recomendación UIT-T X.1205, *Aspectos generales de la ciberseguridad*, proporciona una taxonomía de las amenazas de seguridad desde un punto de vista organizativo, junto con un análisis de las amenazas en diversas capas de una red.

3.3 Objetivos generales de seguridad para las redes TIC

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 de la red;

d) todos los usuarios deben ser responsables única 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 el plan predefinido para minimizar los posibles daños;

h) cuando se detecte una violación de seguridad, debe ser posible restablecer los niveles de seguridad normales; y

i) la arquitectura de seguridad de las redes de telecomunicaciones debe proporcionar cierta flexibilidad para soportar diferentes políticas y mecanismos de seguridad.

Los objetivos (a) a (e) se pueden lograr implementando los siguientes servicios de seguridad:

- confidencialidad;
- integridad de los datos, del sistema y del programa;
- responsabilidad, incluida la autenticación, el no repudio y el control de acceso; y
- disponibilidad.

Un tipo de red TIC que está creciendo rápidamente en importancia es la red de la próxima generación (NGN). Los requisitos y objetivos de seguridad de las redes de la próxima generación se tratan en la sección 8.

3.4 Antecedentes de las normas de seguridad

La necesidad de un marco de seguridad de red genérico para las telecomunicaciones internacionales surgió de diferentes fuentes que incluyen clientes/abonados, autoridades/comunidades públicas y operadores de red y proveedores de servicio. Conviene que los requisitos de seguridad para las redes de telecomunicaciones se basen en normas internacionalmente aceptadas, puesto que promueven el acercamiento de los planteamientos y contribuyen a la interconexión, además de resultar más económico que la elaboración de planteamientos individuales para cada jurisdicción.

En algunos casos proporcionar y utilizar mecanismos y servicios de seguridad puede resultar bastante oneroso en relación con el valor de los elementos que se protegen, por lo que es importante tener la capacidad de adaptar los servicios y los mecanismos de seguridad a las necesidades locales. Sin embargo, la capacidad de adaptar la seguridad también puede dar lugar a diversas combinaciones posibles de las características de seguridad. Por lo tanto, es conveniente definir *perfiles de seguridad* que cubran una amplia gama de servicios de redes de telecomunicaciones para garantizar el alineamiento de las opciones de las diferentes implementaciones. La normalización y el uso de perfiles autorizados facilitan el interfuncionamiento y la reutilización de soluciones y productos, lo que redunda en una introducción más rápida y en un menor coste de la seguridad.

Entre los importantes beneficios de las soluciones de seguridad normalizadas, tanto para fabricantes como para usuarios del sistema, se encuentran la economía de escala en el desarrollo del producto y el interfuncionamiento de los componentes en las redes de telecomunicaciones.

3.5 Evolución de las normas de seguridad del UIT-T

El trabajo del UIT-T sobre seguridad ha evolucionado considerablemente en los últimos años como se verá en las siguientes secciones, en las que se tratan muchas de las Recomendaciones con más detalle. En la presente sección, se consideran algunos aspectos fundamentales de esa evolución, en particular los relativos a los requisitos de seguridad.

En general, los requisitos de seguridad de las TIC se definen en términos de amenazas a la red y/o al sistema, las vulnerabilidades inherentes de la red y/o del sistema y las medidas que hay que tomar para contrarrestar las amenazas y reducir las vulnerabilidades. Los requisitos de protección se aplican a la red y a sus componentes. En la Recomendación UIT-T X.800, *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones del CCITT*, 1991, se definen los conceptos fundamentales de la seguridad, incluidas las amenazas, las vulnerabilidades y las contramedidas de seguridad. La Recomendación UIT-T E.408, *Requisitos de seguridad de las redes de telecomunicaciones*, mencionada anteriormente, que se publicó en 2004, establece los conceptos y la terminología de la Recomendación UIT-T X.800. La Recomendación UIT-T E.408 es genérica por naturaleza y no identifica ni considera los requisitos para redes específicas. No se consideran nuevos servicios de seguridad. En cambio, la Recomendación se centra en la utilización de los servicios de seguridad existentes definidos en otras Recomendaciones UIT-T y en las normas pertinentes de otros organismos.

La necesidad de contrarrestar el creciente número y variedad de amenazas a la ciberseguridad (virus, gusanos, caballos de Troya, ataques pirata, suplantación de la identidad, correo indeseado y otras formas de ciberataques) se refleja en la Recomendación UIT-T X.1205, 2008, *Aspectos generales de la ciberseguridad*. Esa Recomendación pretende crear los fundamentos del conocimiento que permitan garantizar la seguridad de las futuras redes. Se tratan diversas tecnologías disponibles para contrarrestar amenazas como son: encaminadores, cortafuegos, protección antivirus, sistemas de detección de intrusiones, sistemas de protección ante intrusiones, cómputo seguro y auditorías y verificación. También se consideran principios de protección de red tales como la defensa en profundidad y la gestión de acceso. Se analizan las estrategias y técnicas de gestión de riesgos, destacando la importancia de la formación y la enseñanza en la protección de la red. También se facilitan ejemplos que ofrecen seguridad a diversas redes basados en las tecnologías consideradas.

La Recomendación UIT-T X.1205 define la ciberseguridad como una colección de instrumentos, políticas, conceptos de seguridad, salvaguardias de seguridad, directrices, planteamientos de gestión de riesgos, actuaciones, formación, prácticas idóneas, garantías y tecnologías que se pueden utilizar para proteger el entorno cibernético, la organización y los bienes de los usuarios. Los elementos referenciados incluyen dispositivos de cómputo conectados, usuarios de ordenadores, aplicaciones/servicios, sistemas de comunicaciones, comunicación multimedios y la totalidad de la información transmitida y/o almacenada en el medio cibernético. Como se define aquí, la ciberseguridad garantiza la consecución y el mantenimiento de las propiedades de seguridad de la organización (incluidas la disponibilidad, integridad y confidencialidad) y protege los bienes de un usuario frente a los riesgos de seguridad más importantes del medio cibernético.

En el entorno de trabajo actual, está desapareciendo el concepto de perímetro. Las fronteras entre redes interiores y exteriores cada vez son más "diáfanas". La seguridad debería considerarse como un proceso continuo que cubre la protección de los sistemas, las redes, las aplicaciones y los recursos. Asimismo, la seguridad debe ser completa en todas las capas de un sistema. Adaptar para la seguridad un planteamiento por capas combinado con una política fuerte de gestión y seguridad, proporciona una gama de soluciones de seguridad que puede ser modular, flexible y escalable.

Las técnicas actuales de ciberseguridad incluyen:

- la criptografía: pujante tecnología que sustenta diversos servicios de seguridad que incluyen la criptación de los datos durante la transmisión y el almacenamiento;
- los controles de acceso: destinados a restringir la capacidad de los usuarios para acceder, utilizar, ver o modificar información en ordenadores anfitriones o redes;

- la integridad del sistema: destinada a garantizar que un sistema y sus datos no son modificados ni manipulados por partes no autorizadas o de una forma no autorizada;
- las auditorías, catalogación y verificación: ayudan a los administradores de sistemas a recopilar y revisar catálogos de red durante y después de un ataque. Los datos se pueden utilizar para evaluar la efectividad de la estrategia de seguridad desplegada por la red;
- la gestión: ayuda a los administradores del sistema a analizar y establecer las configuraciones de seguridad en las redes anfitrionas o en sus propias redes. Los controles de gestión se pueden utilizar para verificar la exactitud de las configuraciones de red y de los elementos adjuntos.

3.6 Requisitos de seguridad personal y física

La mayoría de las Recomendaciones UIT-T relacionadas con la seguridad se centran en los aspectos técnicos del sistema y de la red. En la Recomendación UIT-T X.1051, *Directrices de gestión de seguridad de la información para las organizaciones de telecomunicaciones* se identifican algunos aspectos de la seguridad personal. La seguridad física también es una dimensión muy importante de la protección aunque se encuentra en gran medida fuera del ámbito del mandato del UIT-T. No obstante, los requisitos de seguridad física generales se identifican en la Recomendación UIT-T X.1051 y la seguridad física relativa a la planta exterior se considera en los dos documentos identificados a continuación.

Los requisitos de protección física para la planta exterior incluyen la necesidad de garantizar que el equipamiento es capaz de resistir la amenaza del fuego, los desastres naturales y los daños accidentales o intencionados. En las publicaciones del UIT-T *Tecnologías de planta exterior para redes públicas* (1991) y *Aplicación de ordenadores y microprocesadores a la construcción, instalación y protección de cables de telecomunicaciones* (1999) consideran métodos para lograr la protección de componentes, cables, recintos, cabinas, etc. Estos documentos también consideran la supervisión de los sistemas para evitar daños y sugieren cómo reaccionar ante los problemas y reestablecer la funcionalidad de los sistemas lo antes posible.

4. Arquitecturas de seguridad

4 Arquitecturas de seguridad

Las arquitecturas de seguridad y sus modelos y marcos asociados proporcionan una estructura y un contexto en el que se pueden elaborar con coherencia normas técnicas pertinentes. En la década de 1980 se reconoció la necesidad de un marco en el que se pudiera aplicar la seguridad en una arquitectura de comunicaciones estratificada que dio lugar a la elaboración de la *arquitectura de seguridad para sistemas abiertos* (Rec. UIT-T X.800), primera de una serie de normas arquitecturales 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 otras normas, por ejemplo con los modelos y marcos de seguridad que especifican los tipos de protección que pueden aplicarse a cada entorno.

Posteriormente, se identificó la necesidad de arquitecturas de seguridad tanto genéricas como para aplicaciones específicas. En consecuencia se elaboró la Recomendación UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*, así como algunas arquitecturas específicas de la aplicación para abordar temas como la gestión de red, las comunicaciones entre pares y los servidores móviles de la web. La Recomendación UIT-T X.805, que se describe más adelante en esta sección, sirve de complemento a otras Recomendaciones de la serie X.800 con soluciones para la seguridad de las redes de extremo a extremo.

4.1 Arquitectura de seguridad de sistemas abiertos y normas relacionadas

La primera arquitectura de seguridad de comunicaciones normalizada fue la arquitectura de seguridad de sistemas abiertos de la Recomendación UIT-T X.800. En esa Recomendación se definen los elementos de la arquitectura de seguridad que pueden aplicarse según los requisitos de protección y, en concreto, presenta una descripción general de los servicios de seguridad y los mecanismos que son necesarios. También se define, mediante el modelo de referencia básico de la interconexión de sistemas abiertos (OSI), el lugar más apropiado (es decir, la capa) en el que se deberían implantar los servicios de seguridad.

La Recomendación 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 ninguna medida de seguridad adicional que pueda ser necesaria en los sistemas extremos para soportar las características de seguridad de comunicaciones.

Aunque UIT-T 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, auditoria* y *recuperación de seguridad*. También indica qué mecanismos de seguridad se pueden utilizar para proporcionar los servicios de seguridad. Antes de la publicación de la Recomendación UIT-T X.800 había una gran divergencia de opiniones sobre los servicios de seguridad básicos necesarios y las funciones de cada uno de ellos. UIT-T X.800 es el fruto de un consenso internacional muy amplio sobre estos servicios.

El valor y la aplicabilidad general de esa Recomendación 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 la Recomendación UIT-T 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.

4.2 Servicios de seguridad

Los marcos de seguridad son representaciones completas y uniformes de todos los servicios de seguridad definidos en la Recomendación UIT-T X.800. El objetivo de estas normas 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 prestar 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.

La Recomendación UIT-T X.810, *Marcos de seguridad para sistemas abiertos: Visión general*, presenta otros marcos y describe conceptos comunes como 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.

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 la norma UIT-T 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* (Recomendación UIT-T X.811) 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.

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* (Recomendación UIT-T X.812) describe un modelo que incluye todos los aspectos del control de acceso en los sistemas abiertos, su relación con otras funciones de seguridad (como la autenticación y la auditoria), y los requisitos de gestión del control de acceso.

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 la Recomendación UIT-T 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* (Recomendación UIT-T X.813) amplía los conceptos de los servicios de seguridad de no repudio descritos en la Recomendación UIT-T 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.

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* (Recomendación UIT-T X.814) 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.

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. El *marco de integridad* (Recomendación UIT-T X.815) considera 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, los requisitos de gestión y los servicios conexos necesarios para de cada clase de mecanismo. (Cabe destacar que, aunque las normas de arquitectura de seguridad se centran fundamentalmente en la integridad de los datos, también son importantes para la seguridad otros aspectos de la integridad, como la integridad de sistema.)

4.3 Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

En 2003, tras un análisis más detallado de la arquitectura de seguridad de redes, se aprobó la Recomendación UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*. Esta arquitectura, que se basa en algunos de los conceptos de la Recomendación UIT-T X.800 y en los marcos de seguridad explicados anteriormente, puede aplicarse a distintos tipos de redes y es independiente de la tecnología que utilice la red.

4.3.1 Elementos de la arquitectura UIT-T X.805

La arquitectura X.805 se define teniendo en cuenta tres conceptos principales, a saber las capas, los planos y las dimensiones de seguridad para una red extremo a extremo. El sistema de capas y planos proporciona una perspectiva jerárquica de la seguridad extremo a extremo de la red, basada en la seguridad capa por capa y plano a plano, que se consigue diseñando medidas de seguridad en cada una de las dimensiones de seguridad para solventar las amenazas específicas. La figura 1 muestra los elementos de esa arquitectura.

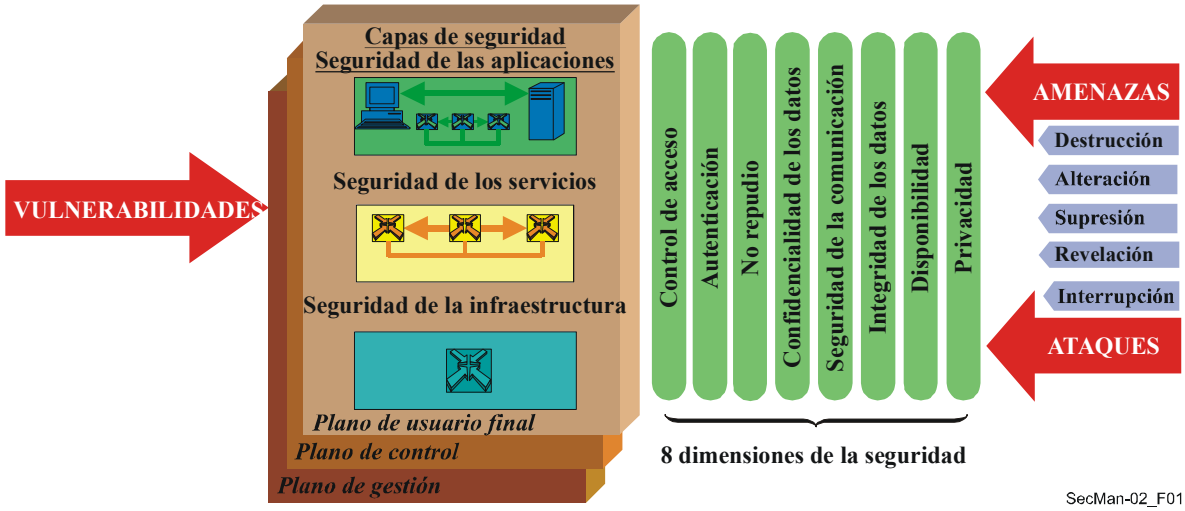


Figura 1 – Elementos de la arquitectura de seguridad de la Rec. UIT-T X.805

En la Recomendación UIT-T X.805, una *dimensión de seguridad* es un conjunto de medidas de seguridad diseñadas para tratar un determinado aspecto de la seguridad de red. Los servicios de seguridad básicos de la Recomendación UIT-T X.800 (*control de acceso, autenticación, confidencialidad de los datos, integridad de los datos y no repudio*) reflejan las funciones de las correspondientes *dimensiones de seguridad* UIT-T X.805 (que se muestran en la figura 1). Además, la Recomendación UIT-T X.805 introduce tres dimensiones (*seguridad de las comunicaciones, disponibilidad y privacidad*) que no figuran en la Recomendación UIT-T X.800. Estas dimensiones ofrecen más protección para la red y protegen de las principales amenazas de seguridad. Estas dimensiones no están limitadas a la red sino que incluyen aplicaciones e información de usuario final. Las dimensiones de seguridad aplican a los proveedores de servicio o a empresas que ofrecen servicios de seguridad a sus clientes.

Las ocho dimensiones de seguridad de la Recomendación UIT-T X.805 son:

- la dimensión *control de acceso* que protege contra la utilización no autorizada de recursos de red y garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones;
- la dimensión *autenticación* que confirma la identidad de las entidades comunicantes, 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 *no repudio* que proporciona los medios para impedir 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). También 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 *confidencialidad de los datos* que impide la divulgación no autorizada de los datos y garantiza que las entidades no autorizadas no pueden entender el contenido de los datos;
- la dimensión *seguridad de la comunicación* que garantiza que los flujos de información sólo tienen lugar entre puntos extremos autorizados, es decir, la información no puede desviarse ni ser interceptada cuando fluye entre estos dos puntos extremos;

- la dimensión *integridad de los datos* que garantiza que los datos están protegidos contra las acciones no autorizadas de modificación, supresión, creación y copia y proporciona un aviso cuando surgen actividades que pueden comprometer la integridad de los datos;
- la dimensión *disponibilidad* que 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; y
- la dimensión *privacidad* que 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.

Como se muestra en la figura 1, además de las dimensiones de seguridad, la Recomendación UIT-T X.805 define tres capas y tres planos de seguridad. Para facilitar una solución de seguridad de extremo a extremo, se deben aplicar las capas de seguridad a una jerarquía de equipos de red y a agrupaciones de dispositivos, conocidas como *capas de seguridad.* Un *plano de seguridad* representa cierto tipo de actividad de red protegida por dimensiones de seguridad. Cada plano de seguridad representa un tipo de actividad de red protegida. 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. Las tres capas son:

- la capa *infraestructura* que comprende los dispositivos de transmisión de red, así como los elementos que la componen. Por ejemplo, son parte de esta capa los encaminadores, los centros de conmutación y los servidores y los enlaces de comunicación entre ellos;
- la capa *servicios* que tiene que ver con la seguridad de los servicios de red que se prestan a los clientes, desde servicios básicos de transporte y conectividad, como las líneas arrendadas, hasta los servicios de valor añadido como la mensajería instantánea; y
- la capa *aplicaciones* que 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 más sofisticadas como la colaboración en vídeo, en la que se utilizan transferencias de vídeo de mucha mayor definición, por ejemplo para la prospección petrolera, el diseño de automóviles, etc.

Los 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 los usuarios finales. Las redes se deben diseñar de forma que los eventos de un plano de seguridad estén aislados de los otros planos de seguridad.

Los planos de seguridad son:

- el plano de *gestión* que tiene que ver con las actividades, operaciones, administración, mantenimiento y suministro como aprovisionar a un usuario o una red;
- el plano de *control* que se relaciona con los aspectos de señalización necesarios para establecer (y modificar) la comunicación de extremo a extremo a través de la red, sin importar el medio y la tecnología utilizados en ella; y
- el plano de *usuario final* que tiene que ver con la seguridad cuando el abonado accede y utiliza la red. Este plano también considera la seguridad de flujos de datos del usuario final.

La arquitectura UIT-T X.805 puede utilizarse como referencia para las políticas de seguridad, las arquitecturas tecnológicas y los planes de respuesta ante incidentes y recuperación. La arquitectura también puede servir de base para una evaluación de la seguridad. Una vez implantado, es necesario mantener el programa de seguridad, es decir, adaptarlo al entorno de amenazas cambiante. La arquitectura de seguridad X.805 puede contribuir al mantenimiento de un programa de seguridad, al garantizar que las modificaciones del programa tienen en cuenta las dimensiones de seguridad correspondientes en cada capa y cada plano de seguridad.

Aunque la arquitectura de la Recomendación UIT-T X.805 es de seguridad de red, algunos de los conceptos se pueden ampliar a los dispositivos de usuario final. El asunto se considera en la Recomendación UIT-T X.1031, *Cometidos de los usuarios finales y de las redes de telecomunicaciones en la arquitectura de seguridad*.

4.3.2 Disponibilidad de la red y de sus componentes

La disponibilidad de la red es un aspecto importante de la seguridad de las TIC. Como se ha indicado anteriormente, el objeto de la dimensión de seguridad *disponibilidad* de la Recomendación UIT-T X.805 es garantizar la continuidad del servicio y autorizar el acceso a los elementos, información y aplicaciones de red. En esta dimensión también se incluyen las soluciones de recuperación ante desastres.

La capa de seguridad de infraestructura está constituida por las instalaciones de transmisión de la red, así como por elementos de red individuales protegidos por las dimensiones de seguridad. La capa de infraestructura representa los elementos de construcción fundamentales de las redes, sus servicios y aplicaciones. Entre los ejemplos de componentes que pertenecen a la capa de infraestructura se incluyen los encaminadores, los conmutadores y los servidores, así como los enlaces de comunicación entre ellos.

Son numerosos y diversos los requisitos funcionales, de implementación y operacionales para limitar los riesgos y las consecuencias de la falta de disponibilidad de los recursos de red. También son numerosos los factores que han de considerarse, por ejemplo, las características de los errores, el control de congestiones, la notificación de fallos y las acciones correctivas. La Recomendación UIT-T G.827, *Parámetros y objetivos de disponibilidad para trayectos digitales internacionales de extremo a extremo de velocidad binaria constante*, define los parámetros y objetivos de calidad de la red para los elementos de trayecto y la disponibilidad de extremo a extremo de trayectos internacionales digitales de velocidad binaria constante. Estos parámetros son independientes del tipo de red física que sustenta el trayecto de extremo a extremo. El anexo A a la Recomendación UIT-T G.827 ofrece directrices detalladas sobre las metodologías para evaluar la disponibilidad de extremo a extremo y proporciona ejemplos de topologías de trayecto y de cálculos de disponibilidad de los trayectos de extremo a extremo. Otras Recomendaciones que tratan las características de calidad de las redes son: UIT-T G.1000, *Calidad de servicio de comunicaciones: marco y definiciones*; UIT-T G.1030, *Estimación de las características de funcionamiento de extremo a extremo en redes IP para aplicaciones de datos*; UIT-T G.1050, *Modelo de red para evaluar las características de funcionamiento de transmisión multimedios por el protocolo de Internet* y UIT-T G.1081, *Puntos de control de calidad de funcionamiento de la IPTV*.

4.4 Directrices de implementación

Las normas de arquitectura de seguridad del UIT-T forman parte de la serie de Recomendaciones UIT-T X.800-849 sobre seguridad. En un suplemento de esta serie de Recomendaciones (X Sup. 3, UIT-T X.800-X.849 – *Suplemento sobre directrices para la implementación de la seguridad en sistemas y de redes*) se proporcionan directrices de implementación. Este suplemento facilita directrices para actividades críticas durante el ciclo de vida de la seguridad de la red. Estas directrices consideran cuatro ámbitos: política de seguridad técnica; identificación de elementos jerárquicos; amenazas, vulnerabilidades y mitigaciones basadas en elementos jerárquicos; y evaluación de la seguridad. Las directrices y sus plantillas asociadas pretenden permitir la implementación sistemática de la planificación, análisis y evaluación de la seguridad de las redes.

4.5 Algunas arquitecturas específicas de la aplicación

En esta sección, se introducen aspectos de algunas arquitecturas relativas a aplicaciones específicas.

4.5.1 Comunicaciones entre pares

Entre pares (P2P) es una instanciación de arquitecturas de red en la que todos los pares tienen autoridad y responsabilidades equivalentes, en comparación con el modelo cliente/servidor. En el caso de las comunicaciones P2P, un par puede ser a la vez el servidor y el cliente. Cuando los datos o mensajes se intercambian en una red P2P, un par comunica con otros pares directamente. Puesto que el tráfico y el tratamiento se distribuyen para cada par, la red P2P no precisa gran capacidad de cálculo ni de una red de banda ancha.

La red P2P es una red superpuesta por encima de la red de telecomunicaciones e Internet. Aprovecha las diversas conectividades entre nodos y la capacidad de cálculo y de almacenamiento disponible en cada nodo, en lugar de los recursos convencionales centralizados.

Con los rápidos adelantos de las redes de telecomunicaciones y de las tecnologías de cómputo, se puede disponer de mucha más información y de muchos más recursos de cálculo en los nodos distribuidos que a partir de un número limitado de servidores centralizados.

Las redes P2P normalmente se utilizan para conectar nodos a través de conexiones ad hoc. Estas redes son útiles para muchos fines. Es muy común compartir archivos de datos que contienen audio, vídeo, texto o cualquier cosa en formato digital. Los datos de comunicaciones en tiempo real, tales como el tráfico telefónico, también utilizan la tecnología P2P.

4.5.1.1 Arquitectura de seguridad y operaciones para redes entre pares

En la Recomendación UIT-T X.1162 se describe un modelo general de arquitectura relacionado con la seguridad que se puede aplicar a diversas redes P2P.

La figura 2 muestra una arquitectura básica de servicio P2P. La información procesada por cada par se intercambia directamente entre los usuarios. Debido a que no existe un servidor central para almacenar la información, cada par precisa encontrar qué pares disponen de datos de interés antes de ser poder recuperarlos. Además, cada par tiene que permitir el acceso a otros pares para posibilitar el intercambio de los datos.

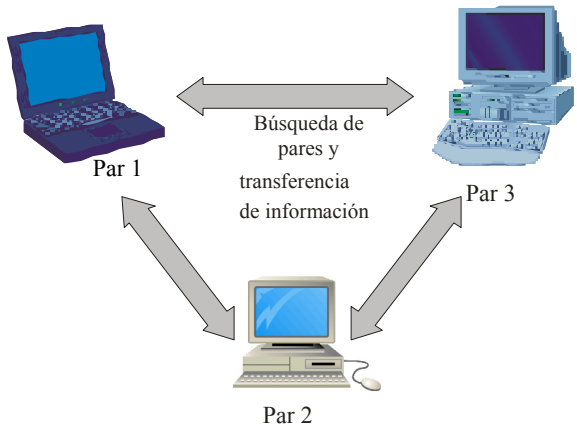


Figura 2 – Arquitectura de servicio P2P

La figura 3 muestra la arquitectura de red P2P física y lógica. En la red P2P física, un usuario puede unirse a los servicios P2P a través de un dispositivo. Generalmente el término "par" se utiliza para representar al usuario o a un dispositivo propiedad de este. Los tipos de conexión entre las entidades en una red P2P se pueden categorizar de la forma siguiente:

- conexión con un par dentro del dominio;
- conexión con un par fuera del dominio; y
- conexión con un par proveedor de servicio situado en otro dominio de red.

La figura 3 también muestra la arquitectura de red P2P lógica como una red virtual situada por encima de la capa de transporte. Se supone que la operación de cada par no está limitada por la arquitectura de la red física y que un par puede comunicar con cualquier otro par independientemente de su ubicación (si es preciso, mediante la ayuda de un superpar). La estructura de la red entre pares se divide en dos estratos: el estrato superpuesto P2P y el estrato de transporte. El estrato de transporte es el responsable de transferir los paquetes desde y hacia la capa superior y el estrato superpuesto es responsable de prestar los servicios P2P.

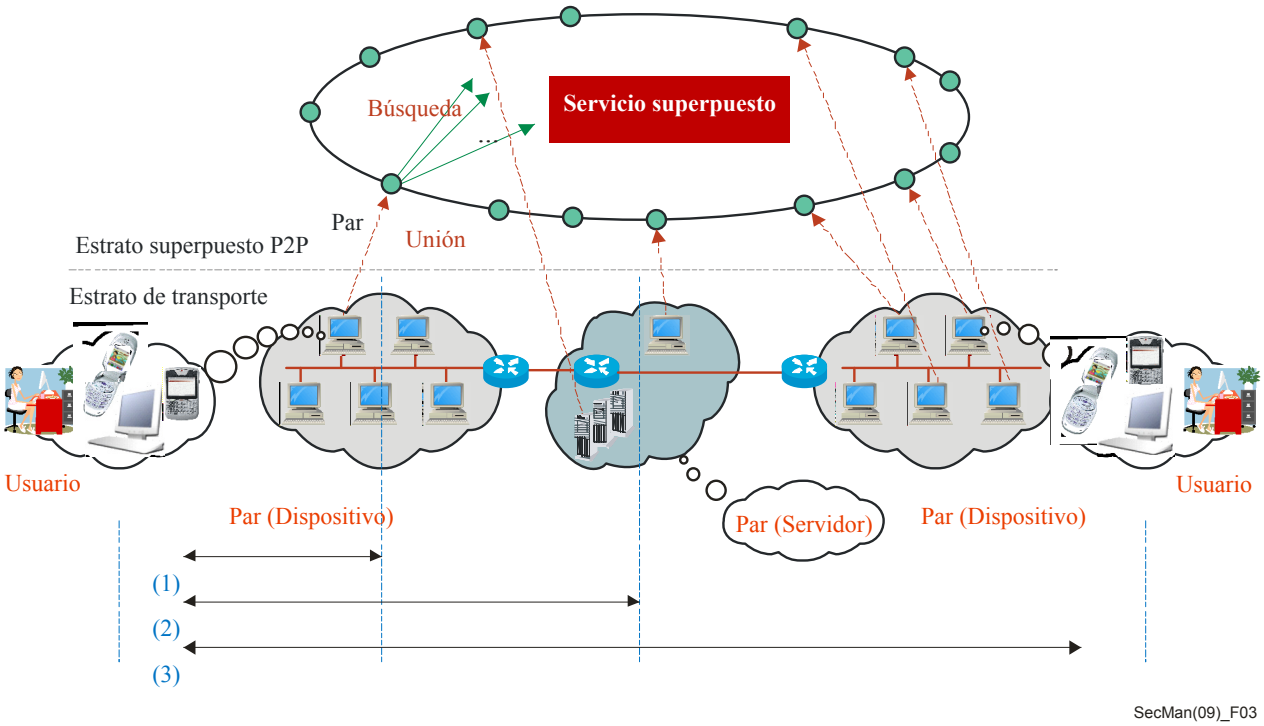


Figura 3 – Modelo de referencia arquitectónico para la red P2P

4.5.1.2 Marco para comunicaciones seguras entre pares

Los requisitos de seguridad para redes P2P, junto con los servicios y mecanismos necesarios para satisfacer esos requisitos se especifican en la Recomendación UIT-T X.1161, *Red para comunicaciones seguras entre pares*.

Entre las amenazas para las comunicaciones P2P se encuentran las escuchas clandestinas, la interferencia deliberada, la introducción y modificación, el acceso no autorizado, el repudio, los ataques de intermediarios y los ataques Sybil. En el cuadro 3 se muestran las contramedidas a las amenazas P2P.

Cuadro 3 – Relación entre los requisitos de seguridad P2P y las contramedidas

Funciones / Requisitos	Cifrado	Intercambio de claves	Firma digital	Gestión de confianza	Control de acceso	Mecanismo de integridad de los datos	Intercambio de autenticación	Notarización	Encaminamiento seguro	Mecanismo de control de tráfico	Asignación de ID
Autenticación du usuario	X	X	X	X	X		X				X
Anonimato	X			X							X
Privacidad	X				X		X				
Integridad de los datos	X	X	X		X	X	X				
Confidencialidad de los datos	X	X			X		X				
Control de acceso					X		X				X
No repudio			X				X	X			X
Usabilidad					X						
Disponibilidad					X		X		X	X	
Trazabilidad			X						X		X
Control de tráfico		X								X	

4.5.2 Arquitectura de seguridad para la seguridad de mensajes en los servicios móviles por Internet

La arquitectura de seguridad y los escenarios para la seguridad de los mensajes en servicios móviles por Internet se describen en la Recomendación UIT-T X.1143, *Arquitectura de seguridad para la seguridad de mensajes en los servicios móviles por Internet*. Esta norma proporciona:

- una arquitectura de seguridad para la seguridad de los mensajes que se basa en mecanismos de política de servicio de la red adecuados;
- mecanismos de interfuncionamiento y escenarios de servicio entre aplicaciones que soportan la totalidad de las pilas de protocolos de seguridad de los servicios de red y las aplicaciones heredadas que no soportan toda la pila de protocolos de seguridad de servicios de red;
- mecanismos de autenticación, integridad y confidencialidad de los mensajes;
- un mecanismo de filtrado de mensajes basado en el contenido de los mismos; y
- una arquitectura de seguridad de los mensajes de referencia y escenarios de servicio de seguridad.

La figura 4 ilustra la arquitectura de seguridad de la Recomendación UIT-T X.1143 para los servicios móviles por Internet.

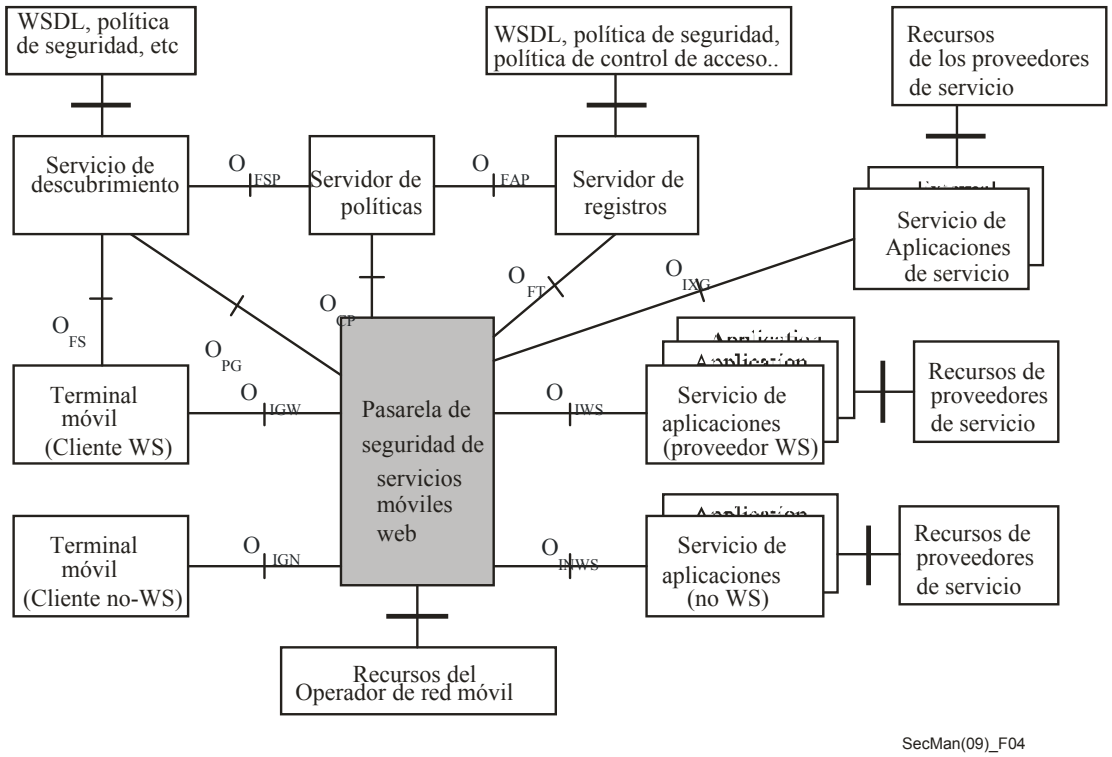


Figura 4 – Arquitectura de seguridad para servicios móviles por Internet

La arquitectura de seguridad está constituida por los componentes siguientes:

- terminales móviles, que son clientes de los servicios móviles por Internet;
- una pasarela de seguridad de servicios móviles por Internet (MWSSG). Todas las solicitudes de los clientes móviles se envían a la MWSSG que también facilita el control de acceso;
- el servidor de políticas que gestiona las políticas de seguridad relativas al tratamiento de seguridad de los mensajes y las políticas de control de acceso para los mensajes;
- el servicio de aplicación que facilita diversos servicios de valor añadido a los clientes;
- el servicio de descubrimiento, que almacena la información de interfaz para los servicios de aplicación y las políticas de seguridad conexas para el acceso de los clientes a los servicios de aplicación; y
- el servidor de registro, que reside en el dominio interno de un operador móvil y gestiona la información de interfaz para los servicios de aplicación, las políticas de seguridad correspondientes para el acceso de los clientes a los servicios de aplicación y las políticas de control de acceso relativas a los servicios objetivo.

4.6 Otras arquitecturas y modelos de seguridad de red

En este documento se consideran más adelante otros aspectos de las arquitecturas de seguridad de red. En particular, véanse las cláusulas 7.2 Arquitectura de gestión de red; 8.1 Seguridad de las redes de la próxima generación (NGN); 8.4.1 Arquitectura de IPCablecom; 8.5.1 Arquitectura IPCablecom2; y 9.2 IPTV.

5. Aspectos de la gestión de seguridad

5 Aspectos de la gestión de seguridad

La gestión de seguridad es un tema amplio que engloba muchas actividades asociadas con el control y la protección del acceso a los recursos de sistemas y redes, la supervisión de eventos, la notificación, la política y la auditoría, así como la gestión de la información relativa a esas funciones y actividades. En esta sección se consideran algunas de las actividades genéricas de la gestión de seguridad. Las actividades de la gestión de seguridad relativas a la seguridad de las infraestructuras de red se tratan en la sección 7.

5.1 Gestión de seguridad de la información

La información, como otros elementos, contribuye de forma fundamental a las actividades de la organización. La información se puede imprimir, almacenar electrónicamente, transmitir por correo, transferir de forma electrónica, en películas, en una conversación o se puede transmitir por otros medios. Independientemente de la forma o funcionalidad de la información o de los medios mediante los que se comparte o almacena, siempre debería estar adecuadamente protegida.

Una vez violada la seguridad de la información, por ejemplo mediante un acceso no autorizado a un sistema de tratamiento de la información de la organización, esta puede sufrir daños importantes. Por lo tanto, es fundamental para una organización garantizar la seguridad de su información implementando un proceso de gestión de seguridad estructurado.

La gestión eficaz de la seguridad de la información se logra implantando un conjunto adecuado de controles. Estos controles, que se aplican a las instalaciones de telecomunicaciones, los servicios y las aplicaciones, se deben establecer, implementar, comprobar, revisar y mejorar continuamente. Si no se logra desplegar eficazmente controles de seguridad, la organización puede no cumplir sus objetivos de seguridad y de negocio.

Las organizaciones de telecomunicaciones cuyas instalaciones son utilizadas por abonados, cuando traten información que pueda incluir datos personales, datos confidenciales y datos sensibles para la empresa, deben garantizar un nivel adecuado de protección a fin de evitar poner en peligro la información, es decir, necesitan establecer un sistema eficaz de gestión de seguridad de la información (IMSM).

La especificación de sistema ISMS más ampliamente reconocida es la que se define en la serie de normas ISMS ISO/CEI 27000 que incluye normas sobre los fundamentos y requisitos ISMS, un código de prácticas, directrices de implementación y asuntos conexos. El UIT-T y la ISO/CEI han elaborado conjuntamente la Recomendación UIT-T X.1051 | ISO/CEI 27011, *Directrices para la gestión de la seguridad de la información para organizaciones de telecomunicaciones*, basada en la norma ISO/CEI 27002, el Código de Prácticas ISMS.

La Recomendación UIT-T X.1051 establece directrices y los principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en organizaciones de telecomunicaciones y proporciona una base para la gestión de seguridad de la información con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de las instalaciones y servicios de telecomunicaciones. Se incluyen directrices específicas para el sector de las telecomunicaciones sobre los temas siguientes.

- organización de la seguridad de la información;
- gestión de activos;
- seguridad de los recursos humanos;
- seguridad física y medioambiental;
- gestión de comunicaciones y explotación;

- control de acceso;
- adquisición de sistemas de información;
- desarrollo y mantenimiento;
- gestión de incidentes; y
- gestión de continuidad del negocio.

Además de la aplicación de los objetivos y controles de seguridad descritos en la Recomendación UIT-T X.1051, las organizaciones de telecomunicaciones también deben tener en cuenta los asuntos de seguridad específicos siguientes:

- se debe proteger la información relacionada con las organizaciones de telecomunicaciones para impedir su divulgación no autorizada. Esto implica no divulgar información notificada en relativa a la existencia, contenido, origen, destino, fecha y hora;
- debería controlarse la instalación y uso de los dispositivos de telecomunicaciones para garantizar la autenticidad, precisión y compleción de la información transmitida, reenviada o recibida por cable, radio o cualquier otro método; y
- todo acceso a la información, instalaciones y el medio de telecomunicación utilizado para la prestación de servicios de comunicaciones tiene que ser autorizado y debería facilitarse sólo cuando sea preciso. Como ampliación de las disposiciones de disponibilidad, las organizaciones de telecomunicaciones deberían dar preferencia a las comunicaciones esenciales en casos de emergencia y cumplir con los requisitos reglamentarios.

Es necesario gestionar la seguridad de la información en las organizaciones de telecomunicaciones independientemente del medio o modo de transmisión. Si la gestión de seguridad de la información no se implanta adecuadamente, se asumirán mayores riesgos al utilizar el sistema.

Las organizaciones de telecomunicaciones prestan sus servicios como intermediarios transfiriendo datos de otros usuarios, tanto de organismos como individuales. Por lo tanto, se debe tener en cuenta que en una organización de telecomunicaciones a las instalaciones de tratamiento de la información acceden no sólo sus propios empleados y contratistas, sino también diversos usuarios externos a la organización.

Si se tiene en cuenta que los servicios e instalaciones de telecomunicación pueden compartirse y/o pueden estar interconectados con otros proveedores de servicio, la gestión de seguridad de la información en organizaciones de telecomunicaciones tiene que ampliarse a todas y cada una de las dependencias de infraestructura de red, aplicaciones de servicios e instalaciones.

5.2 Gestión de riesgos

La gestión de riesgos es un proceso para evaluar y cuantificar los riesgos y tomar medidas para garantizar que el riesgo residual se encuentra por debajo de un nivel predeterminado aceptable. Este asunto se introdujo brevemente en la sección 3 al tratar la Recomendación UIT-T X.1205, *Aspectos generales de la ciberseguridad*. En la Recomendación UIT-T X.1055, *Gestión de riesgos y el perfil de riesgos para organizaciones de telecomunicación*, se encuentran directrices más detalladas sobre la gestión de riesgos que identifican los procesos y técnicas para reducir los riesgos de seguridad de la información. Estos procesos y técnicas se pueden utilizar para evaluar los requisitos y riesgos de seguridad de las telecomunicaciones y para contribuir a seleccionar, implementar y actualizar los controles pertinentes con el fin de mantener el nivel de seguridad requerido.

Se han desarrollado muchas metodologías específicas para tratar la gestión de riesgos. La Recomendación UIT-T X.1055 proporciona los criterios para evaluar y seleccionar las metodologías adecuadas para una

organización de telecomunicaciones. No obstante, no propone ninguna metodología específica para la gestión de riesgos.

El proceso de gestión de riesgos se muestra en la figura 5.

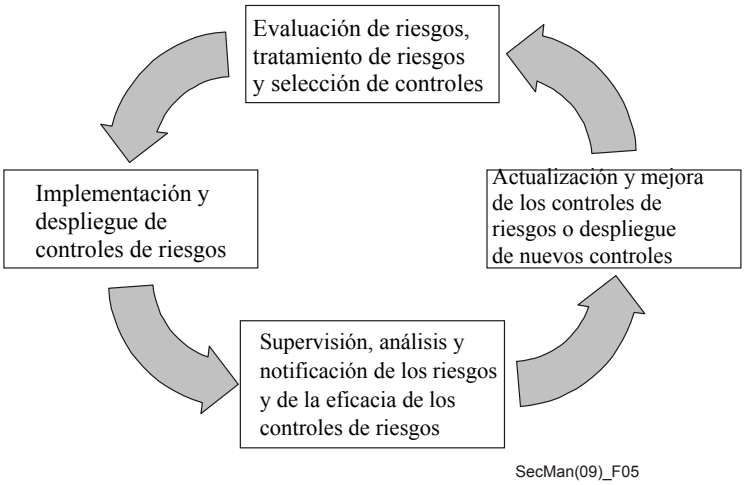


Figura 5 – Proceso de gestión de riesgos de la Recomendación UIT-T X.1055

Los perfiles de riesgo se utilizan para dirigir el proceso de gestión de riesgos en su conjunto. En particular, se utilizan para contribuir al proceso de toma de decisiones y ayudar a establecer prioridades entre los riesgos en función de su criticidad y ayudar a determinar la asignación de recursos y contramedidas. También pueden contribuir al desarrollo de los parámetros pertinentes y se pueden utilizar junto a otros instrumentos tales como las metodologías de análisis de carencias. La Recomendación UIT-T X.1055 proporciona directrices para el desarrollo de los perfiles de riesgo e incluye una plantilla y algunos ejemplos de esos perfiles.

5.3 Tratamiento de incidentes

Una parte rutinaria de la gestión de seguridad es la coherencia en la detección, respuesta y difusión de la información sobre incidentes relacionados con la seguridad. Mientras todos esos incidentes no sean adecuadamente evaluados y manejados, las organizaciones serán vulnerables a ataques posteriores, probablemente más graves.

A menos que se disponga de un procedimiento de tratamiento de incidentes, cuando se detecta un incidente relacionado con la seguridad, puede que no se realice la notificación o el análisis adecuados del incidente. Puede también que no existan procedimientos para determinar la magnitud u obtener asistencia técnica o dirección de gestión, aunque los problemas producidos por esos incidentes a menudo tienen ramificaciones que van más allá de las tecnologías de la información y de las redes. Por ejemplo, los incidentes pueden implicar riesgos legales, financieros o de reputación o pueden tratar asuntos de responsabilidad legal. La falta de procedimientos eficaces para el tratamiento de incidentes puede provocar una solución rápida, en lugar de considerar adecuadamente el problema, documentarlo y notificarlo, en cuyo caso existe el riesgo de sufrir posteriormente problemas más graves.

Cada vez más las organizaciones están más sensibilizadas sobre la necesidad de una gestión de seguridad eficaz y coherente de las redes y operaciones, por lo que el tratamiento de los incidentes es cada vez más una práctica rutinaria. Una unidad o grupo adecuadamente entrenado y responsabilizado puede manejar los incidentes de seguridad de forma oportuna y correcta.

Para tratar y notificar adecuadamente los incidentes, es preciso comprender cómo se detectan, gestionan y resuelven. Al establecer una estructura general para el tratamiento de incidentes (es decir, incidentes físicos, administrativos u organizativos y lógicos) es posible obtener una visión general de la estructura y flujo de un incidente. La Recomendación UIT-T E.409, *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones*, proporciona una visión general y un marco que ofrece directrices para la planificación de una organización con el fin de detectar y manejar los incidentes relativos a la seguridad. Es genérico por naturaleza y no identifica ni considera requisitos para redes específicas.

Es fundamental una terminología coherente cuando se notifican o manejan incidentes. El uso de terminología diferente puede dar lugar a malentendidos que pueden resultar en que un incidente de seguridad no reciba la atención adecuada ni se trate con la prontitud necesaria con el fin de reducirlo y evitar su repetición. Además, la definición de lo que se considera un incidente puede variar entre las profesiones, las organizaciones y las personas. La Recomendación UIT-T E.409 pretende normalizar la detección de incidentes y la terminología de notificación y también clasificar los incidentes en función de su gravedad, como se ilustra en la figura 6.

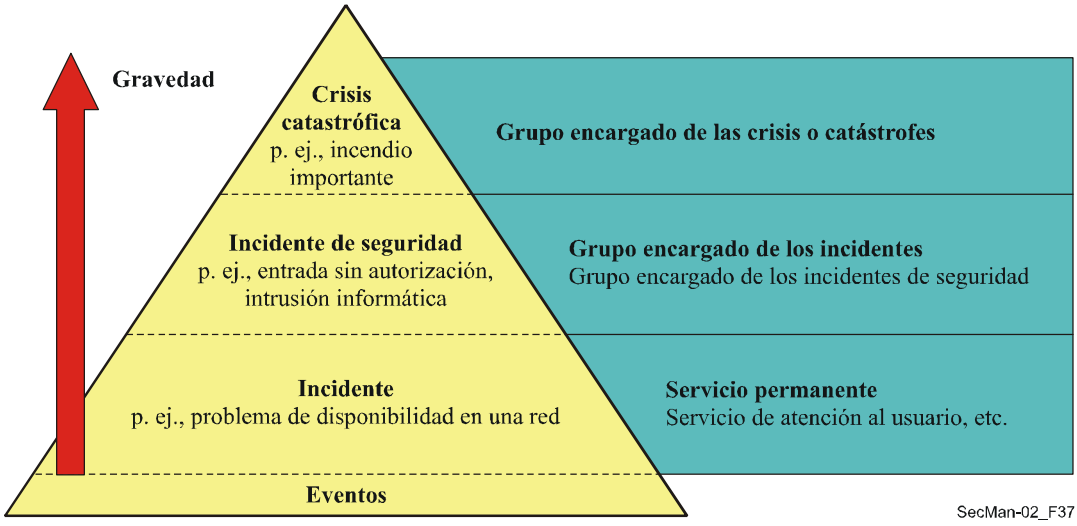


Figura 6 – Pirámide de eventos e incidentes de la Recomendación UIT-T E.409

La Recomendación UIT-T E.409 también define una estructura de tratamiento de incidentes (como se muestra en la figura 7) y establece procedimientos para detectar, clasificar, evaluar, tratar y hacer un seguimiento de los incidentes.

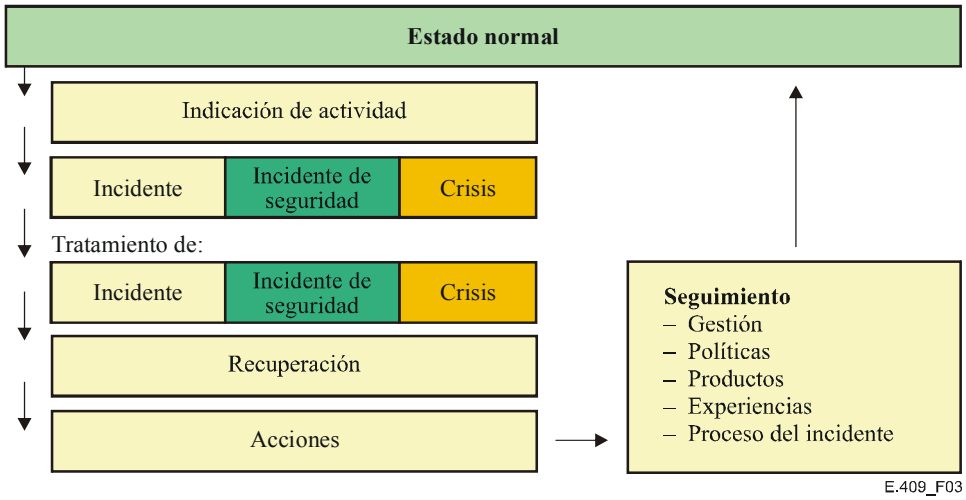


Figura 7 – Estructura para tratar los incidentes de la Recomendación UIT-T E.409

La recién aprobada Recomendación UIT-T X.1056, *Directrices para la gestión de incidentes de seguridad para las organizaciones de telecomunicaciones*, se basa en las directrices facilitadas en la Recomendación UIT-T E.409. Las organizaciones de telecomunicación necesitan procesos para el tratamiento de incidentes y para evitar su reaparición. En la Recomendación UIT-T X.1056 se describen cinco procesos de gestión de incidentes de alto nivel junto con la relación con la gestión de seguridad. Estos se muestran en la figura 8 y en la figura 9.

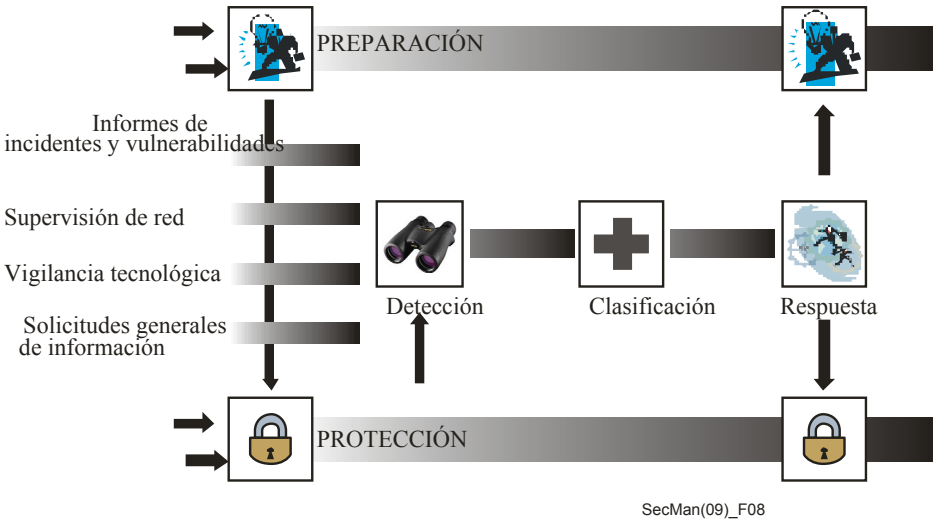


Figura 8 – Los cinco procesos de alto nivel para la gestión de incidentes

(Origen: Visión general de SEI MOSAIC: Informe técnico CMU/SE-2004-TR-015 – Definición de los procesos de gestión de incidentes para los CSIRT: una tarea en marcha)

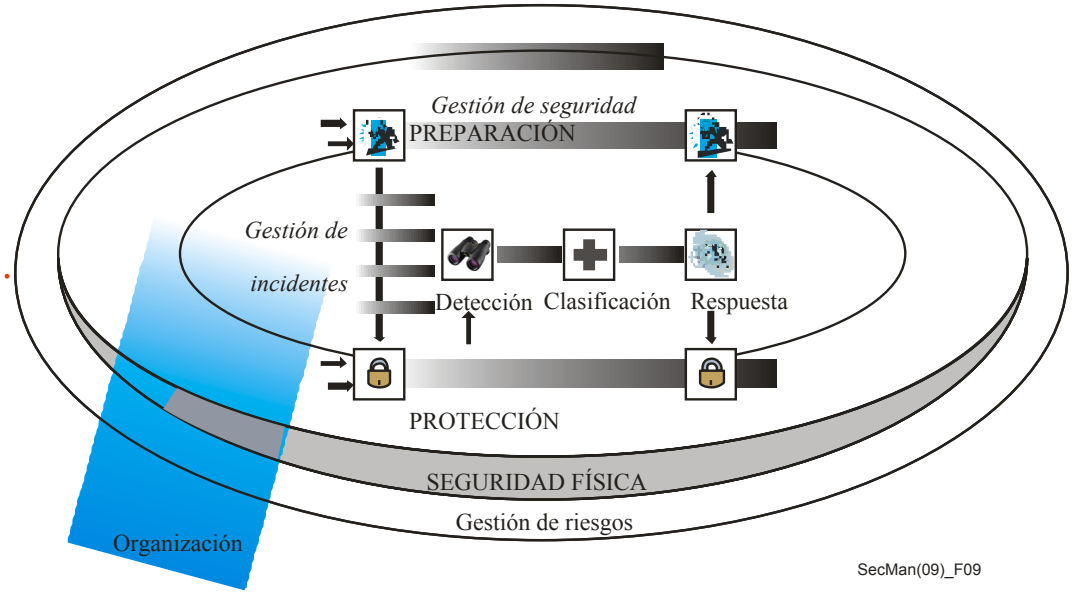


Figura 9 – Comparación de la gestión de incidentes y de la gestión de seguridad

(Origen: Visión general de SEI MOSAIC: Informe técnico CMU/SE-2004-TR-015 – Definición de los procesos de gestión de incidentes para los CSIRT: una tarea en marcha)

Además, la Recomendación UIT-T X.1056 identifica una gama de los servicios de gestión de calidad reactivos, proactivos y de seguridad que puede proporcionar un equipo de gestión de incidentes de seguridad.

6. El directorio, autenticación y gestión de identidad

6 El directorio, autenticación y gestión de identidad

En general, el término directorio se utiliza para indicar un conjunto organizado de información o archivos que se pueden consultar para obtener información específica. En el UIT-T y, de forma más general, en el contexto de la seguridad y de la normalización de las telecomunicaciones, el término *el directorio* se refiere a un depósito de información basado en la serie de Recomendaciones UIT-T X.500 que se desarrollaron conjuntamente con las normas ISO/CEI. El directorio, que se introduce en la Recomendación UIT-T X.500, *El directorio: Visión de conjunto de conceptos, modelos y servicios*, y se detalla en las Recomendaciones UIT-T X.501, *El directorio: Modelos*, UIT-T X.509, *El directorio: Marcos para certificados de claves públicas y atributos*, y UIT-T X.519, *El directorio: Especificaciones de protocolo*, presta servicios de directorio para facilitar la comunicación y el intercambio de información entre entidades, personas, terminales, listas de distribución, etc. Además de los servicios convencionales de directorio, tales como la denominación, la correspondencia de nombre con dirección y la vinculación entre los objetos y su ubicación, el directorio representa un papel importante de apoyo a los servicios de seguridad al definir y mantener las credenciales de autenticación en la forma de certificados de seguridad. En particular, la serie de Recomendaciones UIT-T X.500 cubre dos aspectos de seguridad:

- la protección de la información de directorio definida fundamentalmente en las Recomendaciones UIT-T X.501 y UIT-T X.509; y
- los principios básicos para la infraestructura de clave pública (PKI) y la infraestructura de gestión de privilegios (PMI) que se define en la Recomendación UIT-T X.509.

Esta sección se inicia considerando la importancia de la seguridad del propio directorio y la necesidad de proteger la información de directorio. A continuación se analiza el papel del directorio en apoyo de una autenticación, unas infraestructuras de clave pública, una gestión de identidad y una telebiometría sólidas.

6.1 Protección de la información de directorio

6.1.1 Objetivos de la protección del directorio

La protección de datos, que es un tema fundamental en la gestión de identidad, está permanentemente presente en las tareas del directorio. La protección de los datos de directorio es principalmente un asunto de privacidad (es decir, protección frente a la divulgación no autorizada de información personal sensible), pero también implica garantizar la integridad de los datos y proteger los bienes representados por los datos.

Un directorio mantiene información sobre entidades. La información de identidad puede ser sensible y sólo se debe revelar a aquellos que tengan derecho y necesiten conocerla.

Existen tres aspectos de la protección de datos:

- autenticación del usuario que pretende acceder a la información;
- control de acceso para proteger los datos frente al acceso no autorizado (NOTA – el control de acceso depende de una autenticación adecuada);
- protección de la privacidad de los datos, que depende de un control de acceso adecuado.

Prácticamente desde el principio las características de la protección de datos han constituido una parte importante de la Recomendación UIT-T X.500, que es la única especificación de directorio que tiene las características adecuadas.

6.1.2 Autenticación de los usuarios de directorio

Un directorio UIT-T X.500 puede permitir el acceso anónimo a parte de su información no sensible. Sin embargo, para tener acceso a datos más sensibles, es necesario cierto nivel de autenticación del usuario. La Recomendación UIT-T X.500 permite diversos niveles de autenticación, en particular:

a) sólo mediante el nombre;

b) mediante el nombre y una contraseña sin protección (es decir, el nombre y una contraseña que se transmite en texto sin cifrar);

c) mediante el nombre y una contraseña protegida (es decir, una contraseña que se ha troceado con alguna información adicional para garantizar que se detecta cualquier intento de acceso al directorio que utilice el valor troceado); y

d) con autenticación fuerte, cuando el transmisor firma digitalmente cierta información. La información firmada está constituida por el nombre del receptor y cierta información adicional que también permite detectar una repetición de intento de acceso.

Se requieren diferentes niveles de protección de datos para los diferentes tipos de usuario entrante. El nivel de autenticación de un usuario también afecta a los derechos de acceso de ese usuario.

6.1.3 Control de acceso al directorio

El control de acceso se utiliza para permitir o denegar operaciones en partes de la información de directorio. La Recomendación UIT-T X.500 es muy flexible sobre cómo se puede subdividir la información de directorio y los usuarios para el control de acceso. Un elemento de información que se ha de proteger se denomina elemento protegido. Los elementos protegidos se pueden agrupar por propiedades de control de acceso comunes. Igualmente los usuarios se pueden agrupar según los permisos o negaciones de acceso.

Los derechos de acceso de un usuario o de un grupo de usuarios dependen del nivel de autenticación. La extracción de información sensible, o la actualización de datos, normalmente requiere un nivel más alto de autenticación que la extracción de información menos sensible.

El control de acceso también tiene en cuenta el tipo de acceso a los datos, por ejemplo, lectura, adición, supresión, actualización y cambio de nombres. En algunos casos, los usuarios pueden no ser ni siquiera conscientes de la existencia de ciertos elementos de información.

El control de acceso trata del derecho a conocer. Sin embargo, la necesidad de conocer va más allá del control de acceso. Disponer del *derecho a conocer* no permite a un usuario extraer información si no se ha establecido una *necesidad de conocer*. Si no se ha establecido esa *necesidad*, la divulgación de información podría constituir una violación de privacidad.

Existen otros ejemplos cuando no basta con el *derecho a conocer*. Por ejemplo:

– aunque un usuario tenga el derecho de extraer las direcciones postales individuales de algunas entidades, puede no ser apropiado permitir la extracción en bloque de direcciones postales; y

– si un usuario tiene derechos de acceso a parte de la información, puede no ser relevante para la propia aplicación para la que se extrajo, en cuyo caso no existe una *necesidad de conocer* y la información no debería revelarse.

6.1.4 Protección de privacidad

La protección de privacidad de los datos de la Recomendación UIT-T X.500 es única y muy potente. La protección de privacidad de los datos es sobre todo un problema cuando un usuario busca el directorio suministrando criterios de búsqueda generales que podrían dar lugar a la entrega de una importante cantidad de información. (Este tipo de búsquedas se denominan a veces barrido de datos (data trawling)).

La Recomendación UIT-T X.500 tiene un concepto de administración de servicio mediante tablas que, además de la administración de los servicios generales, facilita también capacidades de protección de privacidad de datos. El administrador crea una o más tablas para cada combinación de tipos de servicio y grupos de usuarios. Para que la recuperación de los datos tenga éxito, debe existir una tabla que corresponda exactamente con el tipo de servicio y el tipo de grupo de usuario. Sin embargo, no basta con esto. La tabla está protegida mediante el control de acceso, es decir, el usuario también tiene que tener permiso para acceder a la tabla correspondiente. Una tabla, también denominada regla de búsqueda, puede contener información como:

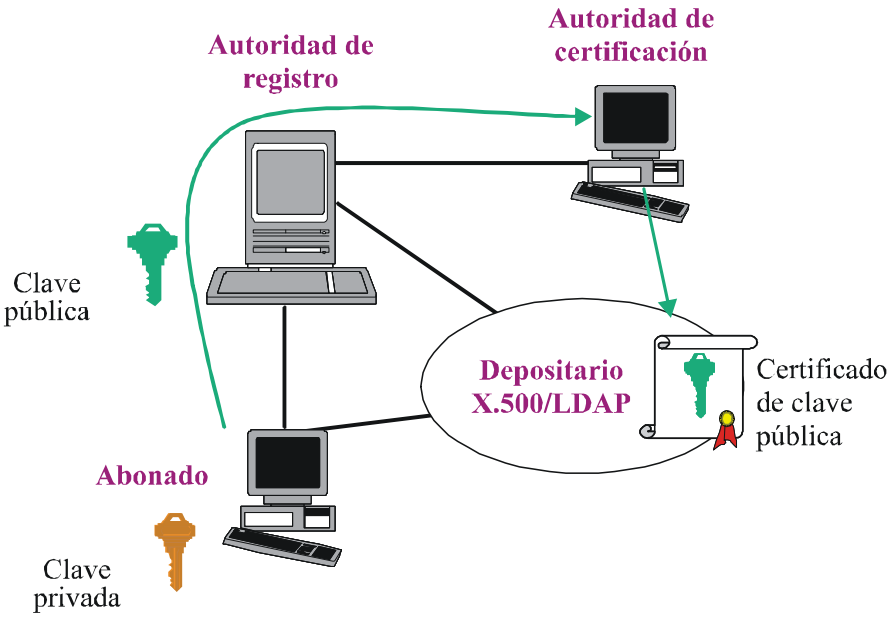
- los criterios de búsqueda necesarios para garantizar que la búsqueda está destinada a proporcionar información sobre una, o muy pocas, entidades. Esto evita las búsquedas que detraen mucha información y protege frente al barrido de datos;
- una lista de elementos de información relevantes para el tipo de servicio; e
- información de control para entidades individuales representadas en el directorio. La tabla que se está utilizando interactúa con la información de control de una entidad para restringir la información obtenida para esa entidad. Esto permite adaptar los datos a los criterios de protección de privacidad para cada entidad individual. Una entidad puede tener requisitos especiales, tales como no desvelar la dirección postal y en su lugar enviar una dirección falsa. Otras entidades pueden desear que no se revelen sus direcciones de correo electrónico a ciertos grupos de usuarios.

La protección de información personal sensible tiene interés por diversas razones. Varias normas de seguridad, en particular las relativas a la autenticación de individuos y a la gestión de identidad, implican la recolección y almacenamiento de información sensible, identificable personalmente. Un número creciente de jurisdicciones tienen requisitos legales relativos a la recolección y uso de ese tipo de información. Los servicios y dispositivos de seguridad, muchos de los cuales se basan en las normas del UIT-T, sirven como mecanismo para proteger información sensible desde el punto de vista de la privacidad. La privacidad está considerada en diversas Recomendaciones, y en algunas se considera directamente la incidencia de ciertas tecnologías en ella. Entre los ejemplos se puede citar la recién aprobada Recomendación UIT-T X.1171, *Amenazas y requisitos para la protección de información identificable personalmente en las aplicaciones que utilizan la identificación basada en etiquetas*, que se trata con mayor detalle en la sección 9.5 sobre servicios basados en etiquetas, y las directrices sobre protección de información identificable personalmente en aplicaciones RFID que se están actualmente elaborando en la SG 17 como parte de las tareas de la IdM (véase la sección 6.4).

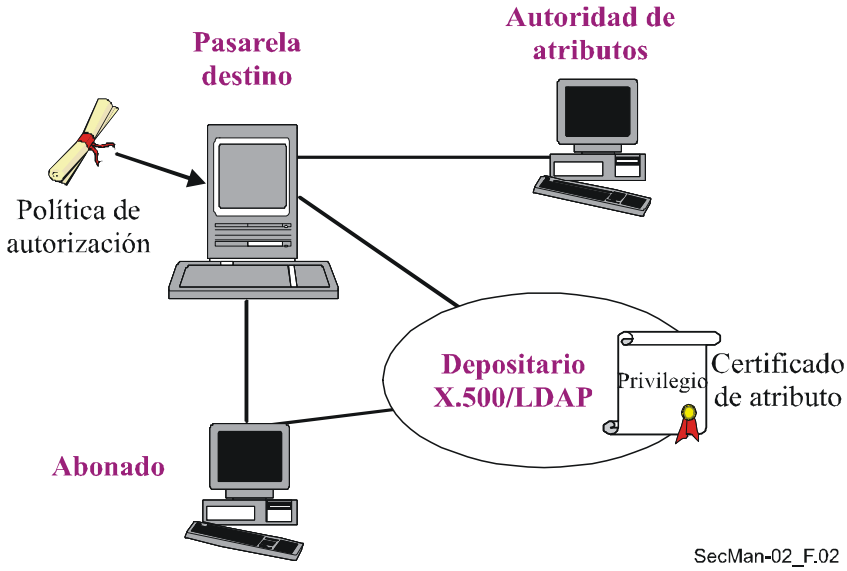
6.2 Autenticación robusta: mecanismos de seguridad de clave pública

Una infraestructura de clave pública (PKI) facilita 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 claves que se describe a continuación. La Recomendación UIT-T X.509, *El Directorio: Marcos para certificados de claves públicas y atributos* es una norma PKI para autenticación robusta basada en certificados de clave pública y en autoridades de certificación. Además de definir un marco de autenticación para PKI, la Recomendación UIT-T X.509 también propone una infraestructura de

gestión de privilegios (PMI) 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 10 se muestran los componentes de la PKI y la PMI.



(a) Componentes de una infraestructura de claves públicas



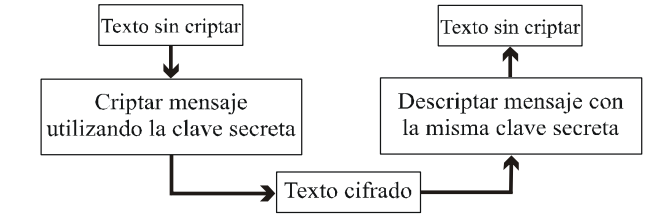
(b) Componentes de una infraestructura de gestión de privilegios

Figura 10 – Componentes de una PKI y de una PMI

6.2.1 Clave secreta y criptografía de clave pública

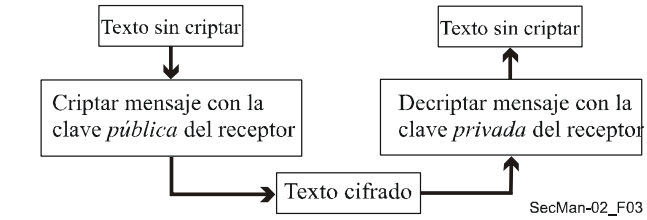
Por criptografía *simétrica* (o *clave secreta*) se entiende un sistema criptográfico en el que se utilizan las mismas claves para la criptación y la descriptación, tal como se muestra en la figura 11(a). En un criptosistema simétrico, algunos participantes comparten una clave secreta única desde un 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 11(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 separados 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 11 – Ilustración de procesos de criptación de clave privada y de clave pública

En el caso de la criptación simétrica, cada par de usuarios debe tener claves distintas que se distribuyen y almacenan de manera segura. En el caso de la criptación asimétrica, las claves de criptación públicas pueden indicarse en el directorio y cualquiera puede utilizar la misma clave de criptación (pública) para enviar datos protegidos 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 para distribuir claves de criptación simétricas con seguridad. Las claves simétricas 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 genera un compendio (o extracto) del mensaje utilizando una función generadora segura unidireccional (SHA1 o MD5). El número generador se cripta mediante la clave privada del remitente y se anexa al mensaje. El destinatario puede confirmar la validez de la firma digital descifrándola mediante la clave pública del remitente para obtener el compendio generado por el remitente y creando entonces su propio compendio del mensaje recibido. Ambos deben ser el mismo compendio para que la firma sea válida.

Independientemente del tipo de criptación (simétrica o asimétrica), no es posible encaminar mensajes a sus receptores si todo el mensaje (incluidos los encabezamientos) está criptado, puesto que los nodos intermediarios no podrán determinar la dirección del receptor. Por tanto, los encabezamientos de los mensajes están 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 el 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 también incluirse en el directorio en la lista de revocación de certificados (CRL). Antes de utilizar las claves públicas, se comprueba su validez consultando la CRL.

6.2.2 Certificados de clave pública

También conocidos como "certificados digitales", los certificados de clave pública son una manera de validar a quien pertenece un par de claves asimétricas. Un certificado de clave pública vincula fuertemente una clave pública a su propietario, y viene firmado digitalmente por una autoridad de confianza que atestigua esta vinculación. Ésta es la autoridad de certificación (CA). En la Recomendación 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 versión de la Recomendación UIT-T X.509 a la que es conforme el certificado, y un conjunto facultativo de campos de extensión que mantienen información sobre la política de certificación de la CA. Todo el certificado se firma digitalmente utilizando la clave privada de la CA, tras lo cual se puede publicar el certificado UIT-T X.509 en, por ejemplo, un sitio web, un directorio LDAP, o en la vCard[1] adjunta a los mensajes de correo electrónico. La firma de la CA garantiza que su contenido no puede ser alterado sin que se sepa.

Para confirmar la validez de un certificado, 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 él. Como puede ocurrir que la CA haya certificado su clave pública ante otra CA (de orden superior), el proceso de validación de claves públicas puede suponer la existencia de una cadena de certificados y de CA. Este proceso termina normalmente cuando se llega al certificado de la CA que es la "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). Esta firma permite a un usuario confirmar 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 dar por descontado que sea correcto. En otras palabras, en una infraestructura de clave pública es fundamental la distribución segura de las claves públicas de la CA raíz, de

[1] Una vCard es una tarjeta electrónica de formato normalizado que a menudo se intercambia por correo electrónico.

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.

6.2.3 Infraestructuras de clave pública

El objetivo principal de una PKI es emitir y gestionar certificados de clave pública, incluido los certificados 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 Recomendación 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 UIT-T 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) y en una declaración de prácticas de certificación (CPS), 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 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.

Las versiones anteriores de la Recomendación UIT-T X.509 (1988, 1993 y 1997) especificaban los elementos básicos necesarios para las infraestructuras de clave pública, incluida la definición de los certificados de clave pública. En la Recomendación UIT-T X.509 revisada, aprobada en 2001 (y actualizada en 2005 y 2008), se amplía significativamente el concepto de certificados de atributo y se proporciona un marco para la infraestructura de gestión de privilegios (PMI).

6.2.4 Infraestructura de gestión de privilegios

Una infraestructura de gestión de privilegios (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 el cuadro 4 se muestran las similitudes entre ambas infraestructuras.

Cuadro 4 – Comparación de las características de la infraestructura de gestión de privilegios y de 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. La información relativa a la política está vinculada al nombre de usuario en el certificado de atributo y contiene diversos elementos, como se muestra en el cuadro 5.

Cuadro 5 – Estructura de un certificado de atributo X.509

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

Los certificados de atributo también se utilizan en telebiométrica (véase la sección 6.5) para generar certificados biométricos y vincular a un usuario con su información biométrica. Los certificados de dispositivos biométricos definen las capacidades y limitaciones de esos dispositivos. Los certificados de política biométrica definen la relación entre un nivel de seguridad y los parámetros del algoritmo biométrico.

En la Recomendación UIT-T X.509 se describen cinco componentes para el control de una PMI, a saber: el asertor de privilegios, el verificador de privilegios, el método de objeto, la política de privilegios, y las variables ambientales (véase la figura 12). El verificador de privilegios puede controlar el acceso al método de objeto mediante el asertor de privilegios, de conformidad con la política de privilegios.

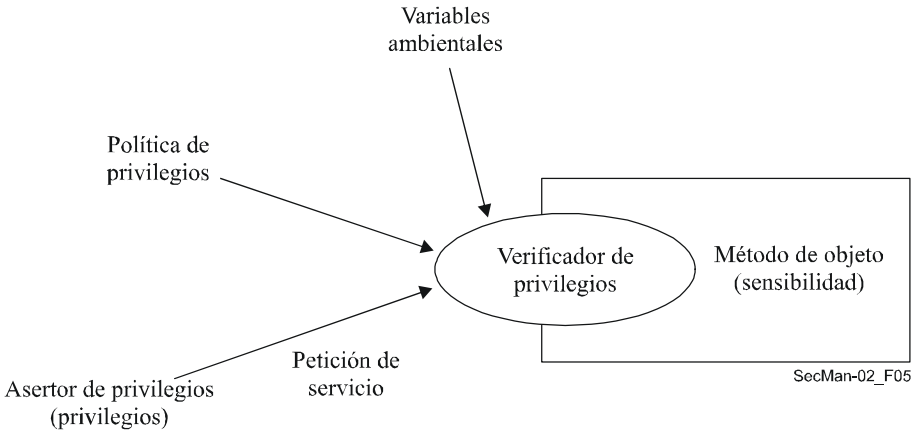


Figura 12 – Modelo de control de una PMI X.509

Cuando sea necesario delegar un privilegio en una implementación, la Recomendación 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 13).

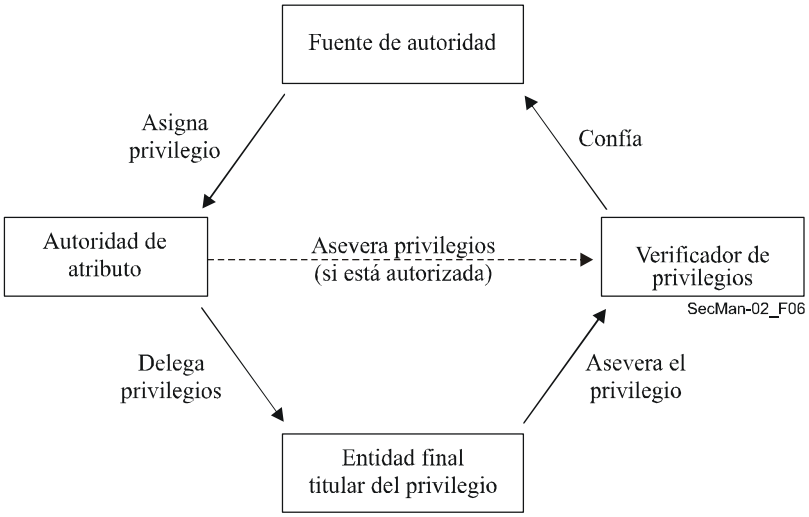


Figura 13 – Modelo de delegación de la PMI X.509

En algunas implementaciones de los métodos de autorización que siguen el modelo de control de acceso basado en las funciones (RBAC) 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.

6.3 Directrices de autenticación

Se han elaborado algunas directrices que pueden desarrollar aspectos específicos de la autenticación. Se resumen a continuación.

6.3.1 Protocolo de autenticación basado en contraseña segura con intercambio de clave

El protocolo de autenticación basado en contraseñas segura con intercambio de clave (SPAK) es un protocolo de autenticación simple en el que se utiliza una contraseña que se puede memorizar entre el cliente y el servidor como autenticación mutua y un secreto compartido que se puede usar como clave de sesión para la siguiente sesión.

En la Recomendación UIT-T X.1151, *Directrices sobre el protocolo de autenticación basado en contraseña segura con intercambio de clave*, se definen los requisitos para el SPAK junto con directrices para seleccionar el SPAK más adecuado a partir de protocolos de autenticación de contraseña segura. Este protocolo es muy simple. Es sencillo de implementar y utilizar y no requiere ninguna otra infraestructura (como la PKI). Se espera que tenga una importancia creciente para muchas aplicaciones en el próximo futuro. El SPAK proporciona tanto la autenticación de usuario como un intercambio de clave robusto con una sencilla contraseña, de forma que se puede proteger una comunicación subsiguiente mediante un secreto compartido durante el procedimiento de autenticación (véase la figura 14).

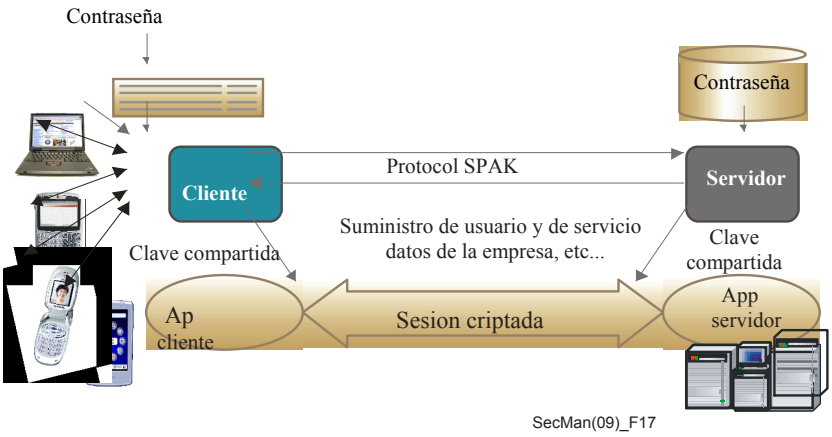


Figura 14 – Funcionamiento habitual para el protocolo SPAK

6.3.2 Protocolo de autenticación extensible

El protocolo de autenticación extensible (EAP) soporta múltiples mecanismos de autenticación entre un solicitante y un servidor de autenticación en una red de comunicaciones de datos. El EAP se puede utilizar como instrumento básico para permitir la autenticación de usuarios y distribuir claves de sesión. Puede realizar autenticación de dispositivos para establecer una conexión punto a punto segura y evitar e impedir el acceso a un dispositivo no autorizado.

La Recomendación UIT-T X.1034 describe un marco para la autenticación basada en el EAP y la gestión de claves dar seguridad a las capas más bajas en una red de comunicaciones. Proporciona directrices sobre la selección de los métodos EAP y describe el mecanismo para la gestión de claves para las capas más bajas de una red de comunicaciones de datos. El marco se aplica tanto a redes de acceso inalámbricas como alámbricas con un medio compartido.

Se requieren tres entidades para la autenticación y la gestión de claves: un solicitante (o par), un autenticador y un servidor de autenticación como se muestra en la figura 15. El solicitante actúa como un usuario final que accede a la red desde una estación de usuario final. El autenticador actúa como un elemento de reforzamiento de políticas, intercambiando mensajes EAP entre el solicitante y el servidor de autenticación. El servidor de autenticación autentifica al solicitante, puede compartir un secreto que se puede utilizar para derivar claves criptográficas, envía el resultado de la autenticación de un usuario final al autenticador y transmite el secreto compartido al autenticador. Este secreto compartido se puede utilizar para derivar claves criptográficas entre el autenticador y el solicitante y garantizar la confidencialidad e integridad así como permitir la autenticación del mensaje.

La autenticación y la gestión de claves generalmente incluyen cuatro fases de funcionamiento: descubrimiento de capacidad de seguridad, autenticación de EAP, distribución de claves y gestión de claves (véase la figura 15). En la fase de capacidad de seguridad, un solicitante negocia las capacidades de seguridad y los diversos parámetros del protocolo que ha de utilizar con el autenticador. En la fase EAP el servidor de autenticación autentifica un solicitante y deriva un secreto compartido maestro con el solicitante a partir del protocolo EAP. En la fase de distribución de claves, el servidor de autenticación transporta el secreto maestro a un autenticador para permitir que la autenticación derive diversas claves criptográficas para una sesión subsiguiente entre un solicitante y un autenticador. Para impedir el uso de la misma clave secreta una y otra vez, se deben utilizar claves criptográficas nuevas para cada sesión. Finalmente, en la fase de gestión de claves, el autenticador intercambia números aleatorios con el solicitante para obtener una clave criptográfica renovada, logrando el secreto en la comunicación.

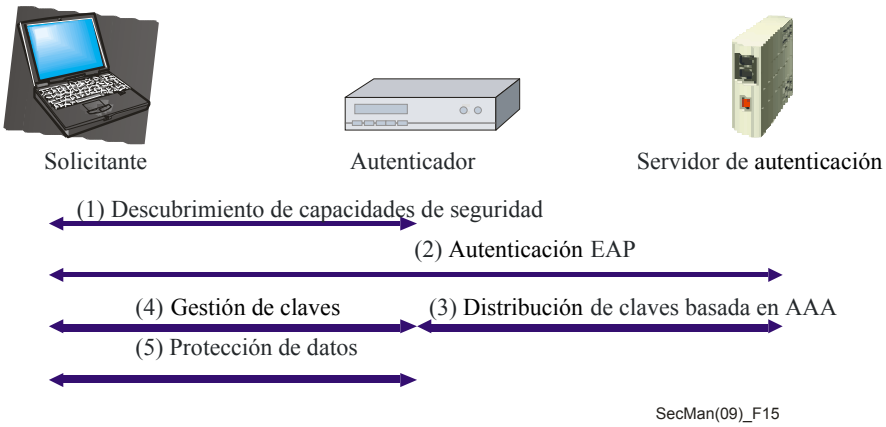


Figura 15 – Cuatro fases de funcionamiento para la autenticación y la gestión de claves de la capa más baja

6.4 Gestión de identidad

6.4.1 Visión general de la gestión de identidades

La gestión de identidad (IdM) es el proceso de gestionar y controlar con seguridad información de identidad (por ejemplo, credenciales, identificadores, atributos y repudios) que se utiliza para representar entidades (como los proveedores de servicio, las organizaciones de usuarios finales, personas, dispositivos de red, aplicaciones de software y servicios) en el ámbito de las comunicaciones. Una única entidad puede tener múltiples identidades digitales con el fin de acceder a diversos servicios con diferentes requisitos, y estos pueden existir en múltiples ubicaciones. La IdM soporta la autenticación de una entidad. Para los fines del UIT-T, la identidad aseverada por una entidad presenta la singularidad de esa entidad en un determinado contexto.

La IdM es un componente clave de la ciberseguridad puesto que proporciona la capacidad de establecer y mantener comunicaciones fiables entre entidades y permite el acceso bajo demanda nómada a redes y servicios electrónicos. También permite la autorización de una gama de privilegios (en lugar de privilegios de todo o nada) y facilita el cambio de privilegios cuando cambia el cometido de una entidad. La IdM mejora la capacidad de la organización para aplicar sus políticas de seguridad, permitiendo la supervisión de una actividad de la entidad en la red y su evaluación y puede facilitar acceso a entidades tanto internas como externas a una organización.

La IdM proporciona la garantía de la información de identidad soportando el control de acceso seguro y fiable. Esta capacidad se consigue mediante el inicio/final ce sesión unificado, un control de usuario de información identificable personalmente y la capacidad para que un usuario seleccione un proveedor de identidad que pueda facilitar funciones de verificación y de delegación en su nombre, en lugar de proporcionar credenciales a todos los proveedores de servicio. La IdM también soporta múltiples servicios basados en la identidad incluidos: publicidad dirigida; servicios personalizados basados en la geolocalización y el interés; y servicios autentificados para reducir el fraude y el robo de identidad.

La IdM es una tecnología compleja que incluye:

- el establecimiento, la modificación, la suspensión, la consecución y la finalización de información de identidad;

- el reconocimiento de identidades parciales que representa entidades en un determinado contexto o cometido;
- el establecimiento y la evaluación de confianza entre entidades; y
- la ubicación de la información de identidad de la entidad (por ejemplo, a través de un proveedor de identidad con autoridad que sea legalmente responsable de mantener los identificadores, las credenciales y algunos o todos los atributos de la entidad).

El suplemento de la serie de Recomendaciones UIT-T X.1250, *Visión de conjunto de la gestión de identidad en el contexto de la ciberseguridad*, proporciona una breve introducción al asunto de la gestión de identidades.

6.4.2 Tareas del UIT-T en la gestión de identidades

Aunque todavía se están debatiendo algunos de los conceptos básicos y del vocabulario subyacente, los trabajos están progresando en diversos ámbitos de la CE 17 (que es la CE rectora sobre la IdM), así como en la CE 2 (aspectos operativos de la prestación de servicios y de la gestión de las telecomunicaciones) y la CE 13 (redes futuras incluidas la móvil y las NGN).

La CE 2 es responsable de los estudios relativos a garantizar la coherencia del formato y la estructura de los identificadores IdM y de especificar interfaces para sistemas de gestión con miras a las comunicaciones de la información de identidad dentro y entre dominios organizativos.

La CE 13 es responsable de la arquitectura funcional de gestión de identidad específica de las NGN que apoyan servicios de identidad de valor añadido, el intercambio seguro de información de identidad y la aplicación de interfuncionamiento entre un conjunto diverso de formatos de información de identidad. La CE 13 también es responsable de identificar cualesquiera amenazas de gestión de identidad dentro de las NGN y los mecanismos para contrarrestarlas. La Recomendación UIT-T Y.2720, *Marco general para la gestión de identidades en las redes de la próxima generación*, ya ha sido aprobada. Esta norma describe un planteamiento estructurado para diseñar, definir e implementar soluciones IdM que faciliten el interfuncionamiento en entornos heterogéneos.

La CE 17 es la responsable de los estudios relativos al desarrollo de un modelo de gestión de identidad genérico, independiente de las tecnologías de red, y soporta el intercambio seguro de información de identidad entre entidades. Este trabajo también incluye: el estudio de procesos para descubrir las fuentes fidedignas de información de identidad; mecanismos genéricos para la conexión/interfuncionamiento de un conjunto diverso de formatos de información de identidad; las amenazas a la gestión de identidad y los mecanismos para contrarrestarlas; la protección de información identificable personalmente (PII) y el desarrollo de mecanismos para garantizar que el acceso a la PII solo se autoriza cuando es pertinente. En septiembre de 2009 se aprobaron dos Recomendaciones: la Recomendación UIT-T X.1250, *Capacidades básicas para una confiabilidad y una interoperabilidad mejoradas de la gestión de identidad global*, y la Recomendación UIT-T X.1251, *Marco para el control por el usuario de la identidad digital*. Además, se está preparando un conjunto básico de definiciones relativas a la IdM para lograr una terminología uniforme y coherente en las normas UIT-T sobre IdM.

Se ha establecido una actividad de coordinación conjunta para la gestión de identidad (JCA-IdM) con el fin de coordinar los trabajos del UIT-T en materia de IdM. También se ha establecido una iniciativa de normas globales IdM (IdM-GSI) para armonizar los diferentes planteamientos en todo el mundo respecto a la IdM y colaborar con otros organismos que trabajan en este asunto. La página de la Comisión de Estudio rectora

sobre IdM proporciona amplia información sobre las actividades IdM, las Recomendaciones aprobadas y en desarrollo y otra información relativa a los trabajos en IdM.

6.5 Telebiometría

La telebiometría se centra en la identificación y autenticación personal utilizando dispositivos biométricos en entornos de telecomunicaciones. En particular, se basa en cómo se puede mejorar la identificación y autenticación de los usuarios mediante métodos telebiométricos seguros. Los trabajos del UIT-T sobre este asunto se realizan en estrecha cooperación con otras organizaciones normativas y cubre temas que incluyen: la interacción entre el ser humano y el entorno; las claves digitales biométricas; las extensiones biométricas para certificados X.509 y la autenticación biométrica en una red abierta.

6.5.1 Autenticación telebiométrica

La biometría es capaz de soportar servicios de autenticación muy seguros, aunque la normalización de la autenticación telebiométrica en una red abierta se enfrenta a diversos retos:

- los proveedores de servicio pueden no disponer de información relativa a los dispositivos biométricos que se están utilizando en el entorno del usuario final, al nivel/configuración de seguridad de dichos dispositivos o cómo son operados;
- la precisión (tasa de aceptación falsa) determinada por el parámetro umbral difiere entre diferentes productos biométricos. Por lo tanto, el proveedor de servicio no puede pretender mantener un nivel de precisión uniforme;
- la precisión de la verificación biométrica puede disminuir con la edad de los usuarios finales, ya que la biometría utiliza características del cuerpo humano.

Los protocolos y perfiles generales de la autenticación biométrica para los sistemas de telecomunicaciones en una red abierta se especifican en la Recomendación UIT-T X.1084, *Protocolo general de autenticación biométrica y características de un modelo de sistema para sistemas de telecomunicaciones*.

La figura 16 ilustra la autenticación de un usuario final a través de una red abierta no cara a cara.

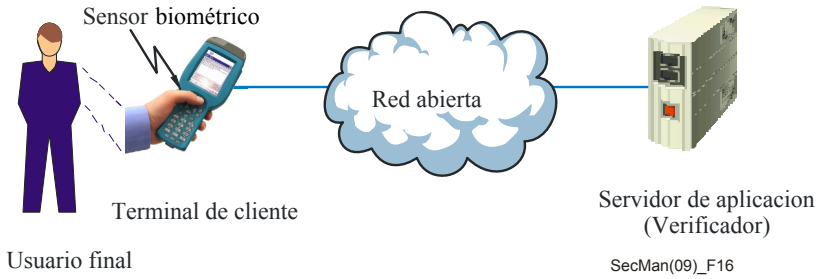


Figura 16 – Autenticación telebiométrica de un usuario final

6.5.2 Generación y protección de claves digitales telebiométricas

En la Recomendación UIT-T X.1088, *Un marco de generación y protección de claves digitales biométricas*, se define un marco para la generación de claves digitales biométricas. Este marco define la protección utilizando una plantilla biométrica con un certificado de clave pública y un certificado biométrico con el fin de facilitar autenticación segura criptográficamente y comunicaciones seguras en redes abiertas. También se

definen los requisitos de seguridad para la generación y protección de claves digitales biométricas. El marco se puede aplicar al cifrado biométrico y a las firmas digitales. Se proponen dos métodos:

- generación de claves biométricas, donde se crea la clave a partir de una plantilla biométrica (figura 17); y
- vinculación/reestablecimiento de claves biométricas, donde la clave se almacena en una base de datos mediante autenticación biométrica (figura 18).

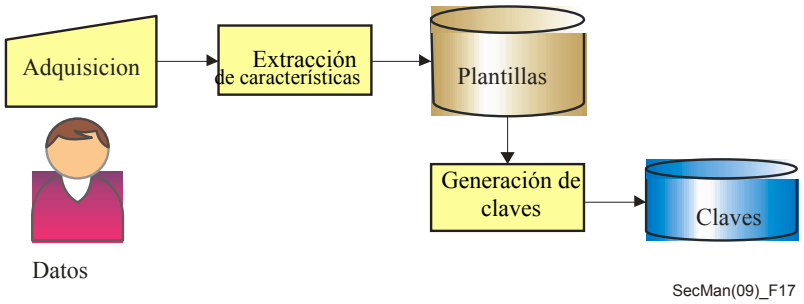


Figura 17 – Generación de claves biométricas

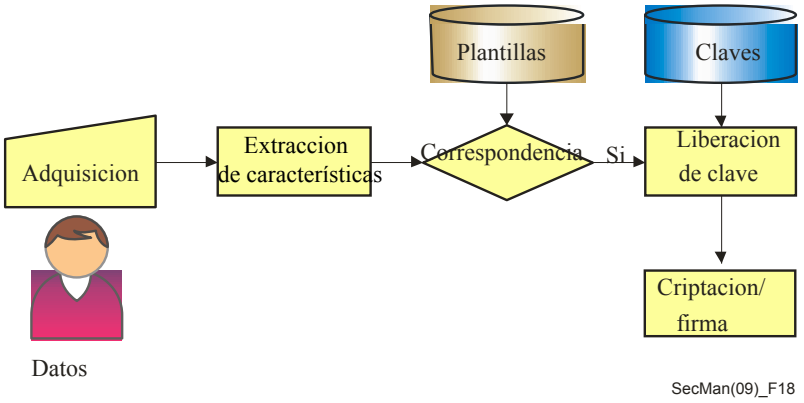


Figura 18 – Vinculación/reestablecimiento de claves biométricas

6.5.3 Aspectos de seguridad de la telebiometría

Se ha definido un marco para los aspectos de seguridad de la telebiometría para el modelo multimodal telebiométrico (Recomendación UIT-T X.1081, *Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad*), que define las interacciones entre el ser humano y el entorno y también las cantidades y unidades utilizadas para medir esas interacciones. El modelo multimodal telebiométrico no se limita a la consideración de interacciones puramente físicas sino que también reconoce las interacciones de comportamiento que actualmente no se cuantifican mediante unidades normalizadas.

6.5.4 Telebiometría relacionada con la fisiología humana

Los aspectos de seguridad de la telebiométrica también se consideran en la Recomendación UIT-T X.1082, *Telebiometría relacionada con la fisiología humana*, que define cantidades y unidades para características fisiológicas, biológicas y de comportamiento que podrían mejorar las aportaciones y los resultados a los

sistemas de identificación o verificación telebiométricos (sistemas de reconocimiento) incluidos cualesquiera umbrales de detección o de seguridad conocidos. Ofrece nombres, definiciones y símbolos para cantidades y unidades de la fisiología humana relacionada con la telebiometría (es decir, características y emisiones humanas que se pueden detectar mediante sensores). También incluye cantidades y unidades relativas a los efectos producidos sobre los seres humanos por la utilización de dispositivos telebiométricos.

6.5.5 Elaboración de otras normas sobre telebiometría

Se han definido extensiones para los certificados UIT-T X.509 utilizados en infraestructuras de clave pública o en infraestructuras de gestión de privilegios para certificados de productos biométricos. Estos se especifican en la Recomendación UIT-T X.1089, *Infraestructura de autenticación de telebiometría*.

La Recomendación UIT-T X.1083, *Protocolo para el interfuncionamiento con interfaces de programación de aplicaciones de tecnologías biométricas*, especifica la sintaxis (utilizando ASN.1), la semántica y las codificaciones de mensajes que permiten a una aplicación conforme a BioAPI solicitar operaciones biométricas en proveedores de servicio de biometría que cumplen BioAPI a través de los límites de nodos o procesos, y recibir información de eventos originados en esos BSP.

7. Seguridad de la infraestructura de red

7 Seguridad de la infraestructura de red

Los datos utilizados para supervisar y controlar el tráfico de gestión de la red de telecomunicaciones se suelen transmitir 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 las telecomunicaciones (RGT), que se describe en la Recomendación UIT-T M.3010, *Principios para una red de gestión de las telecomunicaciones*. Es fundamental que este tráfico sea seguro. 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 de red supone tanto el establecimiento de una red de gestión segura como la gestión de la seguridad de la información relacionada con los tres planos de seguridad de la arquitectura de seguridad X.805.

La actividad de gestión relativa a los elementos de infraestructura de una red debe siempre realizarla un usuario autorizado. Para lograr una solución segura de extremo a extremo, conviene aplicar todas las medidas de seguridad (por ejemplo, control de acceso, autenticación) a cada tipo de actividad de red 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 y sistemas de gestión que forman parte de la infraestructura de red.

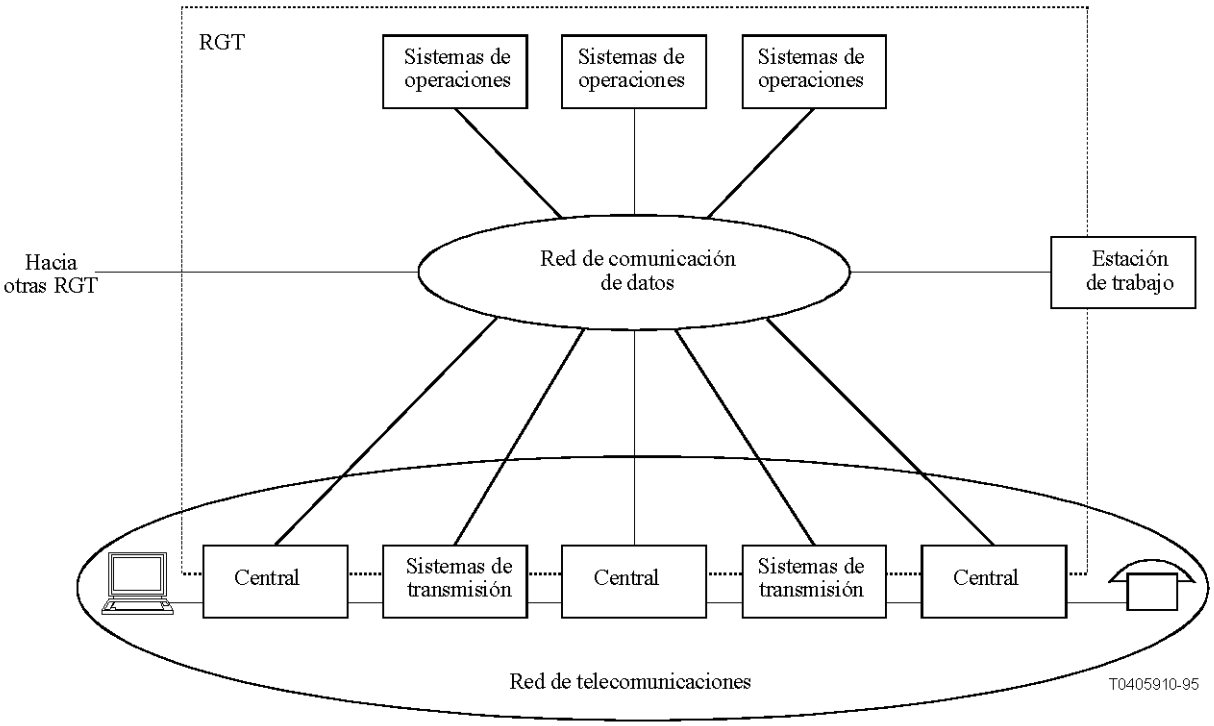
Entre otras aplicaciones de gestión de red se incluyen las relacionadas con entornos en los que los diversos proveedores de servicio deben interactuar para poder ofrecer servicios de extremo a extremo, como por ejemplo instalaciones de comunicaciones para las instituciones gubernamentales o de regulación para la recuperación en caso de desastre y en situaciones en las que líneas arrendadas a los clientes atraviesen fronteras geográficas.

7.1 Red de gestión de las telecomunicaciones

La RGT se separa y aísla de la infraestructura de red pública, de tal manera que no se contamine con los problemas producidos por 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 una aplicación de usuario final 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, ya que el plano de gestión deviene ahora accesible a muchos usuarios finales, y múltiples variedades de actividades maliciosas son ahora posibles.

7.2 Arquitectura de gestión de red

La arquitectura necesaria para la gestión de una red de telecomunicaciones se define en la Recomendación UIT-T M.3010. La relación entre una RGT y una red de telecomunicación se muestra en la figura 19. La arquitectura de la red de gestión define interfaces que establecen los intercambios necesarios para realizar las funciones de operaciones, administración, mantenimiento y suministro.



NOTA – Los límites de la RGT, representados por líneas punteadas, podrán abarcar y gestionar servicios y equipos de cliente/usuario.

Figura 19 – Relación entre una RGT y una red de telecomunicación

En la Recomendación 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. UIT-T M.3016.1 define los requisitos en detalle, la Rec. M.3016.2 los servicios de seguridad y la Rec. UIT-T M.3016.3 los mecanismos que pueden contrarrestar las amenazas dentro del contexto de la arquitectura funcional de la RGT, como se define en la Recomendación UIT-T M.3010. Como no es necesario que todas las organizaciones de normalización admitan todos los requisitos, la Recomendación UIT-T 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.

Cuando se trata de la seguridad de gestión de red, hay que considerar dos facetas diferentes. Una tiene que ver con el plano de gestión para una actividad de usuario de extremo a extremo (por ejemplo, servicios VoIP). La administración de los usuarios se debe efectuar de una manera segura. Esto es lo que se conoce como *seguridad de la información de gestión* que se intercambia en la red a fin de soportar una aplicación extremo a extremo. La segunda faceta es la gestión de la información de seguridad, que se aplica independientemente del tipo de aplicación. Por ejemplo, la actividad de informe de dificultades entre dos proveedores de servicio debe llevarse a cabo de forma segura, lo que puede requerir que los intercambios estén criptados, en cuyo caso hay que considerar la gestión de las claves de criptación.

Se dispone de varias Recomendaciones que especifican funciones de gestión de seguridad de la arquitectura X.805 para las tres capas del plano de gestión (véase la figura 1). Además, como se trata en las siguientes subsecciones, otras Recomendaciones 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.

7.3 Seguridad de los elementos de infraestructura de una red

La conectividad de extremo a extremo puede considerarse en términos de la o las redes de acceso y troncales, en las que pueden utilizarse diversas tecnologías y para las que se han elaborado varias Recomendaciones. La red de acceso óptica pasiva de banda ancha se utiliza aquí como un ejemplo. Para la administración de privilegios de usuario de esta red de acceso se utiliza la metodología de modelado unificado de la Recomendación UIT-T Q.834.3. Los intercambios de gestión mediante la arquitectura de intermediario de petición de objetos común (CORBA) se especifican en la Recomendación UIT-T Q.834.4. La interfaz que se describe en dichas Recomendaciones se aplica entre el sistema de gestión de elementos y el sistema 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 el segundo ejecuta actividades al nivel de red de extremo a extremo y cubre sistemas de gestión provenientes de muchos fabricantes. En la figura 20 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 usuario incluye la enumeración de las actividades de gestión que son permitidas a cada usuario autorizado. 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.

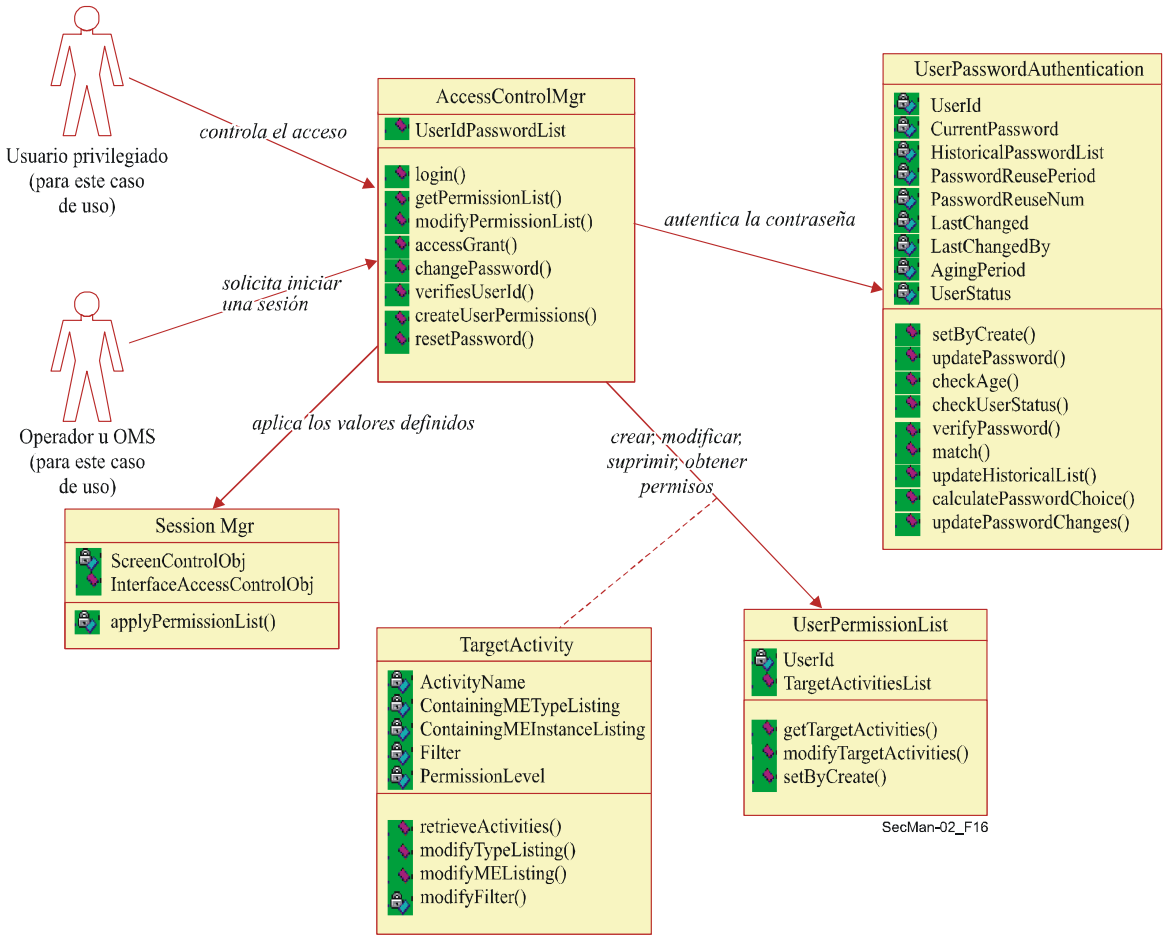


Figura 20 – Administración de privilegios de usuario conforme a UIT-T Q.834.3

7.4 Seguridad de las actividades de supervisión y control

Dos aspectos de seguridad tienen que ver con la intersección entre el plano de gestión y la capa de servicios. El primer aspecto consiste en poder garantizar que se disponga de las medidas de seguridad adecuadas para los servicios existentes en la red. Por ejemplo, garantizando que sólo se permite 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 para facilitar la detección de violaciones de seguridad.

La Recomendación UIT-T M.3208.2, *Gestión de conexiones de enlaces de servicio proporcionados previamente para formar un servicio de circuitos arrendados*, considera el primer aspecto, la actividad de gestión de un servicio. Este servicio de gestión de conexión permite al usuario 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 X.805 asociadas 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 Recomendación UIT-T M.3210.1, *Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000)*, que define las actividades administrativas asociadas con el plano de gestión para el caso de servicios inalámbricos, es un ejemplo de norma 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 Recomendación 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 registrado en la red visitada. En la figura 21 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 de detección de fraude en la red propia pide información sobre las actividades cuando un abonado se inscribe en una red visitada y se mantiene activo hasta que el abonado suspende el registro. Se pueden definir perfiles de acuerdo con la utilización, basados en los análisis de los registros de llamadas a nivel de servicio o de un abonado. El sistema de detección de fraude puede entonces analizar y generar las alarmas adecuadas cuando se detectan comportamientos fraudulentos.

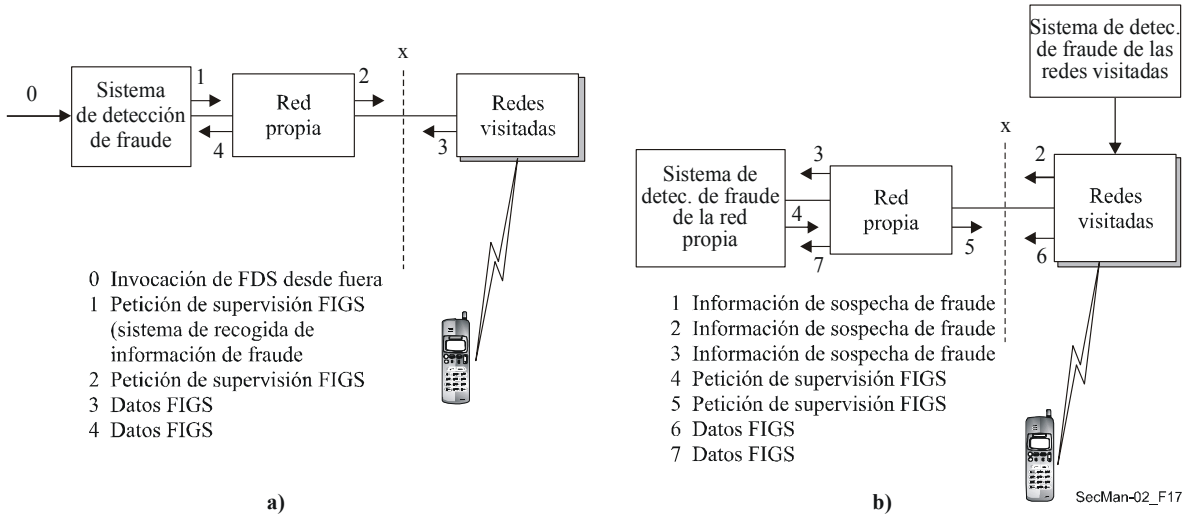


Figura 21 – Gestión de fraudes para los servicios inalámbricos

7.5 Seguridad de las aplicaciones basadas en la red

La intersección entre el plano de gestión y la capa de aplicación en la Recomendación UIT-T X.805 tiene que ver con la seguridad de las aplicaciones basadas en la red del usuario final, que incluyen 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. Es posible explicarlo mejor con algunos ejemplos. El usuario final de estas aplicaciones es el personal de gestión (de operaciones) 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 sobre el problema. Tanto el usuario de dichos sistemas como la aplicación propiamente dicha requieren de autorización para señalar estos problemas. Se recomienda también que los sistemas y usuarios autorizados hagan lo necesario para conocer el estado de los problemas señalados.

En la figura 22 se muestran las interacciones que necesitan protección. 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.

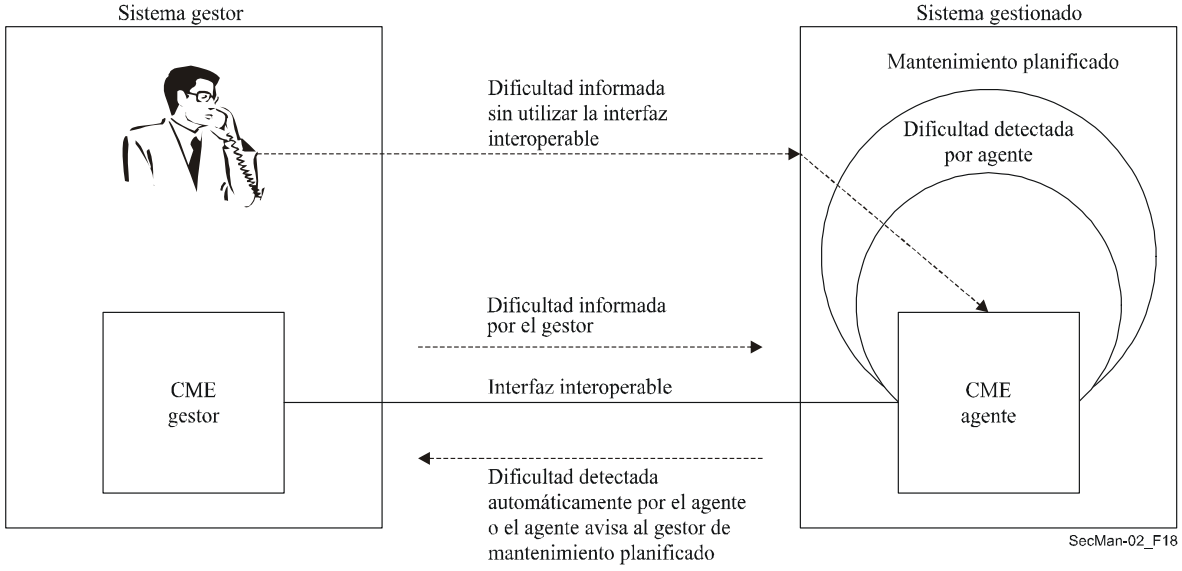


Figura 22 – Creación de informe de gestión de dificultades

En la Recomendación UIT-T X.790, *Función de gestión de dificultades para aplicaciones del UIT-T*, se define esta aplicación de gestión y se utilizan mecanismos como por ejemplo las listas de control de acceso y la autenticación bidireccional para garantizar la seguridad de las actividades.

7.6 Servicios comunes de gestión de seguridad

Existen varios servicios comunes que se consideran actividades X.805 del plano de gestión, en particular cuando se utiliza el protocolo CMIP (Recomendación UIT-T X.711). A continuación se hace una breve descripción de los servicios incluidos en estas Recomendaciones.

7.6.1 Función de informe de alarmas de seguridad

La notificación de alarmas es una función clave de las interfaces de gestión. Cuando se detecta un problema operacional (por ejemplo, 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 y el detector de la violación de seguridad. Las causas de alarma están asociadas con los tipos de eventos como se muestra en el cuadro 6.

Cuadro 6 – 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 la Recomendación UIT-T X.736, *Función señaladora de alarmas de seguridad*.

7.6.2 Función de pista de auditoría de seguridad

Se utiliza una función de pista de auditoría de seguridad para registrar eventos relacionados con la seguridad y, en particular, las violaciones de la seguridad. Estos eventos pueden incluir conexiones, desconexiones, utilizaciones de mecanismos de seguridad, operaciones de gestión y contabilidad de la utilización. La *función de pista de auditoría de seguridad* se define en la Recomendación UIT-T X.740.

7.6.3 Control de acceso para entidades gestionadas

En la Recomendación UIT-T X.741, *Objetos y atributos para el control de acceso*, se presenta una definición muy detallada del modelo utilizado para asignar un control de acceso a las distintas entidades gestionadas. Esta Recomendación satisface varios requisitos: protección de la información de gestión para impedir la creación, supresión y modificación no autorizada, adecuación de las operaciones 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, se pueden aplicar restricciones de acceso a distintos niveles. La política de control de acceso se puede basar en uno o más de los esquemas definidos (por ejemplo, listas de control de acceso, control de acceso basado en capacidades, etiquetas o en el contexto). En el modelo UIT-T X.741 la decisión de admitir o denegar el acceso se basa en la política y en la información de control de acceso (ACI). La ACI incluye, por ejemplo, las normas, la identidad del iniciador, las identidades de los objetivos cuyo acceso se requiere y la información atinente a la autenticación del iniciador.

7.6.4 Servicios de seguridad basados en CORBA

Si bien de las Recomendaciones de la serie UIT-T X.700 están basadas en la hipótesis de utilización del CMIP como protocolo de interfaz de gestión, existen otras tendencias que figuran actualmente en esas Recomendaciones. Entre ellas, un protocolo, servicios y modelos de objetos basados en el intermediario de petición de objetos común (CORBA) para las interfaces de gestión. Cabe destacar la Recomendación UIT-T X.780, *Directrices de la RGT para la definición de objetos gestionados mediante arquitectura de intermediario de petición de objeto común*, la Recomendación UIT-T 780.1, *Directrices de la RGT para la definición de interfaces de objetos gestionados mediante arquitectura de intermediario de petición de objeto común de de granularidad gruesa*, la Recomendación UIT-T X.780.2, *Directrices de la RGT para definir objetos CORBA de gestión orientados al servicio y objetos CORBA de fachada*, y la Recomendación UIT-T X.781, *Requisitos y directrices para los formularios de declaración de conformidad de implementación asociados con sistemas basados en arquitectura de intermediario de petición de objeto común*. Además, en la Recomendación 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, la Recomendación UIT-T Q.816 se refiere a la especificación de grupo de gestión de objeto (OMG) de servicios comunes para la seguridad.

8. Planteamientos específicos a la seguridad de la red

8 Planteamientos específicos a la seguridad de la red

En esta sección se analizan planteamientos para proteger diversos tipos de redes. La sección empieza considerando los requisitos de seguridad para las redes de la próxima generación. Posteriormente, se analizan las redes de comunicaciones móviles que se encuentran en transición entre la movilidad basada en una única tecnología (como AMDC o GSM) y la movilidad entre plataformas heterogéneas que utilizan el protocolo de Internet. Luego, se analizan las características de seguridad de algunas redes domésticas y de la televisión por cable. Finalmente, se presentan los retos de seguridad para las redes de sensores ubicuos.

8.1 Seguridad para las redes de la próxima generación (NGN)

Una red de la próxima generación (NGN) es una red basada en paquetes que es capaz de proporcionar servicios de telecomunicaciones a los usuarios y de utilizar múltiples tecnologías de transporte de banda ancha con habilitación de calidad de servicio. Además, las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes propias del transporte. Una NGN permite a un usuario acceder a redes y competir con los proveedores de servicio y los servicios, sin restricciones. Soporta movilidad generalizada lo que permite prestar servicios coherentes y ubicuos a los usuarios. En la Recomendación UIT-T Y.2001, *Visión general de las redes de próxima generación*, se facilitan más detalles sobre las características generales de las NGN.

8.1.1 Objetivos y requisitos de seguridad de las NGN

Puesto que la seguridad es una de las características que definen una NGN, es fundamental determinar un conjunto de normas que garanticen, en la mayor medida posible, la seguridad de esas redes. Mientras las NGN evolucionan, y aparecen nuevas vulnerabilidades de seguridad para las que no existe un remedio automático inmediato, es preciso documentar adecuadamente dichas vulnerabilidades para que los administradores y los usuarios finales de la red puedan reducirlas.

Los estudios de seguridad de las NGN tienen que considerar y desarrollar arquitecturas de red que:

- proporcionen una seguridad máxima a la red y a los recursos del usuario final;
- permitan una inteligencia de extremo a extremo muy distribuida;
- permitan la coexistencia de múltiples tecnologías de red;
- proporcionen mecanismos de seguridad de extremo a extremo;
- proporcionen soluciones de seguridad que se apliquen a múltiples dominios administrativos;
- proporcionen gestión de identidad segura, que implica, aunque no está limitada a:
  - autenticación fiable de las entidades NGN (por ejemplo, usuarios, dispositivos de usuario, proveedores de red, proveedores de servicio, proveedores de identidad, etc.);
  - prevención de acceso no autorizado a los datos de identidad NGN;
  - intercambio seguro de información de identidad entre las entidades federadas en la NGN;
  - soporte para mantener registros del uso de la información de identidad en la NGN;
  - soporte para la privacidad y anonimato de los usuarios en la NGN; y
  - compatibilidad en el soporte ofrecido a los usuarios de NGN para ayudarles a gestionar su información de identidad de forma segura (por ejemplo, modificando los perfiles de usuario, cambiando las contraseñas, permitiendo servicios basados en la ubicación, mirando registros de facturación, etc.);

- proporcionen soluciones de seguridad para IPTV que sean rentables y tengan un efecto aceptable sobre las características de funcionamiento, la calidad del servicio, la usabilidad y la escalabilidad. Entre los tipos de protección que debería proporcionar la seguridad IPTV se encuentran, aunque no están limitados a:
  - la protección de contenidos;
  - la protección del servicio;
  - la protección de la red;
  - la protección del terminal; y
  - la protección de los usuarios.

La Recomendación UIT-T Y.2701, *Requisitos de seguridad de la versión 1 de la red de próxima generación*, que se basa en los principios de la Recomendación UIT-T X.805, especifica los requisitos de seguridad para proteger las NGN frente a amenazas de seguridad y considera alguno de los aspectos técnicos de la gestión de identidad.

En un entorno multired deben protegerse los elementos siguientes:

- la infraestructura y la red del proveedor de servicio y sus activos (por ejemplo, activos y recursos de la NGN tales como elementos de red, sistemas, componentes, interfaces y datos e información), sus recursos, sus comunicaciones (es decir, señalización, gestión y tráfico de datos/portador) y sus servicios;
- servicios y capacidades de la NGN (por ejemplo, servicios de voz, de vídeo y de datos); y
- comunicación e información de usuario final (por ejemplo, información privada).

Los requisitos tienen que proporcionar seguridad basada en la red y comunicaciones de usuario final a lo largo de dominios administrativos con múltiples redes como se muestra en la figura 23.

Estos requisitos, especificados en la Recomendación UIT-T Y.2701, se consideran como un conjunto mínimo de requisitos. Un proveedor de NGN puede necesitar tomar medidas adicionales más allá de las especificadas.

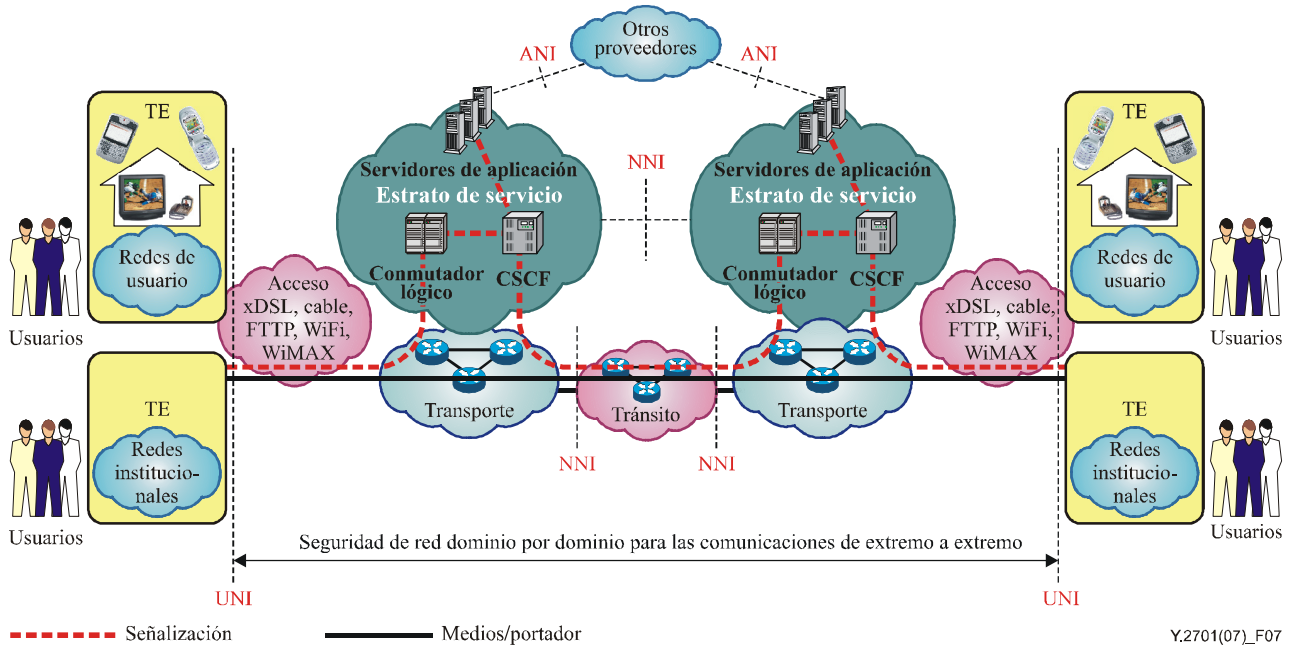


Figura 23 – Seguridad de las comunicaciones a través de múltiples redes

8.2 Seguridad de las comunicaciones móviles

Las comunicaciones móviles están evolucionando desde la movilidad limitada a una tecnología específica (por ejemplo, GSM o AMDC) a la movilidad a través de redes heterogéneas (por ejemplo, GSM, Wi-Fi, RTPC), haciendo uso del protocolo de Internet. En otras palabras, las futuras redes implicarán la integración de las futuras redes inalámbricas y sin hilos prestando una amplia gama de nuevos servicios que no se podrían proporcionar mediante una única red existente.

Con el desarrollo de la verdadera convergencia entre el servicio fijo y el móvil (FMC), un usuario móvil puede itinerar a través de redes heterogéneas tales como GSM, LAN inalámbrica y Bluetooth. Los requisitos de seguridad para cada tipo de acceso se deberán cumplir de diferentes formas pero todos los requisitos de seguridad tienen que mantenerse para proteger a los usuarios, las redes y las aplicaciones de un acceso indebido.

Los asuntos de seguridad se pueden categorizar en términos generales como:

- problemas que surgen del uso del IP en aplicaciones inalámbricas móviles; y
- problemas que surgen del uso de múltiples redes de diversas tecnologías.

Los ataques por Internet y las vulnerabilidades amenazarán a las redes móviles inalámbricas que utilizan el protocolo de Internet como su protocolo de transporte. Además surgirán nuevas amenazas por las características de las nuevas redes inalámbricas, es decir, por su movilidad. Los mecanismos de seguridad que se han desarrollado para las redes IP pueden no satisfacer todas las necesidades de seguridad de los sistemas inalámbricos basados en IP y, por lo tanto, puede ser necesario desarrollar nuevas o mejores medidas de seguridad IP. Además, la seguridad se tiene que garantizar no sólo para la interfaz radioeléctrica sino también para el conjunto del servicio de extremo a extremo y tiene que ser suficientemente flexible para proporcionar diversos niveles de seguridad adaptados al servicio o aplicación que se está prestando. Con el

despliegue de los servicios y aplicaciones móviles por IP las medidas de seguridad son mucho más importantes para el usuario, el operador y el proveedor de servicio.

Al participar múltiples redes, aumentan las oportunidades de amenaza, como intercepción ilegal de perfiles de usuario, contenido (por ejemplo, comunicación de voz o de datos) e información de autenticación.

Las telecomunicaciones móviles internacionales-2000 (IMT-2000) que constituyen una norma mundial para la tercera generación (3G) de comunicaciones inalámbricas, se definen mediante un conjunto de Recomendaciones de la UIT independientes. Las IMT-2000 proporcionan un marco para el acceso inalámbrico en todo el mundo, vinculando los diversos sistemas de redes terrenales y/o por satélite. Aprovecharán la sinergia potencial entre las tecnologías y sistemas de telecomunicaciones digitales móviles para los sistemas de acceso inalámbrico fijo y móvil.

Las actividades de la UIT en las IMT-2000 incluyen la normalización internacional, en particular el espectro de frecuencias y las especificaciones técnicas para los componentes radioeléctricos y de red, las tarifas y la tarificación, la asistencia técnica y los estudios sobre aspectos reglamentarios y políticos.

Los amplios requisitos para las redes IMT-2000 se consideran en las Recomendaciones UIT-T Q.1701, Marco para las redes de las IMT-2000, UIT-T Q.1702, Visión a largo plazo de las características de las redes de sistemas posteriores a las IMT-2000 y UIT-T Q.1703, Marco de capacidades de servicio y de red desde la perspectiva de la red para los sistemas posteriores a las IMT-2000.

Además, las especificaciones 3G incluidas en la serie de Recomendaciones UIT-T Q.1741 (3GPP) y en la serie UIT-T Q.1742 (3GPP2) incluyen una evaluación de las amenazas percibidas y una lista de requisitos de seguridad para contrarrestar esas amenazas. Estas Recomendaciones también incluyen objetivos y principios de seguridad para las comunicaciones móviles, una arquitectura definida de seguridad, requisitos de algoritmos criptográficos, requisitos de interceptación legal y una arquitectura y funciones de interceptación legal.

8.2.1 Comunicaciones de datos móviles seguras de extremo a extremo

Hay muchos terminales móviles disponibles con capacidad de comunicación de datos (por ejemplo, teléfonos móviles IMT-2000, ordenadores portátiles y agendas digitales personales (PDA) con tarjeta inalámbrica) y diversos servicios de aplicación (por ejemplo, comercio electrónico móvil) utilizan terminales conectados a la red móvil. Una seguridad eficaz es esencial para aplicaciones comerciales así como para la protección del usuario final.

Las redes móviles son particularmente vulnerables debido a la propia naturaleza de las redes inalámbricas y a las vulnerabilidades inherentes a las tecnologías de comunicación inalámbrica. Se debe considerar la seguridad desde el punto de vista del operador de la red móvil, del operador del servicio de aplicación y del usuario final. Resulta de particular importancia la seguridad entre el terminal móvil y el servidor de aplicación. Para tratar las comunicaciones móviles de extremo a extremo, el UIT-T ha elaborado un conjunto completo de soluciones de seguridad, algunas de las cuales se consideran a continuación.

8.2.1.1 Marco para las comunicaciones de datos móviles seguras de extremo a extremo

En la Recomendación UIT-T X.1121, *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*, se describen dos modelos de comunicaciones seguras móviles de datos de extremo a extremo entre un usuario móvil y un proveedor de servicio de aplicación (ASP): un modelo general y un modelo de pasarela, como se muestra en las figuras 24 y 25. El ASP proporciona servicios a los usuarios móviles a través del servidor de aplicación. En el modelo de pasarela, la pasarela de

seguridad retransmite paquetes del terminal móvil al servidor de aplicación y transforma un protocolo de comunicaciones de red móvil en un protocolo de red abierta y viceversa.

La figura 26 muestra las amenazas en la red de comunicaciones móviles de datos de extremo a extremo.

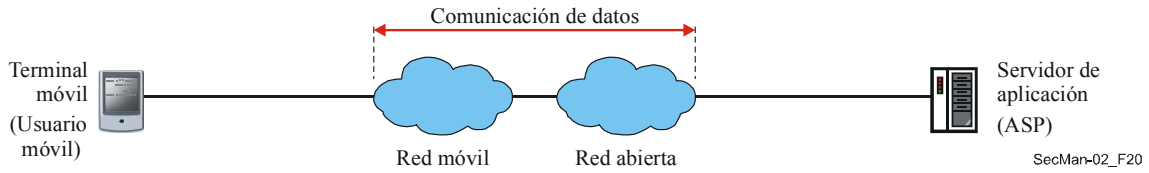


Figura 24 – Modelo general de comunicación de datos de extremo a extremo entre un usuario y un ASP

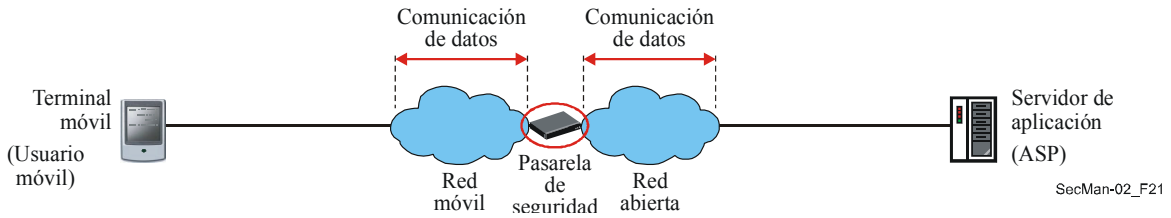


Figura 25 – Modelo de pasarela para las comunicaciones móviles de datos de extremo a extremo entre un usuario móvil y un ASP

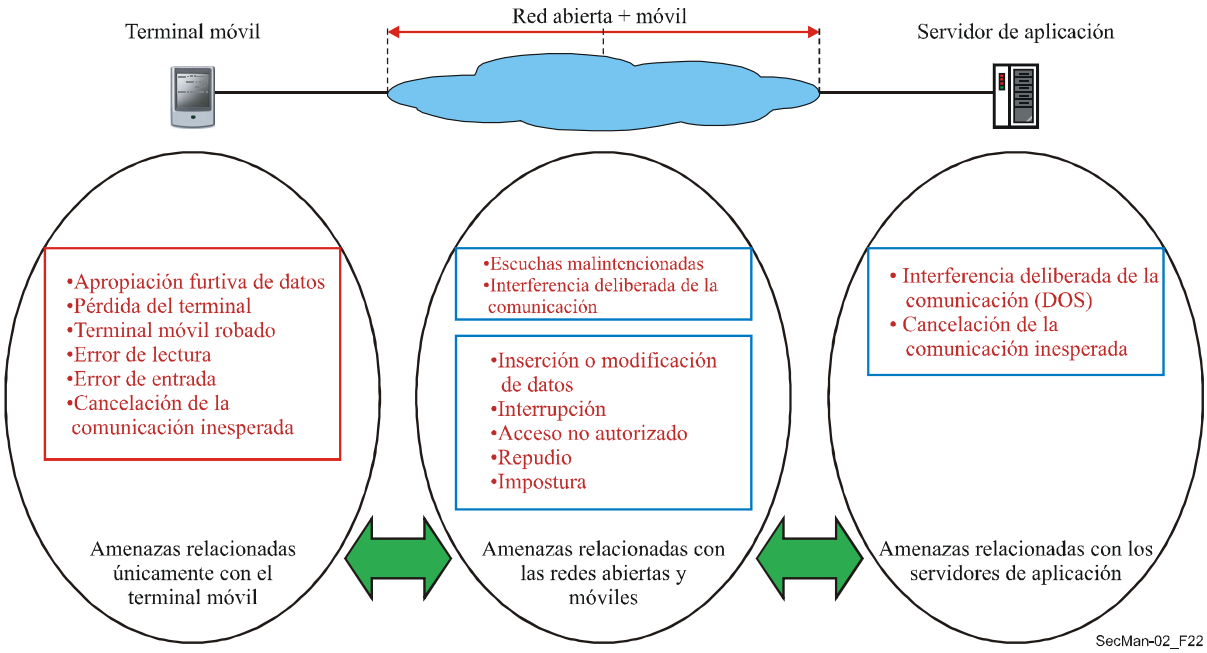


Figura 26 – Amenazas para las comunicaciones móviles de extremo a extremo

La figura 27 muestra dónde se requieren características de seguridad para cada una de las entidades y la relación entre las entidades.

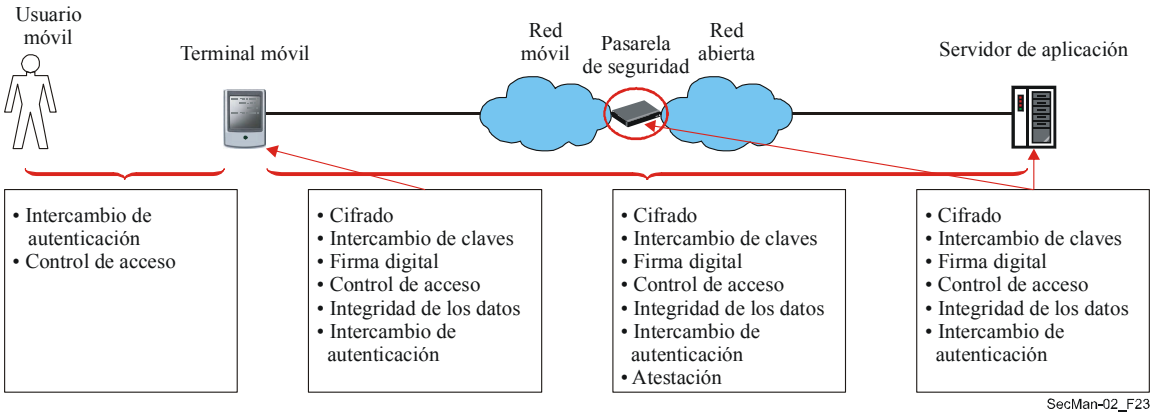


Figura 27 – Funciones de seguridad requeridas para cada entidad y relación entre entidades

8.2.1.2 PKI para las comunicaciones móviles de datos de extremo a extremo seguras

La tecnología PKI es muy útil para facilitar algunas de las funciones de seguridad (por ejemplo, confidencialidad, firma digital, integridad de los datos) que se precisan para las comunicaciones móviles de datos de extremo a extremo pero, debido a las características de esas comunicaciones, se requieren algunas medidas de adaptación. En la Recomendación UIT-T X.1122, *Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas*, que proporciona un modelo PKI general y un modelo PKI de pasarela, se presentan directrices sobre la implementación de la tecnología PKI.

En el modelo general (que se muestra en la figura 28), la CA del usuario expide el certificado y gestiona el registro y la lista de revocación de certificados (CRL). La autoridad de validación de usuario móvil proporciona un servicio de validación de certificados en línea para los usuarios móviles. La CA del ASP expide un certificado del proveedor de servicios de aplicación y gestiona el registro del ASP y la CRL. La autoridad de validación del ASP proporciona un servicio de validación de certificados en línea para los certificados de ASP.

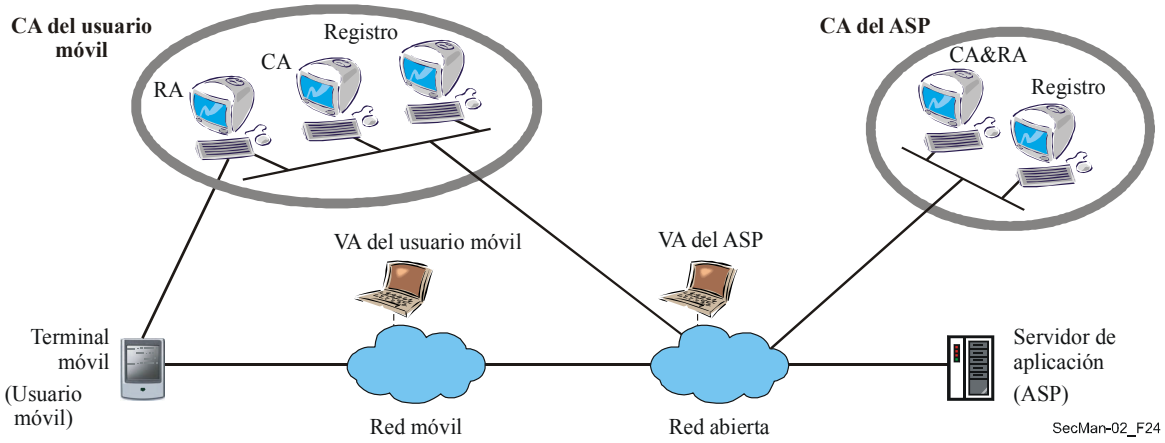


Figura 28 – Modelo PKI general para las comunicaciones móviles de datos de extremo a extremo

Hay dos métodos de expedición de certificados, dependiendo de la ubicación en la que se generan las claves públicas/privadas. En uno, 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, anexa al terminal móvil. En la figura 29 se muestra el procedimiento según el cual un

terminal móvil adquiere un certificado en el que el par de claves criptográficas se genera en el terminal móvil.

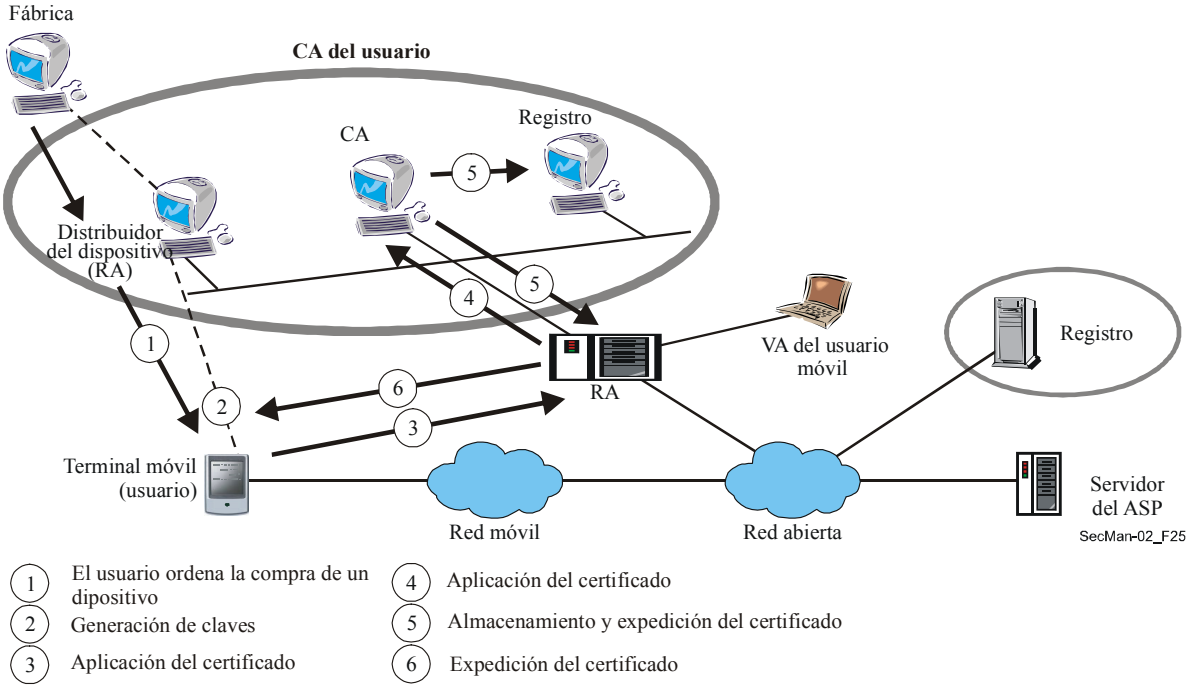


Figura 29 – Procedimiento de expedición de certificados por terminal móvil

El terminal móvil tiene una capacidad computacional y una memoria limitadas. Por eso es preferible utilizar la validación de certificados en línea, en lugar de la validación de certificados fuera de línea basado en una CRL. En la figura 30 se muestra el procedimiento de validación de certificados en línea para un terminal móvil.

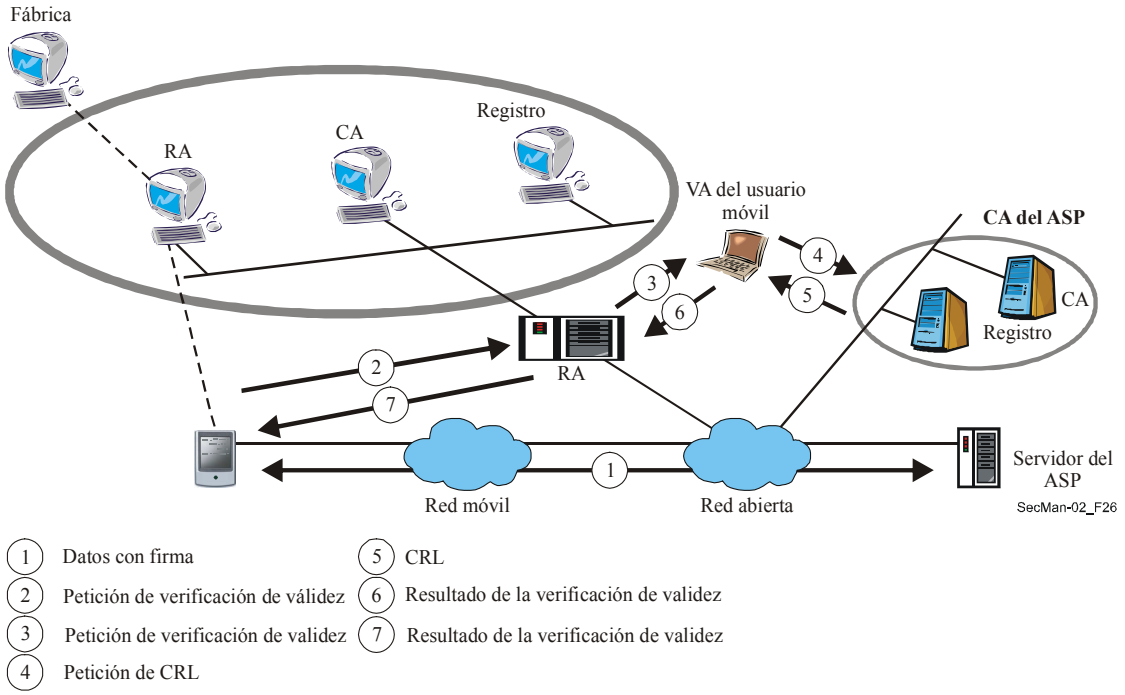


Figura 30 – Validación de certificados para las comunicaciones móviles de datos extremo a extremo

La PKI para comunicación móvil de extremo a extremo se puede utilizar en la capa de sesión donde puede soportar servicios de seguridad, tales como autenticación de cliente, autenticación de servidor, confidencialidad y servicio de integridad o en una aplicación en la que puede prestar servicios de no repudio y confidencialidad.

8.2.1.3 Sistema de reacción correlativo en comunicaciones móviles de datos

El sistema de reacción correlativo se ha concebido para permitir a los terminales y dispositivos móviles y a la red cooperar juntos frente a las amenazas de seguridad. La Recomendación UIT-T X.1125 describe la arquitectura genérica de un sistema de reacción correlativo en el que una red móvil y sus terminales de usuario pueden cooperar interactivamente para combatir diversas amenazas de seguridad y conseguir comunicaciones seguras de datos de extremo a extremo. Entre estas amenazas se encuentran, por ejemplo, virus, gusanos, caballos de Troya u otras amenazas de red contra la red móvil y sus usuarios.

Esta arquitectura proporciona redes de operador que mejoran la capacidad de seguridad mediante actualizaciones de seguridad de la estación móvil, control de acceso de red y restricciones de servicios de aplicación, que proporcionan un mecanismo que impide a los virus y a los gusanos propagarse con rapidez a través de la red del operador.

8.3 Seguridad para redes domésticas

Puesto que una red doméstica utiliza diversas técnicas de transmisión por hilos o inalámbricas, está expuesta a amenazas similares a las de cualquier otra red alámbrica o inalámbrica. Para proteger la red doméstica de esas amenazas, el UIT-T ha desarrollado un conjunto completo de soluciones para los servicios de red domésticos, algunas de las cuales se consideran a continuación.

8.3.1 Marco de seguridad para las redes domésticas

La Recomendación UIT-T X.1111, *Marco de tecnologías de la seguridad para redes domésticas*, se basa en el modelo de amenaza de la Recomendación UIT-T X.1121 para establecer un marco de seguridad para las redes domésticas. Las características de la red doméstica se pueden resumir como sigue:

- se pueden utilizar en la red diversos medios de transmisión;
- la red puede incluir tecnologías alámbricas y/o inalámbricas;
- se pueden considerar muchos entornos posibles desde el punto de vista de la seguridad;
- usuarios distantes pueden transportar terminales distantes; y
- cada tipo de dispositivo de red doméstico requiere diferentes niveles de seguridad.

El modelo general de seguridad de la red doméstica, que se muestra en la figura 31, puede incluir muchos dispositivos tales como PDA, ordenadores personales y TV/VCR. En este modelo, los dispositivos domésticos se clasifican en uno de los tres tipos siguientes:

- dispositivos de tipo A, tales como controladores remotos, ordenadores personales o PDA, que tienen la capacidad para controlar un dispositivo de tipo B o tipo C;
- dispositivos de tipo B, que sirven para conectar dispositivos de tipo C (que no disponen de interfaz de comunicaciones) con la red, es decir, un dispositivo de tipo B comunica con otros dispositivos en la red utilizando un lenguaje propio o un mecanismo de control; y
- dispositivos de tipo C, tales como cámaras de seguridad y dispositivos A/V que prestan un servicio al resto de los dispositivos.

Algunos de los dispositivos combinan funciones de tipo A y tipo C.

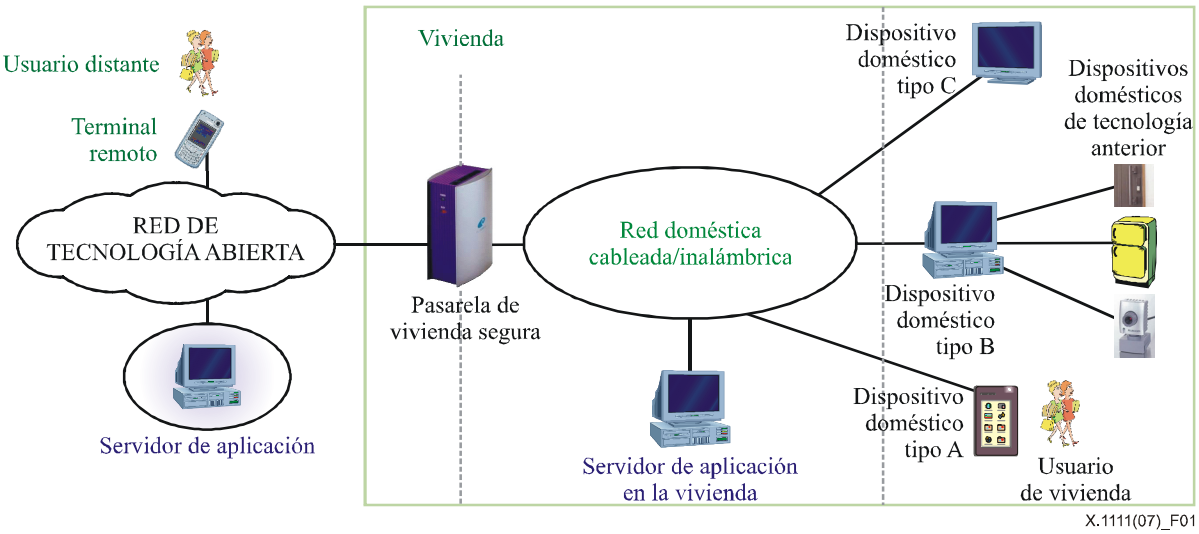


Figura 31 – Modelo general de red doméstica para la seguridad

La Recomendación UIT-T X.1111 describe las amenazas de seguridad y los requisitos de seguridad desde el punto de vista del usuario doméstico y del usuario distante. Además, clasifica las tecnologías de seguridad en términos de funciones que satisfacen los requisitos de seguridad y por la ubicación en la que deben aplicarse las tecnologías de seguridad.

8.3.2 Certificación y autenticación de dispositivos en redes domésticas

Existen dos opciones para la certificación de dispositivos en la red doméstica: el modelo de emisión externa en el que todos los certificados de dispositivos domésticos se expiden por una CA externa; y el modelo de emisión interna en el que los certificados de los dispositivos (incluidos los certificados autofirmados y los certificados de entidad final) son expedidos por una CA interna en la red doméstica. Normalmente, una CA interna es una pasarela doméstica segura con la capacidad de generar un par de claves y emitir un certificado, es decir, la pasarela doméstica puede emitir tanto un certificado CA como certificados de dispositivo doméstico. La propia pasarela doméstica segura puede tener un certificado de dispositivo emitido por una entidad de certificación externa para su uso en servicios domésticos externos. Este certificado de dispositivo de pasarela doméstico expedido externamente se puede utilizar para la autenticación entre la pasarela doméstica y el proveedor de servicio de red.

La Recomendación UIT-T X.1112 describe un marco para el modelo interno de emisión de certificados de dispositivos, su gestión y uso por redes domésticas. El modelo se ilustra en la figura 32.

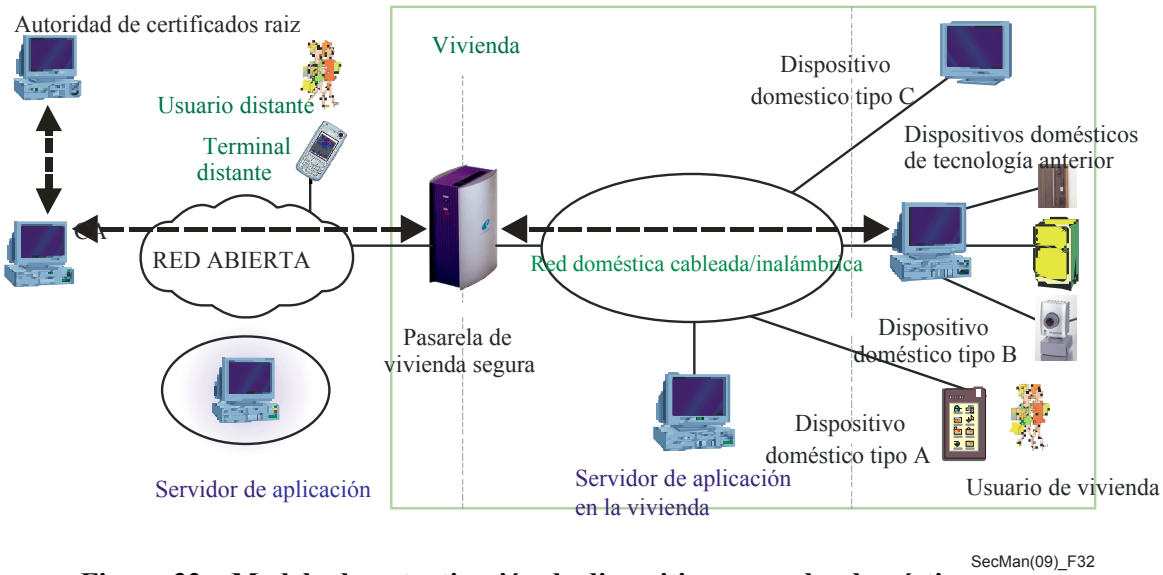


Figura 32 – Modelo de autenticación de dispositivos en redes domésticas seguras

Para la autenticación de dispositivos, se precisa un único identificador para cada dispositivo en la red doméstica. En particular, se precisará un certificado de dispositivo doméstico como único elemento de confianza cuando se utilice en la red doméstica.

La figura 33 muestra cuatro casos típicos de uso de un certificado de dispositivo: 1) entre el terminal distante y la pasarela doméstica segura; 2) entre el servidor de aplicación y la pasarela doméstica segura; 3) entre dispositivos domésticos y la pasarela doméstica segura; y 4) entre dispositivos domésticos.

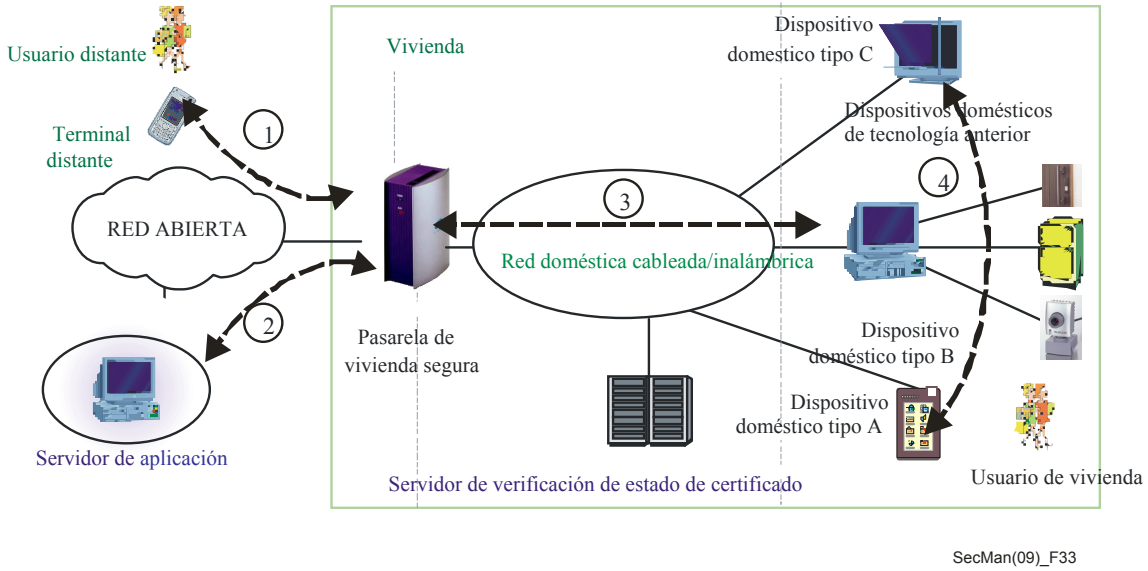


Figura 33 – Caso de uso de autenticación de dispositivos basado en el modelo de red doméstica general para la seguridad

Para servicios de Internet externos desde el dispositivo doméstico al servidor de aplicación externo se debería autenticar el dispositivo doméstico en primer lugar con una pasarela doméstica segura utilizando su propio certificado de dispositivo. La pasarela doméstica segura debería ser entonces autenticada con el servidor de aplicación externo utilizando el certificado de pasarela doméstico emitido por una CA externa. Estos casos de uso se pueden aplicar a diversos protocolos de aplicación para soportar servicios de redes domésticas seguros.

8.3.3 Autenticación de usuario humano para servicios de red doméstica

Algunos entornos exigen la autenticación del usuario humano en lugar de la de un proceso o un dispositivo. En estos casos, el sistema de autenticación requiere que los usuarios humanos demuestren su singularidad. Esta singularidad se basa generalmente en características tales como algo conocido, algo que se posee o algo absolutamente característico del usuario.

La Recomendación UIT-T X.1113 proporciona directrices sobre autenticación de usuario en redes domésticas con el fin de permitir diversas técnicas de autenticación tales como contraseñas, certificados y características biométricas. También define el nivel de garantía de seguridad y el modelo de autenticación en función de los casos de servicios de autenticación. La figura 34 muestra los flujos de servicios de autenticación basados en el modelo general de seguridad de redes domésticas definidos en la Recomendación UIT-T X.1111. En este ejemplo, un usuario distante intenta acceder a entidades en la vivienda, mientras que el usuario doméstico intenta acceder a entidades dentro o fuera de su domicilio.

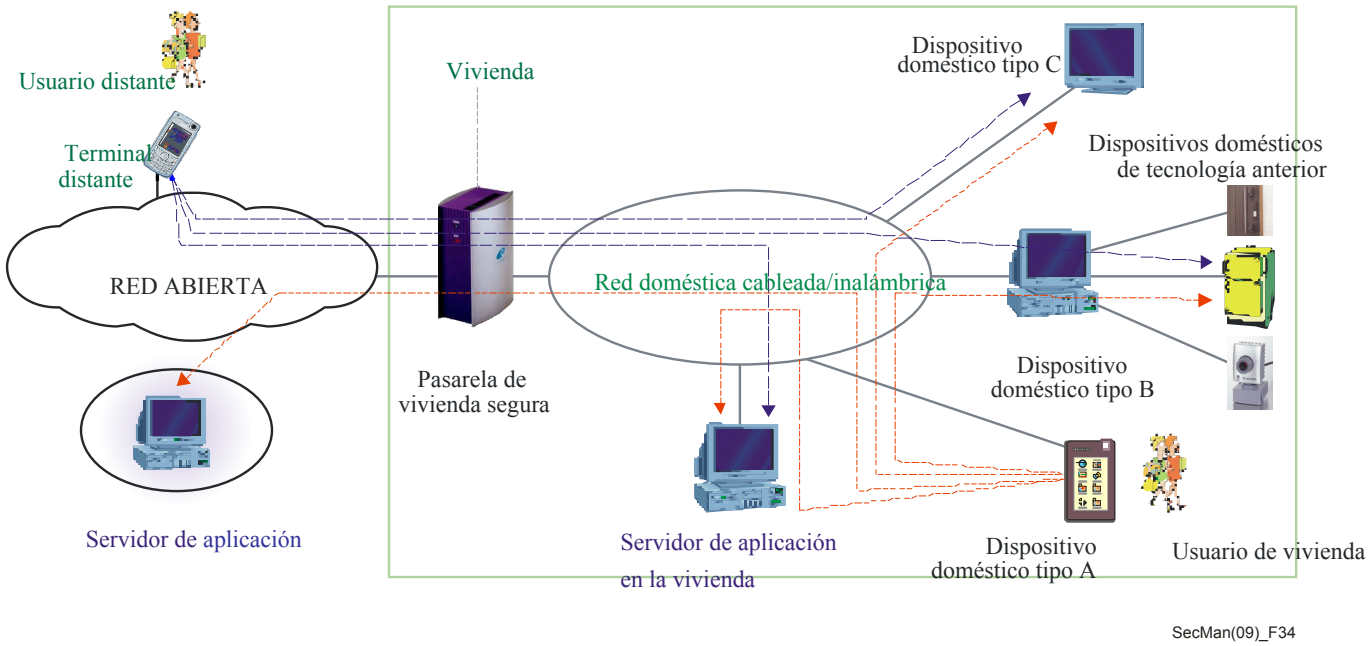


Figura 34 – Flujos de servicio de autenticación en redes domésticas

8.4 IPCablecom

El sistema IPCablecom permite a los operadores de televisión por cable prestar servicios en tiempo real basados en IP (por ejemplo, comunicaciones de voz) mediante redes que se han mejorado para soportar módems de cable.

8.4.1 Arquitectura IPCablecom

La arquitectura IPCablecom se define en la Recomendación UIT-T J.160. En la figura 35 se muestran los componentes IPCablecom. La arquitectura del sistema IPCablecom incluye tanto elementos de red fiables como no fiables. Los elementos de red fiables normalmente están situados en una red de operador troncal gestionada. Los elementos de red no fiables, tales como el modem de cable o el adaptador de terminal de medios (MTA), normalmente están ubicados fuera de las instalaciones del operador de cable en la vivienda del abonado.

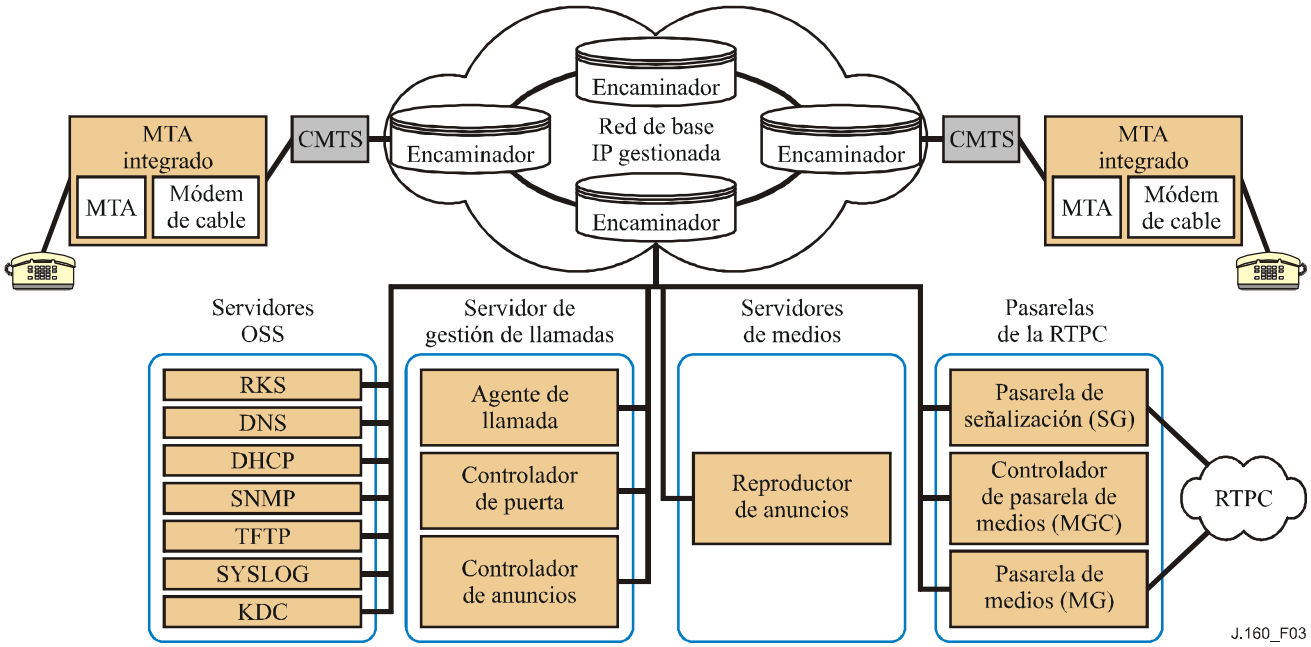


Figura 35 – Modelo de referencia de los componentes IPCablecom

8.4.2 Requisitos de seguridad para IPCablecom

Cada una de las interfaces de protocolo para IPCablecom está sometida a amenazas que podrían afectar tanto al abonado como al proveedor de servicio. Por ejemplo, el trayecto del tren de medios puede atravesar un gran número de proveedores de servicio de Internet y nodales potencialmente desconocidos. En consecuencia, el tren de medios puede ser vulnerable a escuchas clandestinas malintencionadas que resulten en una pérdida de privacidad en la comunicación. Los objetivos de diseño de seguridad identificados en la arquitectura IPCablecom son:

- permitir capacidades de voz residenciales con un nivel similar o mayor de privacidad percibida al de la PSTN;
- proporcionar protección frente a ataques en el MTA; y
- proteger al operador de cable de la ruptura de red, la denegación del servicio y la apropiación indebida de servicios.

Las consideraciones de diseño deben incluir la confidencialidad, la autenticación, la integridad y el control de acceso.

Los requisitos de seguridad se especifican en la Recomendación UIT-T J.170, *Especificación de seguridad del sistema IPCablecom*. Las amenazas que deben considerarse se resumen en las siguientes:

- robo de servicio, que incluye el fraude de suscripción; el impago por los servicios; los clones MTA (por ejemplo, cuando es clonado un MTA registrado en una cuenta fraudulenta); la suplantación de personalidad de un servidor de red; y la manipulación de protocolos;
- difusión de información del canal portador, que incluye: la simple curiosidad, los MTA clones (por ejemplo, de un MTA accesible por el público), la manipulación de protocolo, el análisis criptográfico fuera de línea y la interrupción de servicio;

- divulgación de información de señalización;
- apropiación indebida de los servicios basados en MTA; y
- registro ilegal de un MTA arrendado con un proveedor de servicio diferente.

8.4.3 Servicios y mecanismos de seguridad en IPCablecom

La seguridad en IPCablecom se implementa en los elementos de la pila de protocolos inferior y utiliza especialmente mecanismos definidos por el IETF. En la arquitectura IPCablecom se consideran las amenazas especificando, para cada interfaz de protocolo definida, los mecanismos de seguridad subyacentes (como por ejemplo IPsec) que proporcionan la interfaz del protocolo con los servicios de seguridad requeridos. Con arreglo a la arquitectura X.805, los servicios de seguridad para IPCablecom tienen en cuenta los nueve componentes resultantes de los tres planos y capas de la figura 1.

Los servicios de seguridad disponibles a través de la capa de servicio medular de IPCablecom son la autenticación, el control de acceso, la integridad, la confidencialidad y el no repudio. 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 claves (por ejemplo, IKE, PKINIT/Kerberos). Asimismo, entre los principales servicios de seguridad IPCablecom se incluye un mecanismo para la criptación de extremo a extremo de los trenes de medios RTP, reduciendo así sustancialmente la posibilidad de una amenaza a la privacidad.

8.5 IPCablecom2

IPCablecom2 es una iniciativa del sector del cable diseñada para soportar la convergencia de tecnologías de voz, video, datos y movilidad.

8.5.1 Arquitectura de IPCablecom2

IPCablecom2 se basa en la versión 6 del subsistema multimedios IP (IMS) definido por el proyecto de asociación de tercera generación (3GPP). El ámbito del 3GPP incluye la elaboración de especificaciones técnicas para las redes de sistemas móviles GSM y de tercera generación (3G), y el desarrollo de una arquitectura de comunicaciones por IP basadas en SIP para redes móviles. La arquitectura resultante, *El subsistema multimedios IP*, constituye la base de la arquitectura de IPCablecom2 definida en la Recomendación UIT-T J.360.

8.5.2 Requisitos de seguridad para IPCablecom2

Los objetivos de diseño para la arquitectura de seguridad de IPCablecom2 incluyen:

- soporte de confidencialidad, autenticación, integridad y mecanismos de control de acceso;
- protección de la red ante negación de servicio, interrupción de red, apropiación indebida de servicios;
- protección del equipo de usuario (UE) (es decir, de los clientes) ante ataques de negación de servicio, vulnerabilidades de seguridad, acceso no autorizado desde la red;
- soporte de la privacidad del usuario final mediante criptación y mecanismos que controlen el acceso a los datos de abonado tales como información de presencia;
- mecanismos para la autenticación de dispositivos, equipos de usuario y usuarios; suministro seguro, señalización segura y descarga segura de software; y

- establecimiento y ampliación de la arquitectura de seguridad IMS en la consecución de los objetivos establecidos anteriormente.

Las amenazas generales que aplican a IPCablecom2 son:

Amenazas al dominio de confianza

Un dominio de confianza es un agrupamiento lógico de elementos de red que están facultados para comunicar. Los dominios de confianza se pueden diferenciar mediante límites físicos o lógicos. La comunicación a través de los dominios de confianza tiene siempre que estar protegida con autenticación y autorización. Además, las interfaces que conectan los elementos de red dentro de un dominio, las interfaces entre dominios y las interfaces entre los usuarios y el proveedor de servicio tienen que ser seguras frente a diversas amenazas.

Robo del servicio

El robo del servicio se puede lograr de muchas maneras, entre otras mediante: la manipulación del equipo de usuario; la explotación de las debilidades del protocolo; la falsificación de la identidad; la copia del equipo de usuario (es decir, imitando a un usuario final legítimo); y el fraude de abonado y el impago de los servicios.

Interrupción y negación del servicio

Incluye la negación general de los ataques de servicio; los ataques por inundación (es decir, la inhabilitación de un determinado elemento de red, normalmente enviando una cantidad excesiva de tráfico de red de medios hacia sus interfaces); y los ataques con zombis (es decir, muchos sistemas de punto final comprometidos).

Señalización de amenazas de canal

En un entorno multimedios, los mensajes de señalización incluyen datos relativos a la identidad, los servicios, el encaminamiento y otros datos sensibles y críticos. Existen componentes multimedios tales como los intermediarios en el dominio de acceso, exponiéndolo a un mayor número de amenazas. Los ataques contra las amenazas de señalización incluyen: compromiso de confidencialidad de la información de señalización; ataques mediante intermediarios debidos a la intercepción y la posible modificación del tráfico que pasa entre dos partes en comunicación; y negación de los ataques de servicio en la gama de canales de señalización.

Amenazas de canal portador

Las amenazas al canal portador están relacionadas con el tráfico de medios transferido entre las partes en comunicación.

Amenazas de seguridad específicas del protocolo

Existen diversas amenazas contra cada uno de los protocolos multimedios.

8.5.3 Servicios y mecanismos de seguridad en IPCablecom2

IPCablecom2 hace un amplio uso de la seguridad de capa de transporte y de otros mecanismos referenciados en el subsistema multimedios 3GPP IP (3GPP 23.002 v6.10.0, *Arquitectura de red*, diciembre de 2005). Las secciones siguientes resumen las mejoras de IPCablecom2 en la arquitectura de seguridad IMS.

8.5.3.1 Autenticación de usuario y del equipo de usuario

La arquitectura IPCablecom2 soporta los mecanismos de autenticación siguientes:

- autenticación del subsistema multimedios IP y acuerdo de cable;
- autenticación de ingestión de protocolo de inicio de sesión (SIP); y
- inicialización de certificado.

La arquitectura acomoda a los equipos de usuario con múltiples credenciales de autenticación. Por ejemplo, un equipo de usuario puede tener un certificado para acceder a servicios mientras se encuentre en una red de cable, y una tarjeta universal de circuito integrado (UICC) lo tendrá para acceder a los servicios mientras se encuentra en una red celular.

Un abonado puede tener múltiples credenciales. Un abonado puede tener múltiples equipos de usuario con diferentes capacidades relacionadas con esas credenciales. Por ejemplo, un usuario puede tener un MTA con un certificado para uso doméstico y un equipo de usuario basado en UICC para viajar.

8.5.3.2 Seguridad de señalización

IPCablecom2 añade la seguridad de capa de transporte (TLS) como una posibilidad para la seguridad de señalización entre el equipo y la función de control de la sesión de llamada de intermediario. El uso de TLS (como define el subsistema multimedios IP (IMS)) es optativo para la seguridad de señalización.

8.6 Seguridad para redes de sensores ubicuos

Un sensor es sencillamente un dispositivo que genera una señal eléctrica que representa una propiedad física que se puede medir. Una red de sensores ubicuos (USN) es una red que utiliza sensores de bajo coste y reducida potencia para reconocer el entorno con el fin de obtener información y servicios de conocimiento para todos, en cualquier lugar y en cualquier momento. Una USN puede cubrir una zona geográfica amplia y puede soportar diversas aplicaciones. La figura 36 muestra las posibles aplicaciones de una USN.

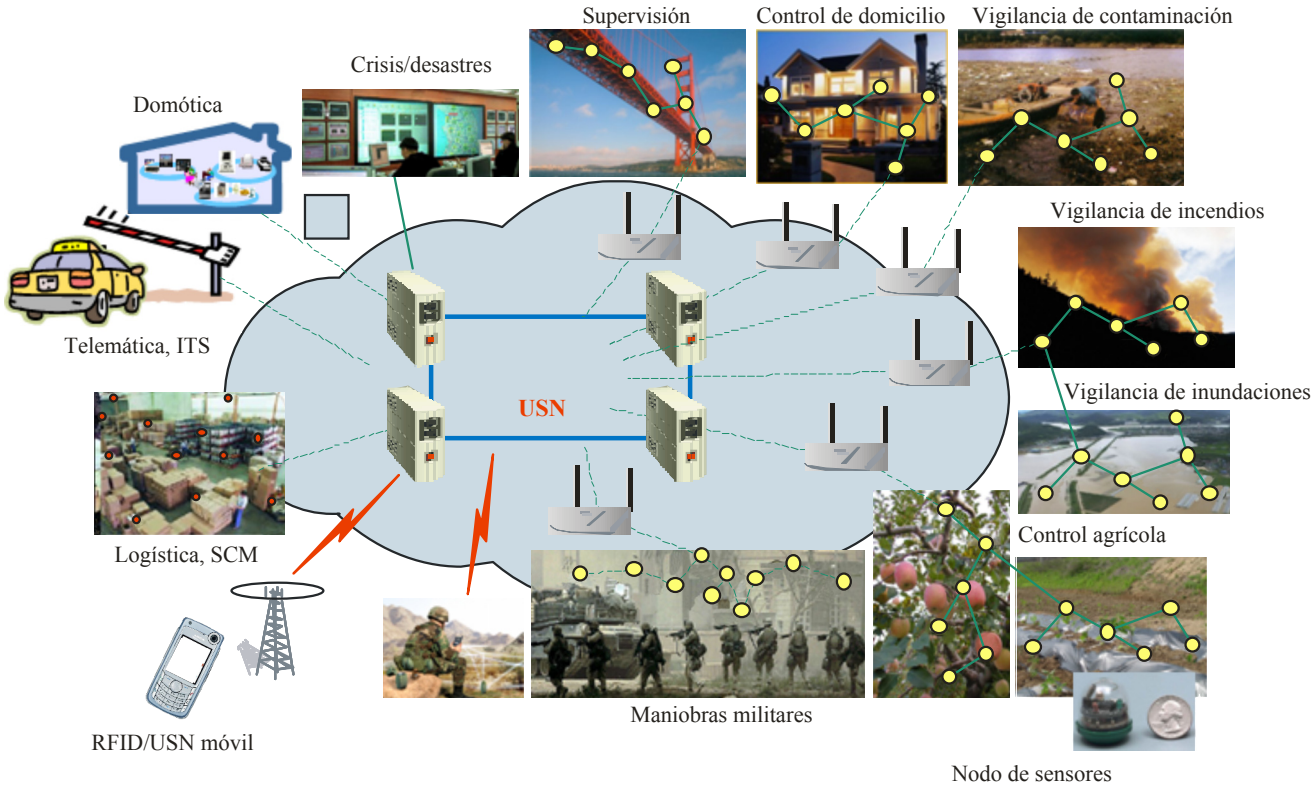


Figura 36 – Posibles aplicaciones USN

Las redes de sensores normalmente están conectadas a redes de usuarios finales y, aunque las redes nucleares de transmisión es probable que utilicen Internet y tecnologías de la próxima generación, utilizarán diversas tecnologías subyacentes (como DSL, satélite, GPRS, AMDC, GSM, etc.).

Puesto que la transferencia de información en una USN se enfrenta a muchas posibles amenazas, se precisan técnicas de seguridad efectivas para contrarrestarlas.

Además de las amenazas habituales de la red, (como las tratadas en la sección 3) existen amenazas específicas a las USN como por ejemplo:

- **infección del nodo de sensores**, debido a ataques o infecciones a los propios sensores o mediante un atacante que incluye sensores ilícitos;
- **escuchas clandestinas**, espiando las transmisiones entre nodos;
- **infección o exposición de los datos de los sensores**;
- **ataques de negación de servicio** contra los sensores o las comunicaciones; y
- **uso malicioso o uso incorrecto de de los sensores de red**, por ejemplo, utilizando los sensores para fines ilegales.

Además, las USN están sometidas a algunas amenazas relacionadas con el encaminamiento a los nodos de sensores.

Las características de una red de sensores complican en gran medida el proceso de diseño de redes seguras. Por ejemplo, debido a limitación de capacidad de cálculo y memoria de los nodos de sensores y a su reducida

potencia y anchura de banda no es posible utilizar criptografía de red pública o almacenar claves únicas con los nodos. Además, los sensores pueden estar ubicados en entornos hostiles y puede que no se conozca su ubicación exacta tras el despliegue. Finalmente, la red de sensores depende en gran medida de su estación base, que no es sólo un posible punto de fallo, sino también un objetivo tentador para los atacantes.

El soporte intermedio de USN facilita una plataforma de aplicación común para soportar diversas funciones en lugar de las aplicaciones y servicios USN y para controlar las redes de sensores. La gran cantidad de datos recogidos por la red de sensores se almacena, gestiona y analiza mediante programas informáticos USN que también tienen que suministrar datos seguros a las aplicaciones correspondientes. Las medidas de seguridad mediante soporte intermedio tienen que considerar la seguridad de los datos mientras estén almacenados y durante las transmisiones así como la seguridad del soporte intermedio.

Aunque las Recomendaciones USN todavía no se han finalizado, los trabajos están encaminados a considerar tanto las necesidades de seguridad de la propia USN como las del soporte intermedio USN.

9. Seguridad de aplicación

9 Seguridad de aplicación

Los diseñadores de aplicaciones, cada vez más conscientes de la importancia de la seguridad, están prestando una creciente atención a la necesidad de introducir la seguridad en sus productos, en lugar de intentar incluir la seguridad después de que la aplicación haya pasado a la fase de producción. A pesar de ello, la mayoría de las aplicaciones muestran en algún momento de su desarrollo que tienen vulnerabilidades inherentes. Además, la evolución de las amenazas a menudo expone y aprovecha vulnerabilidades desconocidas anteriormente.

En esta sección se analizan las características de seguridad de ciertas aplicaciones de las TIC, en particular las características de seguridad consideradas por las Recomendaciones del UIT-T.

9.1 Voz sobre IP (VoIP) y multimedios

La voz sobre IP, conocida también como telefonía IP, consiste en la prestar los servicios que tradicionalmente se ofrecen a través de la red pública telefónica conmutada (RPTC) mediante una red que utilice el protocolo de Internet (IP). Estos servicios incluyen antes que nada el tráfico de voz, pero también otros medios como el video y los datos. El sistema VoIP también incluye los servicios complementarios correspondientes, tales como conferencia (conexión puente), reenvío de llamada, llamada en espera, multilínea, desvío de llamada, depósito y extracción de llamada, consulta y seguimiento de llamada, entre otros servicios de red inteligente. La voz por Internet es un caso particular del desarrollo de la VoIP en el que el tráfico de voz se hace pasar a través de la red troncal pública de Internet.

La Recomendación UIT-T H.323, *Sistemas de comunicaciones multimedios basados en paquetes*, es una Recomendación general que proporciona los fundamentos de las comunicaciones de audio, video y datos por redes de conmutación de paquetes, incluida Internet, redes de área local (LAN) y redes de área extensa (WAN) que no proporcionan una calidad de servicio (QoS) garantizada. Este tipo de redes son las que se imponen en la industria hoy en día y entre ellas se encuentran las redes TCP/IP y el intercambio de paquetes por Internet (IPX) por Ehernet, Ethernet rápido y las tecnologías de red en anillo con paso de testigo. Al cumplir la Recomendación UIT-T H.323, los productos y aplicaciones multimedios de los diferentes fabricantes pueden interfuncionar entre ellos permitiendo así que los usuarios se comuniquen sin tener que preocuparse por los aspectos de compatibilidad. La Recomendación UIT-T H.323 fue el primer protocolo VoIP definido y se considera la piedra angular de los productos basados en VoIP para aplicaciones del mercado de consumo, de empresas, de proveedores de servicio, de ocio y profesionales. Las especificaciones de seguridad para la serie de Recomendaciones UIT-T H.323 se encuentran en la Recomendación UIT-T H.Imp235, *Guía para implementadores sobre la Recomendación UIT-T H.235 V3: "Seguridad y encriptado para la serie H (UIT-T H.323 y otras Recomendaciones UIT-T basadas en H.245) terminales multimedios"*, la Recomendación UIT-T H.235.x, una serie de nueve marcos y normas de seguridad y la Recomendación UIT-T H.530, *Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación UIT-T H.510*. La movilidad para los sistemas y servicios multimedios UIT-T H.323 se consideran en la Recomendación UIT-T H.510.

La Recomendación UIT-T H.323 es amplia e incluye tanto dispositivos individuales como tecnología de ordenadores personales incorporada, así como comunicaciones punto a punto y multipunto.

La Recomendación UIT-T H.323 define cuatro componentes principales para un sistema de comunicaciones basado en la red: terminales, pasarelas, controladores y unidades de control multipunto. Además, también son posibles elementos de frontera o pares. Estos elementos se muestran en la figura 36.

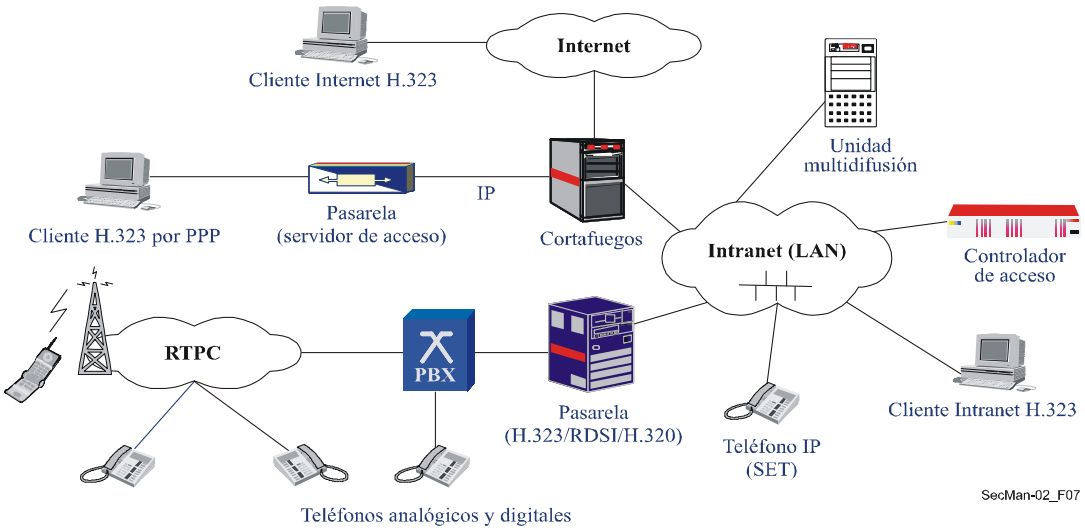


Figura 37 – Sistema H.323: componentes y casos de implementación

La Recomendación UIT-T H.323 es utilizada, por ejemplo, por los operadores al tráfico al por mayor en particular por las rutas troncales de VoIP y los servicios de llamadas con tarjetas. En las comunicaciones empresariales, la Recomendación UIT-T H.323 se utiliza para centralitas IP-PBX, IP-centrex, VPN para tráfico de voz, sistemas integrados de voz y datos, teléfonos Wi-Fi, implementación de centros de llamadas y servicios de movilidad. En el caso de comunicaciones profesionales, se utiliza ampliamente para las conferencias de voz (o audio) y video para la colaboración vocal/de datos/de video y para la formación a distancia. Los particulares la utilizan 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.

9.1.1 Aspectos de seguridad en multimedios y VoIP

Al estar geográficamente distribuidos, y debido a la naturaleza abierta de las redes IP, todos los elementos de un sistema UIT-T H.323 están expuestos a amenazas como se muestra en la figura 38.

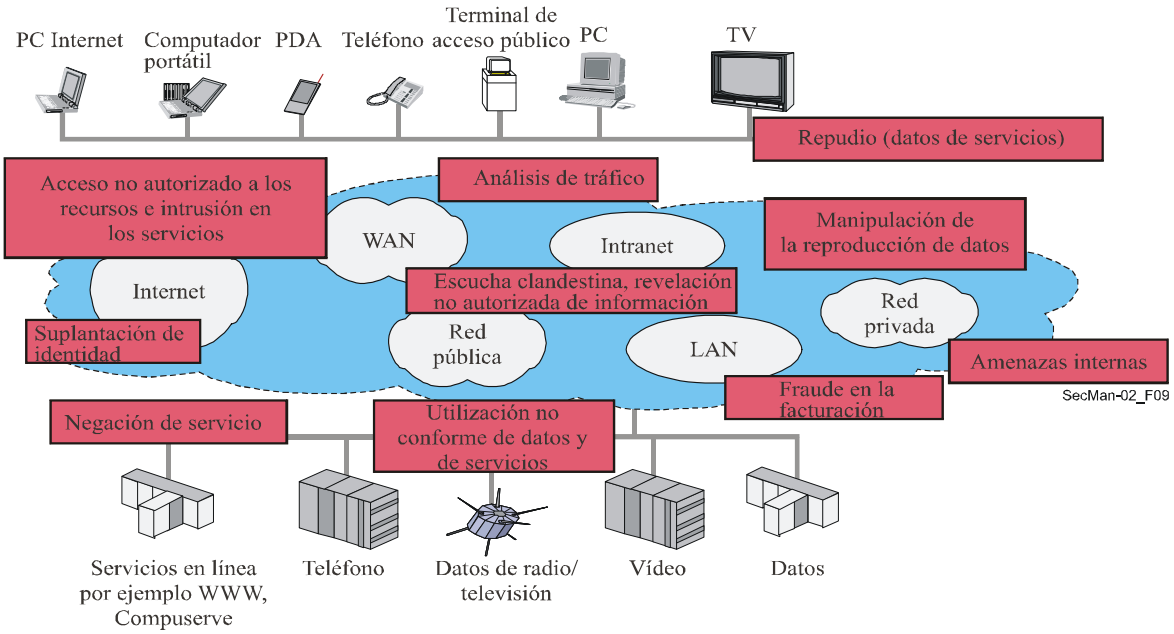


Figura 38 – Amenazas contra la seguridad en las comunicaciones multimedios

Los aspectos de seguridad más importantes en las comunicaciones multimedios y en la telefonía IP son los siguientes:

- 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, 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 UIT-T X.509).
- 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.
- Autenticación de usuario/terminal y servidor: Se precisa para contrarrestar las amenazas de seguridad tales como la usurpación de identidad, los ataques por intermediario, la simulación de dirección IP y el asalto de la conexión.
- Autorización de llamada: Se trata del proceso de toma de decisiones tendiente a establecer si se permite al usuario/terminal utilizar 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.
- 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 para evitar cualquier degradación del servicio causada por el procesamiento de seguridad.

- Confidencialidad en las transmisiones vocales: se logra mediante la criptación de los paquetes de voz para proteger de las escuchas clandestinas. En general, también se criptan los paquetes de medios (por ejemplo, vídeo) de las aplicaciones multimedios, así como los datos de voz. La protección avanzada de los paquetes de medios incluye también la protección de autenticación e integridad de las cabidas útiles.
- 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 la sustitución 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.
- Seguridad entre dominios: tiene que ver con el problema que suele presentarse cuando los sistemas de entorno heterogéneo han implementado características diferentes de seguridad, ya sea debido a requisitos, políticas de seguridad y capacidades de seguridad diferentes. Siendo así, se han de negociar dinámicamente los perfiles y capacidades de seguridad, tales como los algoritmos de criptografía y sus parámetros. Este aspecto es particularmente importante cuando se trata de pasar entre fronteras de dominios y se cuenta con diversos proveedores y redes. La capacidad de atravesar sin problemas los cortafuegos y acomodarse a las restricciones de los dispositivos de traducción de dirección de red (NAT) es un requisito muy importante de seguridad en las comunicaciones entre dominios.

Si bien esta lista no es extensiva, sí constituye el núcleo de la seguridad UIT-T H.323. Entre los aspectos de seguridad que se encuentran fuera del ámbito de la Recomendación UIT-T H.323 están la política de seguridad, la seguridad de gestión de red, el suministro de la seguridad, la seguridad de la implementación, la seguridad operacional o la seguridad en el tratamiento de incidentes.

9.1.2 Recomendaciones de la subserie H.235.x

La serie de Recomendaciones H.235.x cubre once normas además de una guía para diseñadores que, conjuntamente, proporcionan la especificación de los mecanismos y protocolos de seguridad y directrices detalladas sobre la seguridad de implementación según la serie de Recomendaciones UIT-T H.3233. Proporcionan soluciones de seguridad escalable para pequeños grupos, empresas y operadores a gran escala, además de protección criptográfica de los protocolos de control y de los datos de trenes de medios como audio o 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. 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. Permite soportar configuraciones como la comunicación punto a punto "clásica" y configuraciones multipunto gracias a las unidades de multidifusión cuando se comunican varias terminales multimedios dentro de un grupo.

La Recomendación UIT-T H.235 utiliza técnicas especiales de seguridad optimizada como la criptografía de curva elíptica y la criptación 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 mejor implementación con menores huellas en los puntos extremos gracias a una interacción más intensa con el procesador de señal digital y los códecs de compresión de voz, sin tener que depender de una plataforma específica de sistema operativo.

En la figura 39 se muestra el alcance de la Recomendación UIT-T H.235, que comprende disposiciones para el establecimiento de comunicaciones (bloques UIT-T H.225.0 y UIT-T 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 las Recomendaciones UIT-T H.323 y H.235, suele implementarse utilizando los protocolos de seguridad IP (IPSec) y de seguridad de capa de transporte (TLS). Si lo requiere la política del sistema final, estos dos protocolos se pueden utilizar con fines de autenticación y, facultativamente, confidencialidad en la capa IP, de una manera transparente para cualquier protocolo (aplicación) que esté funcionando por encima de ella.

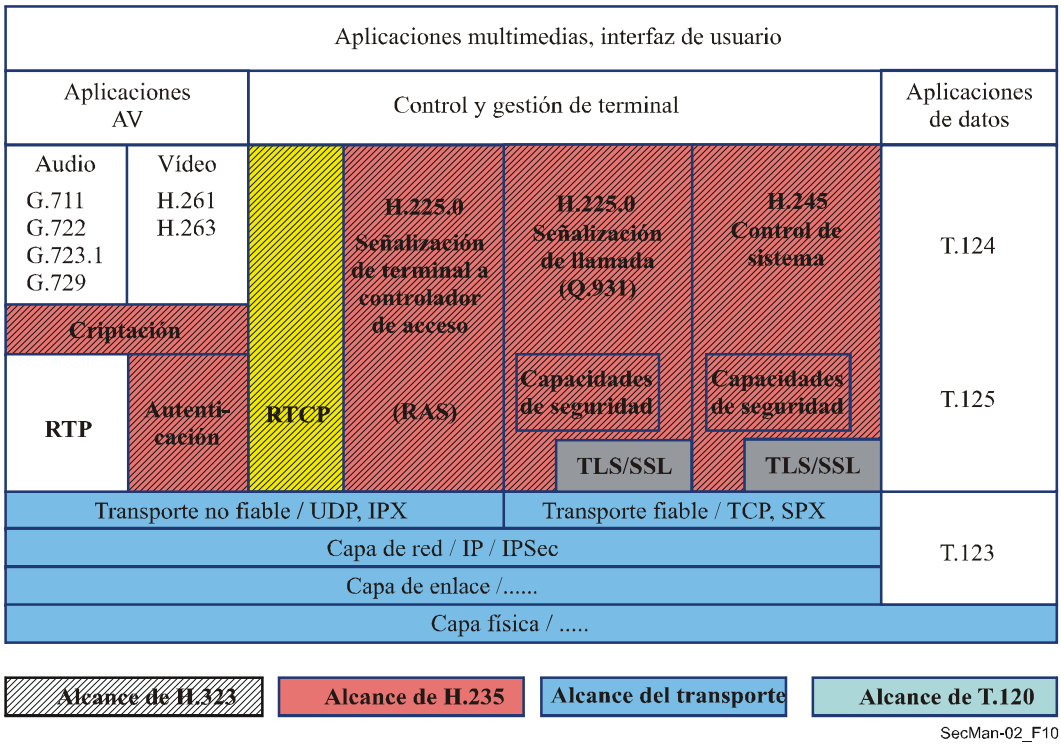


Figura 39 – Seguridad en los sistemas UIT-T H.323 proporcionada por H.235

La serie de Recomendaciones UIT-T H.235.x cubre una amplia gama de medidas de seguridad para distintos entornos (por ejemplo, de una empresa, entre empresas y de operadores) y se puede adaptar a cada caso en función de factores locales como la infraestructura de seguridad disponible y capacidades del terminal (por ejemplo, puntos extremos simples o inteligentes).

Los perfiles de seguridad disponibles ofrecen distintas técnicas de seguridad, desde perfiles simples de secreto compartido, algunos con contraseña protegida hasta los más sofisticados que contienen firmas digitales y certificados PKI UIT-T X.509 (UIT-T H.235.2). De esta manera se puede ofrecer protección salto por salto utilizando técnicas más simples, pero menos escalables, o bien de extremo a extremo utilizando técnicas PKI escalables. UIT-T H.235.3 se denomina perfil de seguridad híbrido ya que esta Recomendación combina procedimientos de seguridad simétricos de la Recomendación UIT-T H.235.1 y certificados PKI y firmas de la Recomendación UIT-T H.235.2, optimizando así la calidad de funcionamiento y reduciendo el tiempo de establecimiento de comunicación. UIT-T H.235.4 relaja la estricta dependencia de un

encaminamiento por controlador de acceso y de una arquitectura centralizada en el servidor y ofrece medidas para dar seguridad a un modelo entre pares. También define procedimientos para la gestión de claves en entornos empresariales y entre dominios.

Para proporcionar mayor seguridad a los sistemas que utilizan números de identificación personal (PIN) o contraseñas para autenticar a los usuarios, UIT-T 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. La Recomendación 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 UIT-T H.245.

La Recomendación UIT-T H.530, *Procedimientos de seguridad simétricos para movilidad de sistemas UIT-T H.323 según la Recomendación UIT-T H.510*, considera la movilidad segura de usuario y terminal en los entornos distribuidos UIT-T H.323, que trata aspectos de seguridad como:

- autenticación y autorización de terminal/usuario móvil en los dominios visitados;
- autenticación de dominio visitado;
- gestión de clave segura; y
- protección de los datos de señalización entre un terminal móvil y un dominio visitado.

La Recomendación UIT-T H.235.0 proporciona el marco de seguridad general para los sistemas multimedios de la serie H. La serie de Recomendaciones UIT-T H.235.0 y UIT-T H.350 permiten una gestión de claves escalable gracias al protocolo de acceso al directorio ligero (LDAP) y el protocolo de capa segura entre puntos extremos (SSL/TLS). En la serie de Recomendaciones UIT-T H.350 se incluyen en particular capacidades que permiten a las empresas y los operadores gestionar con seguridad un gran número de usuarios de servicios de vídeo y voz por IP, junto con un método para conectar UIT-T H.323, SIP, UIT-T H.320 y servicios de mensajería genéricos en un servicio directorio, de tal manera que se puedan aplicar prácticas modernas de gestión de identidad a las comunicaciones multimedios.

9.1.3 Dispositivos de traducción de dirección de red y cortafuegos

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 UIT-T H.323 procedente de dispositivos externos hacia los dispositivos UIT-T H.323 internos, la comunicación simplemente no es posible, lo que supone un problema para cualquier usuario de equipos UIT-T 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 1918 del IETF, 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 UIT-T 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).

Los problemas del paso de dispositivos NAT/FW se consideran en tres Recomendaciones de la serie UIT-T H.460 que permiten el paso sin discontinuidades por uno o más dispositivos NAT/FW a las comunicaciones UIT-T H.323. Estas Recomendaciones son: UIT-T H.460.17, *Utilización de la conexión de señalización de llamadas H.225.0 como transporte de mensajes RAS H.323*, UIT-T H.460.18, *Paso de señalización H.323 a través de traductores de dirección de red y cortafuegos*, y UIT-T H.460.19, *Paso de medios H.323 por traductores de dirección de red y cortafuegos*.

En la figura 40 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:

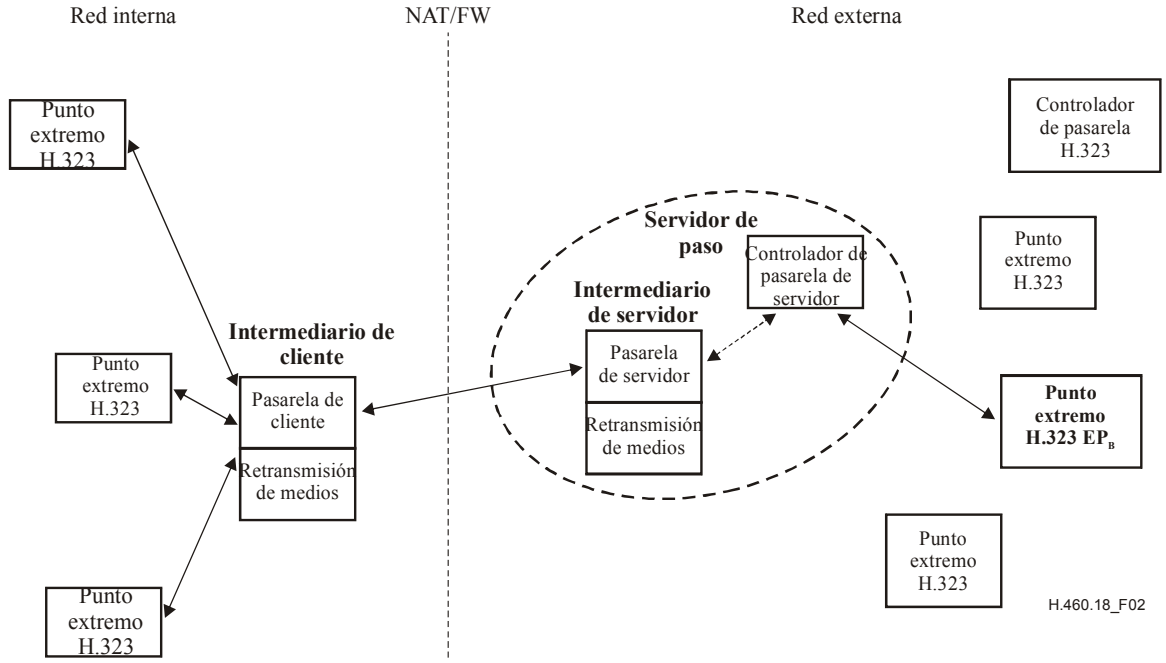


Figura 40 – NAT/FW transversal en la arquitectura H.460.18

Esta topología también puede resultar útil en otros casos, por ejemplo cuando una empresa desea controlar la vía de la señalización de llamada UIT-T H.323 y de los flujos de medios en la red. No obstante, UIT-T H.460.17 y UIT-T H.460.18 permiten también 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 41:

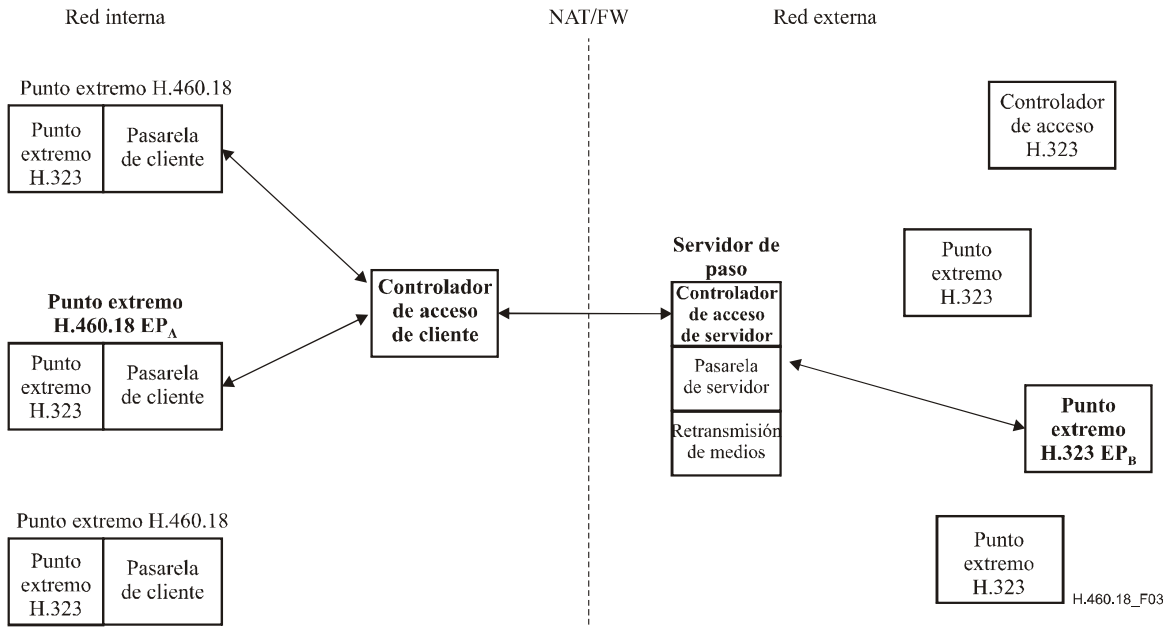


Figura 41 – Arquitectura de comunicación de controlador de acceso

En la figura 40 los puntos extremos de la red interna comunican con el controlador de acceso de red interna para resolver la dirección de las entidades externas (por ejemplo, un número de teléfono o un URL UIT-T 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 la Recomendación UIT-T 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 UIT-T 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 UIT-T 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.

9.2 IPTV

Las disposiciones de seguridad para la televisión por protocolo de Internet (IPTV) deben incluir la protección del contenido entregado mediante los servicios IPTV, los dispositivos de terminal utilizados y el suministro de esos servicios.

La protección de contenidos significa para la IPTV que se garantiza que un usuario final pueda utilizar el contenido sólo de conformidad con los derechos otorgados por el propietario de esos derechos, lo que implica proteger los contenidos ante la copia y distribución ilegales y la interceptación, manipulación y utilización no autorizadas.

La protección de los dispositivos terminales IPTV incluye garantizar que el dispositivo de recepción del servicio empleado por el usuario final puede usar el contenido de forma fiable y segura, utilizar los derechos de uso del contenido y proteger la integridad y confidencialidad del mismo, así como los parámetros críticos de seguridad tales como las claves criptográficas.

La protección del servicio IPTV incluye garantizar que los usuarios finales solo pueden adquirir un servicio y el contenido que están autorizados a recibir. También incluye la protección del servicio frente al acceso no autorizado.

Se están elaborando varias Recomendaciones sobre seguridad específicas para la IPTV entra las que se ha aprobado una, la Recomendación UIT-T X.1191, *Requisitos funcionales y arquitectura para los aspectos de seguridad de la IPTV*. La arquitectura general de seguridad para IPTV definida en esa Recomendación se muestra en la figura 42. Cabe destacar que solo se consideran dentro del ámbito de la Recomendación aquellas funciones que corresponden al usuario final, al proveedor de red y al proveedor de servicio. Las funciones relativas al proveedor de contenidos están sometidas a acuerdos privados entre las partes interesadas y se consideran fuera del ámbito de esa Recomendación.

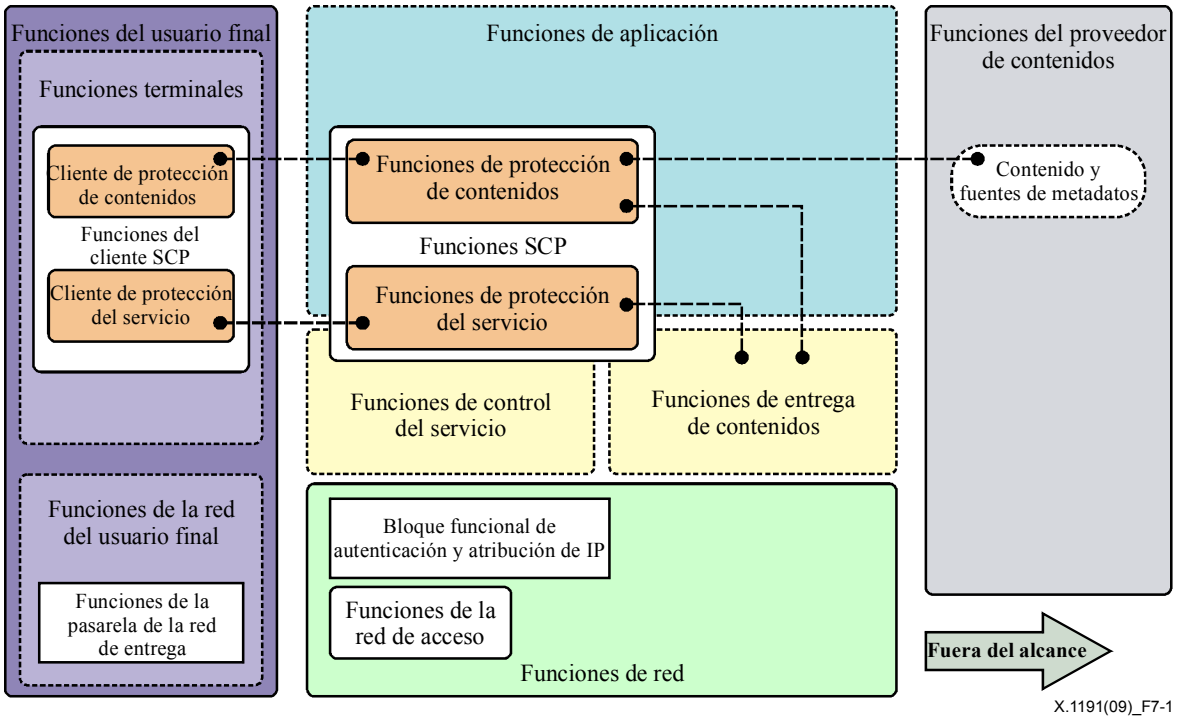


Figura 42 – Arquitectura general de seguridad para IPTV

9.2.1 Mecanismos para proteger el contenido IPTV

Los mecanismos de seguridad que se pueden utilizar para proteger el contenido son:

- criptación del contenido;
- filigranas (es decir, el uso de esteganografía para alterar ciertas características del contenido sin que esa alteración sea inmediatamente detectable);
- identificación e información del análisis del contenido para facilitar la investigación en caso de acceso o uso del contenido sin autorización;

- etiquetado del contenido (como clasificación de la información para permitir cierto grado de control del usuario final en relación con el acceso a contenido inapropiado); y
- transcodificación segura (que permite a los nodos intermedios de red transformar el contenido multimedios a un formato diferente o con una calidad diferente sin descriptar preservando así la seguridad de extremo a extremo).

9.2.2 Mecanismos para proteger el servicio IPTV

Entre los mecanismos de protección del servicio se incluyen:

- autenticación del usuario final (abonado) y/o del dispositivo terminal;
- autorización (para garantizar que el usuario final o el terminal tiene autorización para acceder a los servicios y/o al contenido); y
- control de acceso (en particular para garantizar que únicamente un proveedor de servicio autorizado puede tener acceso al contenido que se está cargando de un cliente a un servidor).

9.2.3 Protección de la información de abonado

Al implementar la IPTV surge una preocupación especial por la necesidad de proteger la información de abonado que puede incluir información sobre los datos buscados como el número de canal antes y después de un cambio de canal, la hora del cambio, información de usuario para el servicio electrónico de guía de programas, la identificación de paquetes, la hora de reproducción, etc. Estos datos se deben considerar sensibles y deben tomarse medidas para impedir su difusión no autorizada a través del terminal, la red o el proveedor de servicio. En un anexo a la Recomendación UIT-T X.1191 se incluyen sugerencias para proteger la información de abonado.

9.3 Transmisión segura de facsímil

El facsímil sigue siendo una aplicación muy extendida pero la confianza en los servicios de facsímil depende en gran medida de la efectividad de las medidas de seguridad incorporadas. Inicialmente, las normas de facsímil se desarrollaron para su transmisión por la RTPC (Recomendación UIT-T T.4), y posteriormente para la RDSI (Recomendación UIT-T T.563). Más recientemente se especificaron ampliaciones para la transmisión de facsímil en tiempo real por redes IP (incluida Internet) (Recomendación UIT-T T.38) y a través de sistemas de almacenamiento y retransmisión (Recomendación UIT-T T.37).

Independientemente del modo de transmisión, los problemas de seguridad a los que se enfrentan los servicios de facsímil incluyen la confidencialidad de los datos transmitidos, la autenticación y el no repudio. Estos asuntos son todavía más importantes al desplazarse el tráfico hacia Internet debido a las características abiertas y distribuidas del medio.

La seguridad de facsímil se considera en la Recomendación UIT-T T.36, *Capacidades de seguridad para su uso con terminales de facsímil del grupo 3*, que define dos soluciones técnicas independientes que se pueden utilizar para cifrar los documentos intercambiados. Una opción especificada es utilizar el algoritmo criptográfico de *Rivest, Shamir y Adleman* (RSA); otro método utiliza una combinación de *Hawthorne Key Management* (HKM) y *Hawthorne Facsimile Cipher* (HFX). Los servicios de seguridad definidos son:

- autenticación mutua (obligatoria);
- servicio de seguridad (facultativo), 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; y
- 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.

La combinación de los sistemas *Hawthorne Key Management* (HKM) y *Hawthorne Facsimile Cipher* (HFX) proporcionan las siguientes capacidades para las comunicaciones seguras de documentos entre entidades:

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

9.4 Servicios web

Se están aplicando ampliamente tecnologías de la web, en particular las arquitecturas orientadas al servicio (SOA) ya que permiten a los diseñadores desarrollar y desplegar nuevos servicios de forma eficaz y rentable e integrar el contenido proveniente de diversas fuentes para constituir servicios compuestos fácilmente y con rapidez. Existen muchos aspectos de seguridad de los servicios web. Son importantes los mecanismos para la autenticación y la firma única (SSO) y, puesto que se están aplicando los servicios web a redes móviles, también es importante considerar los mecanismos de seguridad necesarios para los servicios web móviles.

Las economías de escala han llevado a los vendedores de plataformas de cálculo a desarrollar productos con funcionalidades muy generalizadas, de forma que se puedan utilizar en la mayor gama posible de situaciones. Estos productos se entregan con el máximo privilegio posible para acceder a los datos y ejecutar el software para que puedan utilizarse en tantos entornos de aplicación como sea posible, incluidos aquellos con las políticas de seguridad más permisivas. Cuando se requiera una política de seguridad más restrictiva, los privilegios inherentes a la plataforma deben limitarse mediante la configuración local.

La política de seguridad de una empresa grande tiene muchos elementos y muchos puntos de aplicación. Los elementos de la política se pueden gestionar a través del departamento de sistemas de información, el de recursos humanos, el departamento jurídico y el departamento financiero. La política se puede reforzar a través de extranet, por correo, WAN y sistemas de acceso a distancia – plataformas que implementan de forma inherente una política de seguridad permisiva. La práctica actual consiste en gestionar la configuración de cada punto de aplicación independientemente con el fin de implantar la política de seguridad con la mayor precisión posible. Por consiguiente, modificar la política de seguridad es una propuesta cara y poco fiable. También resulta difícil (quizás incluso imposible) obtener una visión consolidada de las protecciones existentes en toda la empresa para aplicar la política. Al mismo tiempo surge una presión creciente sobre los ejecutivos empresariales y gubernamentales por parte de los clientes, las partes interesadas y los reguladores para que apliquen "las mejores prácticas" en la protección de los elementos de información de la empresa y de sus clientes.

Por estas razones, es preciso un lenguaje común para expresar la política de seguridad. Si se implementa en toda la empresa, el lenguaje de política común permite a la empresa gestionar el cumplimiento de todos los elementos de su política de seguridad en todos los componentes de sus sistemas de información. Gestionar la política de seguridad puede implicar alguno o todos de los pasos siguientes: redactar, revisar, comprobar, aprobar, editar, combinar, analizar, modificar, suprimir, retirar y reforzar esa política.

Además, se precisa un marco para intercambiar información de seguridad. Para facilitar estos intercambios se han desarrollado lenguajes de marcaje como el lenguaje de marcaje de asertos de seguridad y el lenguaje de marcaje de control de acceso extensible (XACML). Originalmente los desarrolló OASIS pero actualmente han sido adoptados y publicados por el UIT-T con la asistencia de OASIS.

9.4.1 Lenguaje de marcaje de asertos de seguridad

La Recomendación UIT-T X.1141 define el lenguaje de marcaje de asertos de seguridad (SAML2.0). El SAML es un marco basado en XML para intercambiar información de seguridad. La información de seguridad se presenta en la forma de aserciones sobre sujetos, donde un sujeto es una entidad que tiene una identidad en algún dominio de seguridad. Una aserción única podría incluir varios enunciados internos diferentes sobre autenticación, autorización y atributos.

Las aserciones SAML se realizan normalmente sobre un *sujeto*. Habitualmente existen varios *proveedores de servicio* que pueden utilizar las aserciones sobre un sujeto con el fin de controlar el acceso y prestar un servicio personalizado y, por lo tanto, se convierten en partes vinculantes de una parte de la aserción denominada *proveedor de identidad*.

La Recomendación UIT-T X.1141 define tres tipos diferentes de enunciados de aserción que pueden ser creados por una autoridad SAML. Todos los enunciados definidos por el SAML están asociados con un sujeto. Los tres tipos de enunciados definidos en la Recomendación UIT-T X.1141 son:

- autenticación: el sujeto de la aserción se autenticó mediante medios particulares en un momento determinado;
- atributo: el sujeto de la aserción está asociado con los atributos suministrados; y
- decisión de autenticación: se ha concedido o denegado una petición de autorización para que el sujeto de la aserción acceda a un recurso específico.

La Recomendación UIT-T X.1141 también define un protocolo mediante el cual los clientes pueden solicitar aserciones de las autoridades SAML y obtener una respuesta de ellas. Este protocolo, constituido por formatos de mensajes de petición y respuesta basados en XML puede estar vinculado con muchas comunicaciones diferentes subyacentes y protocolos de transporte. Al generar sus respuestas, las autoridades SAML pueden utilizar diversas fuentes de información, tales como el almacenamiento y la aserción de política externos que se recibieron como datos de entrada en las solicitudes.

Se define un conjunto de perfiles para soportar la firma única (SSO) de exploradores y de otros dispositivos de clientes. La figura 44 muestra el esquema básico para conseguir la SSO.

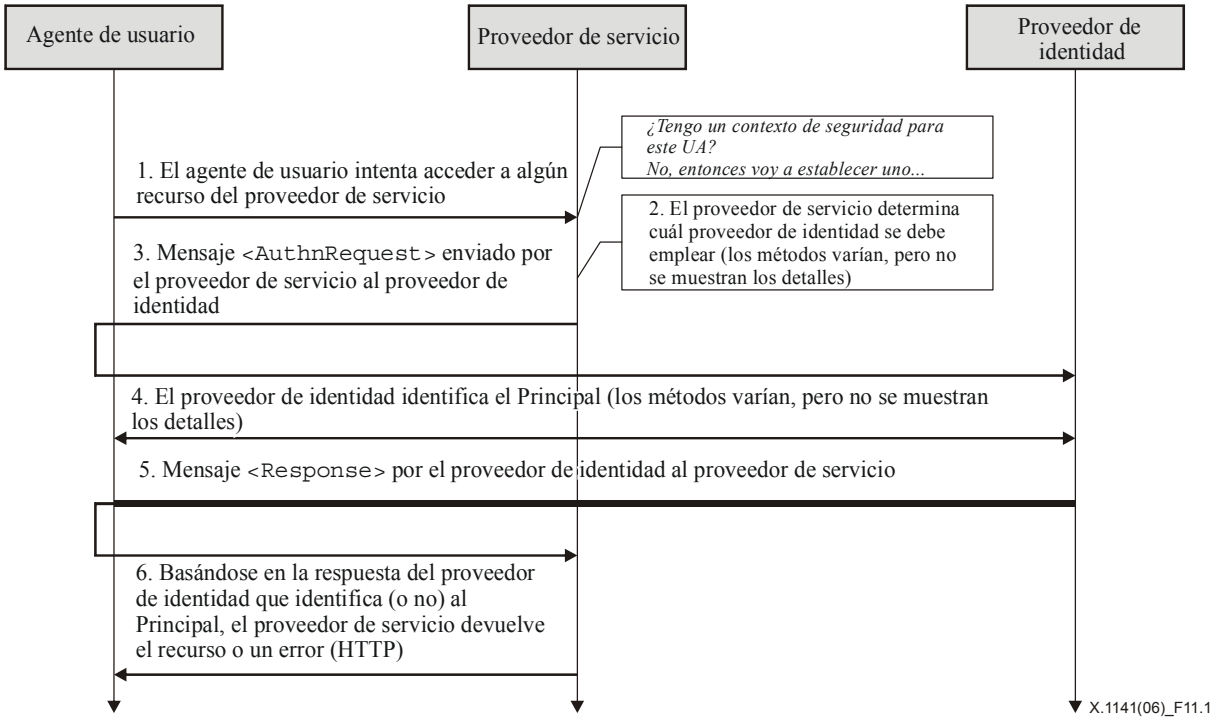


Figura 43 – Plantilla básica para conseguir la SSO

9.4.2 Lenguaje de marcaje de control de acceso extensible

El lenguaje de marcaje de control de acceso extensible (XACML) es un vocabulario XML para expresar políticas de control de acceso. El control de acceso consiste en decidir si se debe permitir un acceso a un recurso solicitado y apoyar esa decisión. La Recomendación UIT-T X.1142 define el XACML básico incluida la sintaxis del lenguaje, los modelos, el contexto con el modelo de lenguaje de política, su sintaxis y las reglas de procedimiento. Para mejorar la seguridad del intercambio de políticas basada en XACML, la Recomendación UIT-T X.1142 también especifica un perfil de firma digital XML XACML para datos de seguridad. Se especifica un perfil de privacidad con el fin de facilitar directrices para los diseñadores. El XACML es adecuado para diversos entornos de aplicación.

9.5 Servicios basados en marcadores

Se están desarrollando ampliamente los marcadores de identificación (incluidas los marcadores RFID) pero crece la preocupación sobre el riesgo de violación de la privacidad. Esto se debe en parte a que la tecnología RFID puede recopilar y procesar automáticamente datos y existe un riesgo de difusión deliberada o accidental de información sensible y/o personal.

Para aplicaciones que utilicen o dependan de la identificación basada en marcadores o que impliquen información personal, tales como datos médicos, pasaportes y permisos de conducir, el tema de la privacidad cada vez es un problema más grave.

En la enseñanza y en la industria, la mayoría de los esfuerzos hacia un mecanismo de protección para información personalmente identificable (PII) se han centrado en protocolos de autenticación entre el marcador ID y el terminal ID. Sin embargo, esos esfuerzos no consideran el problema en su totalidad, puesto que sigue existiendo información substancial sobre el identificador en el servidor en el dominio de red. Una solución a este problema consiste en utilizar un mecanismo de protección PII basado en perfiles.

La Recomendación UIT-T X.1171, *Amenazas y requisitos para la protección de la información identificable personalmente en las aplicaciones que utilizan la identificación basada en marcadores*, examina las amenazas a la PII en un entorno entre empresas y consumidores (B2C) en el que las aplicaciones utilizan identificación basada en marcadores. Identifica los requisitos para la protección de la PII en estos entornos y define la estructura básica de la protección PII a partir de un perfil de política PII definido por el usuario.

Las aplicaciones de empresa a consumidor (B2C) que utilizan identificación basada en marcadores se pueden clasificar en tres tipos:

a) *Siendo cliente el usuario del dispositivo*: en el servicio de entrega de contenido de información, el cliente retira la información utilizando su propio dispositivo de lectura. En este tipo de lectura, la mayoría de los proveedores de servicios de aplicación pueden suponer que el cliente tiene un terminal móvil equipado con un dispositivo de lectura. La figura 44 muestra un modelo básico de este tipo de aplicación. Consiste en dos operaciones de red básicas: resolución de ID y recuperación del contenido. La resolución de ID es el procedimiento de traducir o resolver un identificador a una dirección. El terminal móvil equipado con un lector resuelve en primer lugar un identificador recibido en el marcador ID a través de un servicio de directorio y realiza luego la recuperación del contenido.

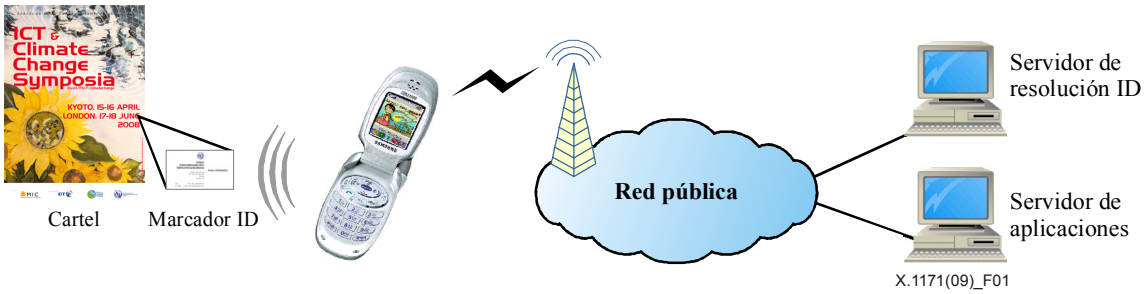


Figura 44 – Modelo básico de una aplicación de empresa-consumidor que utiliza identificación basada en marcadores

b) *Siendo cliente el usuario del marcador ID*: un ejemplo típico de esta aplicación B2C que utiliza identificación basada en marcadores trata del control de acceso y/o la autenticación, por ejemplo, comprobación de entrada, pasaporte, licencia o servicio de gestión postventa. En este tipo de aplicación, los dispositivos de lectura son del tipo terminal fijo y/o móvil. El cliente puede no disponer de su propio dispositivo de lectura.

c) *Siendo cliente tanto el usuario de marcadores ID como el usuario de dispositivo*: en el servicio de recuperación de información de producto, el cliente también es un usuario de marcadores al solicitar el producto marcado tras explorar los contenidos de la información del producto desde su terminal móvil. Otro ejemplo puede ser el de un servicio relacionado con la sanidad solicitado por un paciente que dispone de marcador ID. En esta aplicación, existen muchos tipos de cliente que podrían ser los usuarios de marcadores ID (por ejemplo, paciente, médico, enfermera). El usuario del marcador ID puede explorar sus propios registros de paciente mediante el terminal móvil con un dispositivo de lectura, leyendo su tarjeta de paciente habilitada mediante el marcador ID.

Para aplicaciones B2C que utilizan identificación basada en marcadores, existen dos riesgos importantes de violación de PII:

- fuga de información asociada con el identificador: en este caso, el atacante puede leer información del marcador ID sin conocer al usuario del producto marcado. En primer lugar, el atacante lee un identificador del marcador ID transportado por el usuario. Posteriormente, resuelve el identificador y solicita la ubicación de la información al servicio de directorio. Finalmente, el atacante pide información asociada con el marcador ID.
- fuga de los datos de contexto histórico: el atacante puede extraer los datos del usuario (tales como preferencias, costumbres, temas de interés, etc.) a partir de los datos de contexto histórico asociados con el marcador ID. El atacante puede utilizar esos datos para fines ilegales o comerciales sin el consentimiento del usuario.

La Recomendación UIT-T X.1171 describe los requisitos técnicos siguientes para proteger las violaciones de PII en aplicaciones B2C:

- *control de la PII por parte del usuario del marcador ID*: el usuario del marcador ID debe poder gestionar o actualizar la PII asociada con su marcador ID en la red. De esta forma, el usuario del marcador ID puede determinar qué PII debería suprimirse o mantenerse en la aplicación.
- *autenticación del usuario del marcador ID y/o el usuario del dispositivo*: el servidor de aplicación debe proporcionar un procedimiento de autenticación para el usuario del marcador ID, y el servidor de aplicación puede facilitar un procedimiento de autenticación para el usuario del dispositivo, si es preciso (algunas aplicaciones que utilizan identificación basada en marcadores no necesitan autenticar al usuario).
- *control de acceso a la PII de un usuario del marcador ID en un servidor de aplicaciones*: el servidor de aplicaciones debe controlar el acceso a la información correspondiente relacionada con el PII del usuario de marcador ID.
- *confidencialidad de la información asociada al marcador ID*: el servidor de aplicación debe proporcionar la confidencialidad de los datos para garantizar que la información asociada con un marcador ID solo la puede leer un usuario autorizado.
- *autorización para el acopio de datos de catálogo relacionados con el usuario del dispositivo*: el servidor de aplicaciones puede facilitar un procedimiento de autorización para el acopio de los datos de catálogo relacionados con el usuario del dispositivo, si este tipo de recopilación de datos de catálogo es necesario para la aplicación.

El ejemplo siguiente ilustra un servicio de protección PII (PPS) basado en el perfil de política PII del usuario. El escenario de servicio para el PPS surge normalmente de un procedimiento de personalización de marcadores como la adquisición de productos marcados. La figura 45 muestra el flujo general del servicio PPS de la aplicación utilizando identificación basada en marcadores.

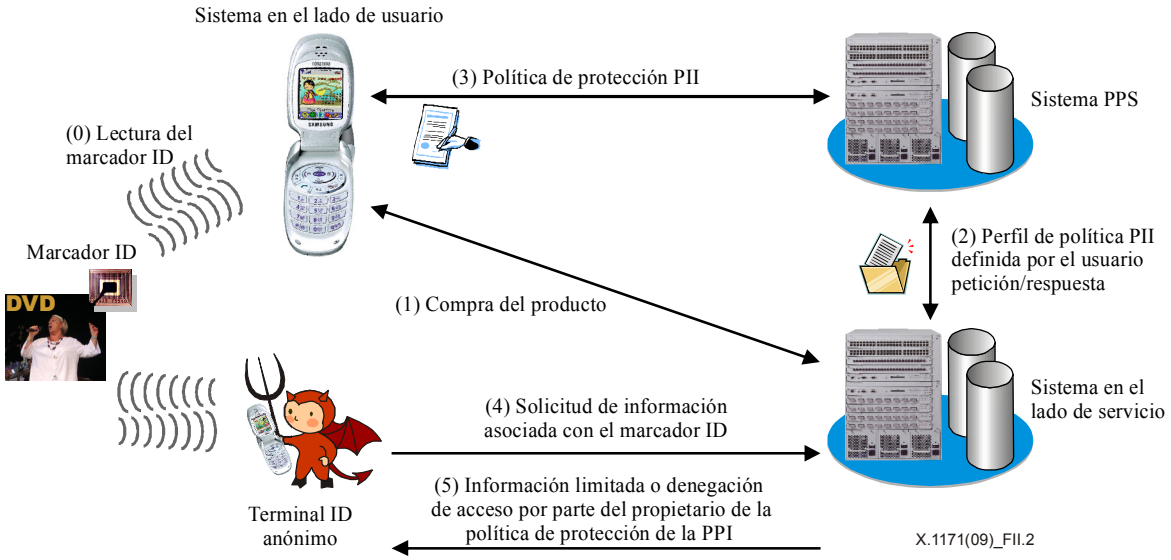


Figura 45 – Flujo general del servicio de protección PII (PPS)

1) Un consumidor lee el identificador del producto marcado utilizando su equipo terminal móvil dotado de un terminal ID.

2) El consumidor consume la información relacionada con el producto en la red del servicio de aplicación y ulteriormente adquiere el producto utilizando uno o más métodos de pago, momento en el cual, el consumidor se convierte en un usuario de marcador ID.

3) Acto seguido, la aplicación que utiliza identificación basada en marcadores solicita un perfil de política PII definido por el usuario al sistema PPS, que responde a la aplicación con el perfil PII definido por el usuario.

4) El sistema PPS recibe la política de protección PII del usuario para esta aplicación

5) Cualquier persona puede solicitar desde el sistema situado en el lado del servicio la información asociada con el marcador ID.

6) El solicitante puede consultar toda la información proporcionada por el sistema situado en el lado de servicio, siempre que el solicitante sea el usuario del marcador ID. En caso contrario, el solicitante obtiene información limitada o no puede acceder a información alguna.

10. Contrarrestar amenazas comunes en las redes

10 Contrarrestar amenazas comunes en las redes

Las amenazas a los sistemas de ordenadores y a las redes que los unen son muchas y variadas. Aunque muchos ataques pueden iniciarse localmente, la gran mayoría de los ataques actualmente se llevan a cabo mediante redes de comunicaciones. El hecho de que cada vez más ordenadores y dispositivos de red están conectados a Internet y de que se utilicen en casa o en los lugares de trabajo o por personas con poca formación, conciencia o conocimiento de la seguridad de las tecnologías de la información, aumenta en gran medida la posibilidad y probabilidad de ataques a distancia, a menudo indiscriminados. El bombardeo electrónico, los programas espía, los virus y otros vectores de ataque existen en un número cada vez mayor. Los atacantes a menudo dependen de sistemas débiles y poco protegidos como cauces para su software malicioso.

En esta sección, se presenta una perspectiva de los trabajos del UIT-T para responder a algunos de esos ataques.

10.1 Contrarrestar el bombardeo electrónico

El bombardeo electrónico (es decir, el correo electrónico basura, no deseado) es muy reconocido como un problema fundamental para los usuarios de la red y los proveedores de red y de servicios. El bombardeo electrónico interfiere con operaciones legítimas, consume ancho de banda y ciclos de procesamiento y, en casos extremos, puede dar lugar a ataques de negación de servicio inundando las redes. Se están utilizando medidas legales tanto como técnicas para contrarrestar el bombardeo electrónico con diversos grados de efectividad. Ninguna medida contra el correo basura por sí sola es eficaz y, dada la agilidad y los recursos de los fabricantes de ese tipo de correo, incluso una combinación de medidas a menudo sólo consigue reducir la magnitud del volumen del correo no solicitado. Entre las medidas que se están utilizando se incluyen por ejemplo: la reglamentación, medidas técnicas que incluyen el filtrado del correo no solicitado, la cooperación internacional y la formación de usuario y de los proveedores de servicio de Internet.

Los trabajos del UIT-T para contrarrestar el bombardeo electrónico se centran fundamentalmente en los aspectos técnicos del problema de forma que, en esta sección, se presentan los medios técnicos para contrarrestar el correo no solicitado y el desarrollo y aplicación de las tecnologías contra el correo basura.

10.1.1 Estrategias técnicas para contrarrestar el bombardeo electrónico

La Recomendación UIT-T X.1231, *Estrategias técnicas contra el correo basura*, establece requisitos para combatir el correo no solicitado y constituye un punto de partida para el trabajo. Esta Recomendación describe los diferentes tipos de bombardeo electrónico y sus características comunes y proporciona una visión general de los planteamientos técnicos para contrarrestar ese tipo de correo. También propone un modelo general que se puede utilizar para desarrollar una estrategia contra el correo basura efectiva.

Este modelo es jerárquico y tiene cinco estrategias distribuidas en tres capas. Las relaciones entre las estrategias se muestran en la figura 46. El modelo indica que existe un alto grado de interdependencia entre las estrategias pero que consideraciones de coste pueden impedir el uso de todas las estrategias en determinados casos. Asimismo, es necesario adaptarse a cada caso de aplicación.

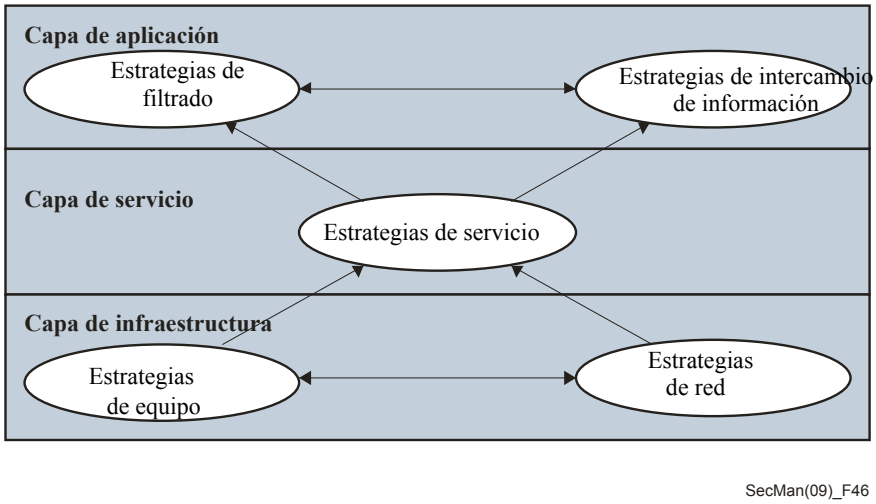


Figura 46 – Modelo general para contrarrestar el bombardeo electrónico

10.1.2 Correo electrónico no solicitado

La forma más ampliamente reconocida de bombardeo electrónico es el correo electrónico no solicitado. Presenta retos técnicos complejos y las soluciones para suprimirlo deben basarse en medidas técnicas adecuadas. Aunque la actuación gubernamental y la legislación son útiles, son insuficientes para satisfacer los retos planteados por el correo electrónico no solicitado. Este problema viene complicado por la dificultad de identificar al que envía los correos cuando se utiliza el protocolo SMTP.

Se han elaborado dos Recomendaciones para contribuir a contrarrestar el correo electrónico no deseado. La Recomendación UIT-T X.1240, *Tecnologías utilizadas contra el correo basura*, se destina a usuarios que desean desarrollar soluciones técnicas para contrarrestar el correo electrónico no solicitado. Especifica los conceptos básicos, las características, los efectos y los problemas técnicos asociados con el asunto. También identifica las actuales soluciones técnicas y actividades relacionadas de las organizaciones normativas y otros grupos que están trabajando para contrarrestar el correo basura.

La Recomendación UIT-T X.1241, *Marco técnico contra el correo basura*, describe una estructura recomendada para un dominio de tratamiento contar el correo basura y define la funcionalidad de los principales módulos en el dominio. El marco establece un mecanismo para compartir información sobre correo basura entre diferentes servidores de correo electrónico. Pretende promover una mayor cooperación entre los proveedores de servicio para combatir el correo basura. En particular proporciona un marco para permitir una metodología de comunicación ante alertas relativas al correo electrónico no solicitado identificado. Otro documento, la *serie de Recomendaciones UIT-T X. 1240 – Suplemento contra el correo basura y amenazas conexas* analiza los foros internacionales donde se está considerando el correo no solicitado e incluye un estudio de caso.

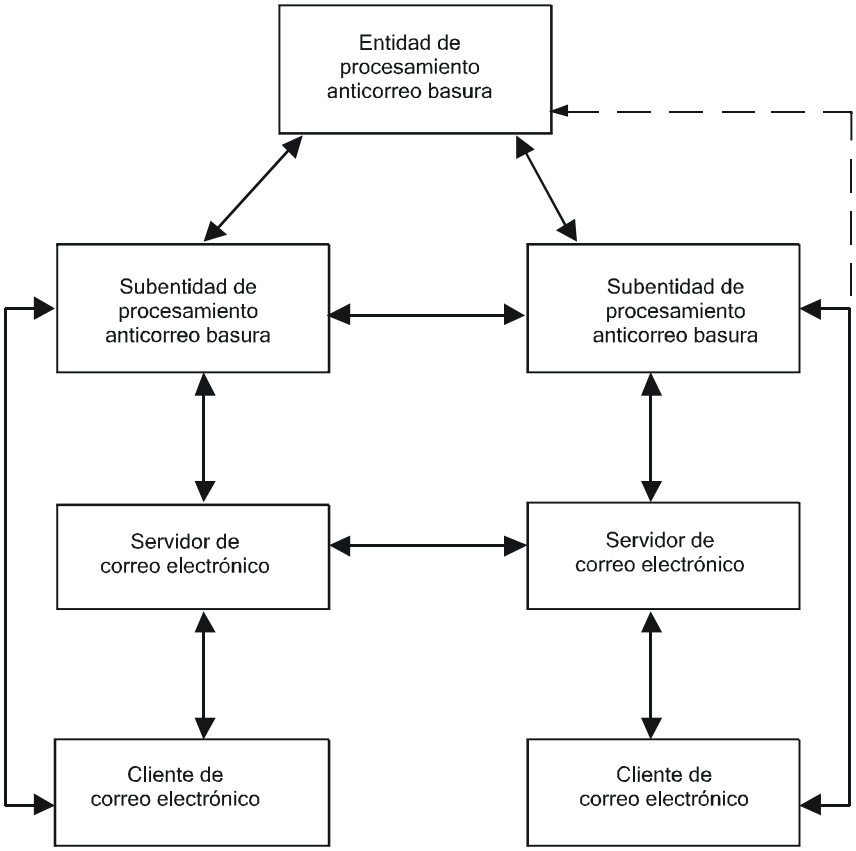


Figura 47 – Estructura general de un dominio de tratamiento contra el correo electrónico basura

La figura 47 ilustra el proceso del marco de la Recomendación UIT-T X.1241. La entidad de tratamiento contra el correo basura está ubicada en un sistema independiente mientras que las subentidades de tratamiento contra el correo basura están ubicadas en uno o más proveedores de servicio de correo electrónico. Esta entidad de tratamiento entrega nuevas reglas a las subentidades que las deben verificar y refinar. También existe una función que resuelve cualquier conflicto en las reglas.

10.1.3 Correo basura en aplicaciones multimedios IP

La Recomendación UIT-T X. 1244, *Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP*, especifica los conceptos básicos, las características y los asuntos técnicos para contrarrestar el correo basura en aplicaciones multimedios IP tales como telefonía IP y mensajería instantánea. Se catalogan los diversos tipos de correo basura en aplicaciones multimedios IP y se describen de conformidad con sus características. La norma describe diversas amenazas de seguridad mediante correo basura que pueden producir correos no solicitados e identifica los aspectos que deberían considerarse para contrarrestarlos. Algunas de las técnicas desarrolladas para controlar el correo electrónico no solicitado también se pueden utilizar para contrarrestar el bombardeo electrónico en aplicaciones multimedios. La Recomendación UIT-T X.1244 analiza los mecanismos convencionales para contrarrestar el correo basura y trata su aplicación contra el spam en aplicaciones multimedios IP.

Las técnicas contra el correo basura (spam) en aplicaciones multimedios IP se pueden aplicar según sus características particulares. El cuadro 7 muestra la clasificación utilizada en la Recomendación UIT-T X.1244.

Cuadro 7 – Clasificación de spam en aplicaciones multimedios IP

	Texto	Voz	Video
Tiempo real	• Spam en mensajería instantánea • Spam en charla	• Spam en VoIP • Spam en mensajería instantánea	• Spam en mensajería instantánea
Tiempo no real	• Spam en texto/multimedios • Spam de texto en el servicio de compartición de ficheros P2P • Spam de texto en sitio web	• Spam de voz/multimedios • Spam de voz en el servicio de compartición de ficheros P2P • Spam de voz en sitio web	• Spam de video/multimedios • Spam de video en el servicio de compartición de ficheros P2P • Spam de video en sitio web

10.1.4 Correo basura en servicios de mensajes cortos (SMS)

La Recomendación UIT-T X.1242, *Sistema de filtrado de correo basura en el servicio de mensajes cortos (SMS) basado en reglas especificadas por el usuario*, define la estructura y funciones del sistema de filtrado de correo basura en SMS junto con la gestión del servicio de los usuarios, los protocolos de comunicación y los requisitos básicos funcionales de los terminales con las funciones SMS. Se definen métodos mediante los cuales los usuarios pueden gestionar (solicitar, suprimir y restablecer) mensajes cortos filtrados. El filtrado se puede basar en características tales como direcciones, números de teléfono, hora o contenido. Los requisitos para el software de terminal que soporta el filtrado de spam SMS se proporcionan en un apéndice a la Recomendación UIT-T X.1242.

10.2 Código malicioso, programas espía y software engañoso

Aunque los sistemas y redes asumen mayores riesgos ante códigos maliciosos (virus, gusanos, troyanos, etc.), los programas espía y otros programas informáticos engañosos (es decir, programas que realizan actividades no autorizadas) también plantean riesgos importantes. A menos que las organizaciones y los individuos implementen una gama de medidas proactivas (entre ellas cortafuegos, medidas antivirus y medidas anti-programas espías) frente a esas amenazas, virtualmente no se podrán evitar. Sin embargo, las contramedidas disponibles varían en eficacia y no siempre son complementarias.

Los organismos reguladores en muchos países piden cada vez más garantías a los proveedores de servicio en lo que respecta a las medidas de seguridad adoptadas y solicitan que ayuden más a los usuarios para lograr un uso de Internet seguro.

La Recomendación UIT-T X.1207, *Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado*, es una norma para:

a) promover las mejores prácticas en lo que respecta a noticias, autorizaciones de usuario y controles de usuario claros para los servicios que albergan la web; y

b) promover las mejores prácticas de seguridad (a través de los proveedores de servicios de telecomunicaciones) a los usuarios residenciales de los ordenadores y de Internet.

La Recomendación UIT-T X.1207 proporciona directrices claras para los proveedores de servicio sobre la gestión de riesgos de seguridad, el uso de productos seguros, la supervisión de la red y la respuesta, soporte y actualización pertinente y el uso seguro de la web. Se proporcionan consejos sobre directrices de usuario y formación y medidas de protección técnicas para los usuarios finales. Un apéndice proporciona vínculos a material adicional.

10.3 Notificación y difusión de actualizaciones de software

Los códigos maliciosos se pueden difundir con una velocidad alarmante e, incluso con las medidas de protección más modernas, se pueden propagar nuevas amenazas tan rápidamente que los sistemas y redes que no incluyan las últimas actualizaciones serán vulnerables. Los sistemas también son especialmente vulnerables a los últimos hallazgos del "día cero" (es decir, amenazas nuevas o no conocidas con anterioridad para las cuales todavía no se ha desarrollado una firma o parche antivirus). En este entorno, la distribución e instalación oportuna de actualizaciones es fundamental. Sin embargo, existen algunos problemas asociados con la distribución e implementación de esas actualizaciones.

La mayoría del software comercial, incluidos los sistemas operativos y los sistemas diseñados para proporcionar protección de seguridad (antivirus, antiespías, cortafuegos, etc.), contienen una característica que permite la actualización automática. No obstante, esta debe ser habilitada por el usuario. Cuando se notifica sencillamente al usuario que están disponibles actualizaciones (o quizás que se han descargado actualizaciones) el usuario debe actuar para permitir su descarga y/o instalación. Muchas actualizaciones requieren que los sistemas se reinicien tras la instalación, algo que cada usuario puede o no realizar inmediatamente. Las organizaciones con un programa de seguridad bien gestionado normalmente gestionan la actualización de forma centralizada, imponiendo las actualizaciones en los sistemas de usuario final. Por el contrario, la actualización de sistemas individuales (por ejemplo, ordenadores domésticos) y las de pequeñas organizaciones generalmente son poco sistemáticas.

Otro problema con la actualización rutinaria es que los vendedores de software no utilizan prácticas coherentes para notificar a los usuarios que disponen de actualizaciones o para indicarles las posibles consecuencias de no instalarlas. No disponen de un método uniforme para mantener informados a los usuarios sobre las mejores prácticas más recientes con el fin de mantener la seguridad del software. Además, no existe un método coherente para la notificación de problemas detectados por los usuarios tras la implementación de una actualización.

La Recomendación UIT-T X.1206, *Marco independiente del proveedor para la notificación automática relacionada con la seguridad y para la difusión automática de actualizaciones*, trata las dificultades asociadas con la actualización del software y facilita una forma independiente del proveedor de resolver los problemas. Una vez que se registra un elemento, se pueden poner automáticamente a disposición de los usuarios o directamente de las aplicaciones, actualizaciones sobre información de vulnerabilidad y parches o actualizaciones. La Recomendación UIT-T X.1206 proporciona un marco que puede utilizar cualquier vendedor para la notificación y también para facilitar información sobre vulnerabilidad y distribuir los parches/actualizaciones necesarios. También define el formato de la información que debería utilizarse en y entre los componentes.

La Recomendación UIT-T X.1206 permite a los administradores de sistemas conocer el estado de cualquier elemento del que es responsable. Describe los problemas de mantenimiento de los elementos desde un punto de vista de su identificación, y también desde el punto de vista de la difusión de información y de la gestión de los sistemas o redes. También proporciona una descripción de la seguridad que debería considerarse en el marco independiente del vendedor.

En la Recomendación UIT-T X.1206 se proporcionan definiciones de las estructuras de datos de los componentes que se precisan para este trabajo, incluido el esquema XML correspondiente, junto con el formato de información que debería utilizarse en y entre los componentes que constituyen este marco.

11. El futuro de la normalización de seguridad de las TIC

11 El futuro de la normalización de seguridad de las TIC

Durante más de 30 años, el UIT-T se ha dedicado a la elaboración de normas TIC. Este trabajo ha aumentado enormemente en los últimos años con el rápido crecimiento del uso de Internet y de otras redes y con el reconocimiento de la necesidad de proteger a los usuarios y a los sistemas frente a un creciente número y variedad de amenazas de seguridad.

Este manual ha proporcionado una visión amplia de algunas de las iniciativas clave relacionadas con la seguridad y de los logros de las Comisiones de Estudio del UIT-T en un esfuerzo por promover un mayor entendimiento de los trabajos y de los problemas técnicos a los que se enfrentan los usuarios y los diseñadores de redes. Se insta a los lectores a que aprovechen los amplios recursos en línea del UIT-T para obtener más detalles sobre los asuntos presentados aquí y a que utilicen las Recomendaciones y los documentos orientativos para contribuir a construir un entorno más seguro en Internet y para mejorar la confianza del usuario en las operaciones en línea.

Mirando hacia el futuro, las redes de telecomunicaciones y las redes de ordenadores seguirán convergiendo. Las redes de nueva generación y los servicios basados en la web seguirán creciendo rápidamente y cada vez serán más importantes, aunque surgirán amenazas, y seguirá siendo un desafío permanente diseñar y desarrollar contramedidas efectivas a esas amenazas. También constituirá un reto lograr el diseño y la implementación de sistemas y de redes mejores y más seguros de forma que se reduzcan sus vulnerabilidades inherentes.

Los 191 Estados Miembros y los más de 551 Miembros del sector de la UIT continuarán respondiendo a estos desafíos elaborando Recomendaciones técnicas y directrices sobre seguridad en un programa de trabajo agresivo impulsado por las necesidades de los Miembros y dirigido por la estructura organizativa establecida durante la Asamblea Mundial de Normalización de las Telecomunicaciones 2008. Siempre que sea posible, para reducir la duplicación de esfuerzos y centrarse en los recursos, el UIT-T colaborará con otras organizaciones de normalización para lograr las soluciones más armonizadas y rápidas posible.

12. Fuentes de información adicional

12 Fuentes de información adicional

Este manual presenta una visión general de los trabajos sobre seguridad del UIT-T. En el sitio web del UIT-T está disponible gratuitamente mucha más información detallada, incluidas muchas normas.

12.1 Visión general de los trabajos de la CE 17

La página inicial de la CE 17 proporciona enlaces a información sobre sus trabajos, en particular seminarios y presentaciones, resúmenes de las Recomendaciones que se están elaborando y personal clave. Los enlaces a la Comisión de Estudio rectora sobre seguridad de las telecomunicaciones y a la Comisión de Estudio rectora sobre gestión de identidad (IdM) proporcionan información sobre las actividades y resultados de los trabajos de estas dos Comisiones.

12.2 El compendio de seguridad

El compendio incluye información sobre las Recomendaciones de la UIT, información conexa y actividades de seguridad de la UIT. Está dividido en cinco partes, que se pueden descargar por separado:

- un catálogo de las Recomendaciones aprobadas relacionadas con la seguridad de las telecomunicaciones que incluye las designadas para fines de seguridad y las que describen o utilizan funciones de interés o necesidad para la seguridad;
- una lista de las definiciones de seguridad aprobadas por el UIT-T, extraída de las Recomendaciones UIT-T aprobadas;
- un resumen de las Comisiones de Estudio del UIT-T con actividades relacionadas con la seguridad;
- un resumen de las Recomendaciones que se están revisando en las Comisiones de Estudio del UIT-T para incluir consideraciones sobre seguridad;
- un resumen de otras actividades de seguridad de la UIT.

12.3 La hoja de ruta de las normas de seguridad

La hoja de ruta de las normas de seguridad es un recurso en línea que proporciona información sobre las normas de seguridad de las TIC existentes y de los trabajos en curso en organizaciones de normalización clave. Además de la información sobre los trabajos de seguridad del UIT-T, la hoja de ruta incluye información sobre los trabajos de normas sobre seguridad de ISO/CEI, ATIS, ENISA, ETSI, IEEE, IEFT, OASIS, 3GPP y 3GPP2.

Como el compendio, la hoja de ruta está dividida en cinco partes y la mayor parte de la información es accesible en línea:

- Parte 1, *Organizaciones de desarrollo de normas TIC y sus trabajos*, que contiene información sobre la estructura de la hoja de ruta y sobre cada una de las organizaciones de normalización enumeradas. La parte 1 también proporciona enlaces a glosarios y vocabularios de seguridad existentes;
- Parte 2, *Normas de seguridad TIC aprobadas*, que incluye una base de datos accesible de las normas de seguridad aprobadas con enlaces directos a la mayoría de ellas;
- Parte 3, *Normas de seguridad en desarrollo*;
- Parte 4, *Futuras necesidades y nuevas normas de seguridad propuestas*; y
- Parte 5, *Mejores prácticas de seguridad*.

12.4 Directrices para la implementación de la seguridad

El suplemento 3 de la serie de Recomendaciones UIT-T X.800-X.849, *Suplemento sobre directrices para la implementación de la seguridad en sistemas y redes*, proporciona unos antecedentes más detallados sobre algunos de los asuntos tratados en este manual y aporta directrices para la implementación de la seguridad en sistemas y redes que se puede utilizar para realizar un programa de seguridad de redes. Estas directrices consideran cuatro ámbitos: la política de seguridad técnica; la identificación de elementos; las amenazas, vulnerabilidades y mitigaciones; y la evaluación de la seguridad. Las directrices indican los componentes clave necesarios para construir y gestionar la política técnica necesaria para gestionar redes que pueden incluir múltiples operadores y contener productos y sistemas provenientes de múltiples vendedores. También proporciona directrices sobre asuntos reglamentarios.

12.5 Información adicional sobre el directorio, la autenticación y la gestión de identidad

Para más información sobre la serie de Recomendaciones UIT-T X.500, la fuente de información es la propia serie de Recomendaciones UIT-T X.500. En www.x500standard.com se puede encontrar más información y una guía para diseñadores. Los enlaces siguientes incluyen información adicional:

http://www.x500standard.com/index.php?n=X509.X509ProtectingDirectory tiene información sobre autenticación de usuario;

http://www.x500standard.com/index.php?n=X500.AccessControl ofrece más información sobre el control de acceso; y

http://www.x500standard.com/index.php?n=X500.DataPrivacyProtection proporciona una descripción más amplia de las características de privacidad de datos X.500.

Anexo A – Definiciones relativas a la seguridad

Anexo A
Definiciones relativas a la seguridad

The following table contains definitions for terms used in the manual. All definitions are contained in current ITU-T Recommendations. A more complete list of security definitions is contained in the compendium of ITU-T approved security definitions extracted from ITU-T Recommendations maintained by Study Group 17.

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
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
algoritmo	Proceso matemático que puede utilizarse para criptar y descriptar flujos de datos.	J.93
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 (AA)	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

Término	Definición	Referencia
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
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
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
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
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

Término	Definición	Referencia
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
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 súper cifrado.	X.800
texto no cifrado	Datos inteligibles, cuyo contenido semántico está disponible.	X.800
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
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
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 la Recomendación UIT-T 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

Término	Definición	Referencia
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
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
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
escucha clandestina	Violación de la confidencialidad mediante la supervisión de las comunicaciones.	M.3016.0
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.	J.170 J.93
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/UIT-T X.811.	X.811
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
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

Término	Definición	Referencia
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
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
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
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
Ataque de intermediarios	Ataque en el que un atacante es capaz de leer, insertar y modificar a voluntad mensajes entre dos partes sin que ninguna de las partes sepa que el vínculo entre ellas ha sido interceptado.	X.800
usurpación de identidad (o impostura)	Cuando una entidad pretende ser una entidad diferente.	X.800
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
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
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

Término	Definición	Referencia
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	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
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

Término	Definición	Referencia
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
certificado de lista de revocaciones	Certificado de seguridad que contiene una lista de certificados de seguridad que han sido revocados.	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
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
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
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 de Recomendaciones UIT-T X.800 se adopta el término certificado de seguridad para evitar conflictos de terminología con la Recomendación UIT-T 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
información de seguridad (SI)	Información necesaria para implementar los servicios de seguridad.	X.810
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
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

Término	Definición	Referencia
Amenaza a la seguridad	Posible violación de la seguridad.	X.800
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
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
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
spam	Correo electrónico no solicitado y no deseado.	H.235
falsificación	Suplantación de personalidad de un recurso o usuario legítimo.	X.509
autenticación robusta	Autenticación por medio de credenciales derivadas criptográficamente.	X.811
Ataque Sybil	Ataque en el que se subvierte el sistema de repudio de una red par a par generando un gran número de pseudo entidades y utilizándolas para lograr una audiencia desproporcionadamente amplia.	X.810
amenaza	Violación potencial de la seguridad.	X.800
testigo	Véase testigo de seguridad.	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
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
Red de sensores ubicua (USN)	Red que utiliza sensores baratos y de baja potencia para obtener datos del contexto con el fin de aportar información y servicios de conocimiento a todos, en cualquier momento y en cualquier lugar. Una USN puede cubrir una amplia zona geográfica y puede soportar diversas aplicaciones.	
acceso no autorizado	Cuando una entidad intenta acceder a datos, violando la política de seguridad en vigor.	M.3016.0
autenticación del usuario	Comprobar la identidad del usuario o el proceso de aplicación.	M.3016.0
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 UIT-T X.509	Especificación de certificado de una clave pública que forma parte de las normas de la Rec. UIT-T X.500.	J.170

Anexo B – Acrónimos y abreviaturas utilizados en este Manual

Anexo B
Acrónimos y abreviaturas utilizados en este Manual

Acrónimos	Significado
ACI	Información de control de acceso (*access control information*)
AES	Algoritmo de criptación avanzada (*advanced encryption standard algorithm*)
AMDC	Acceso múltiple por distribución en el código
AMNT	Asamblea Mundial de Normalización de las Telecomunicaciones
ASN.1	Notación de sintaxis abstracta uno (*abstract syntax notation one*)
ASP	Proveedor de servicio de aplicación (*application service provider*)
ATIS	Alianza para soluciones del sector de la telecomunicaciones (*Alliance for Telecommunications Industry Solutions*)
A/V	Audiovisual
BioAPI	Programa de aplicaciones biométricas/interfaz de programación
BPON	Red óptica pasiva de banda ancha (*broadband passiveoptical network*)
B2C	Empresa a cliente (*business-to-costumer*)
CA	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.
CE	Comisión de Estudio
CMIP	Protocolo común de información de gestión (*common management information protocol*)
CORBA	Arquitectura de intermediario de petición de objeto común (*common object request broker architecture*)
CP	Política de certificado (*certificate policy*)
CPS	Declaración de ejecución práctica de la certificación (*certification practice statement*)
CRL	Lista de revocación de certificados (*certificate revocation list*)
DNS	Servidor/sistema/servicio de nombre de dominio (*domain name server/system/service*)
DSL	Bucle de abonado digital (*digital subscriber loop*)
EAP	Protocolo de autenticación extensible (*extensible authentication protocol)*)
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
ETSI	Instituto Europeo de Normas de Telecomunicaciones
FMC	Convergencia móvil fijo (*fixed mobile convergence*)
FW	Cortafuegos (*firewall*)
GK	Controlador de acceso (*gatekeeper*)
GPRS	Sistema radioeléctrico general por paquetes (*general packet radio system*)
GSM	Sistema mundial para comunicaciones móviles (*global system for Mobile Communications*)
GW	Pasarela (*gateway*)
HFX	Cifrado de facsímil Hawthorne (*Hawthorne facsimile cipher*)
HKM	Algoritmo de gestión de claves de Hawthorne (*Hawthorne key management algorithm*)
HTTP	Protocolo de transferencia hipertexto (h*ypertext transfer protocol*)
ICT	Tecnologías de la información y la comunicación (*information and communication technology*)

Acrónimos	Significado
ID	Identificador (*identifier*)
IdM	Gestión de identidad (*identity management*)
CEI	Comisión Electrotécnica Internacional
IEEE	Instituto de Ingenieros en Electricidad y en Electrónica (*Institute of Electrical and Electronics Engineers*)
IETF	Grupo de Tareas sobre Ingeniería de Internet
IKE	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
IM	Mensajería instantánea (*instant messaging*)
IMS	Subsistema IP multimedios (*IP multimedia subsystem*)
IMT-2000	Telecomunicaciones móviles internacionales-2000 (*international mobile telecommunications 2000*)
IP	Protocolo Internet (*Internet protocol*)
IPSec	Seguridad del protocolo Internet (*Internet protocol security*)
IPTV	Televisión por el protocolo Internet (*Intenet protocol television*)
IPX	Intercambio de paquetes por Internet (*Internet packet Exchange*)
ISMS	Sistema de gestión de seguridad de la información (*information security Management system*)
ISO	Organización Internacional de Normalización (*International Organization for Standardization*)
LAN	Red de área local (*local area network*)
LDAP	Protocolo ligero de acceso al directorio (*lightweight directory access protocol*)
MD5	Sumario de mensaje N.º 5 (un algorítmo hash seguro) (*message digest No. 5*)
MIS	Servicio de información de gestión (*management information service*)
MTA	Adaptador de terminal de medios (en tecnología de cable) (*media terminal adapter*) Agente de transferencia de mensajes (en mensajería) (*message transfer agent*)
MWSSG	Pasarela de seguridad de servicios móviles por la web (*Mobile web services security Gateway*)
NAT	Traducción de direcciones de red (*network address translation*)
NGN	Red de nueva generación (*next generation networrk*)
OASIS	(*Organization for the Advancement of Structured Information Standards*)
OMG	Grupo de gestión de objetos (*objects Management group*)
OSI	Interconexión de sistemas abiertos (*open systems interconnection*)
P2P	Entre pares (*peer-to-peer*)
PDA	Agenda digital personal (*personal data assistant*)
PIN	Número de identificación personal (*personal identification number*)
PII	Información identificable personalmente (*personally identifiable information*)
PKI	Infraestructura de claves públicas (*public key infrastructure*)
PKINIT	Autenticación inicial mediante criptografía de clave pública (*public key cryptography initial authentication*)
PMI	Infraestructura de gestión de privilegios (*privilege management infrastructure*)
PSS	Servicio de protección PII (*PII protection service*)
QoS	Calidad de servicio (*quality of service*)
RBAC	Control de acceso basado en los cometidos (*role-based access control*)
RFID	Identificación de frecuencia radioeléctrica (*radio frequency identification*).

Acrónimos	Significado
RSA	Rivest, Shamir y Adleman (algoritmo de clave pública)
RTP	Protocolo en tiempo real (*real time protocol*)
RTPC	Red telefónica pública conmutada (*public switched telephone network*)
SAML	Lenguaje de marca de aserto de seguridad (*security assertion markup language*)
SHA1	Algoritmo de generación numérica seguro N.º 1 (*secure hash algorithm No. 1*)
SIP	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
SMS	Servicio de mensajes cortos (*short message service*)
SMTP	Protocolo simple de transferencia de correos (*simple mail transfer protocol*)
SNMP	Protocolo simple de gestión de red (*simple network management protocol*)
SoA	Fuente de autoridad (*source of authority*)
SOA	Arquitectura orientada al servicio (*service oriented architecture*)
SPAK	Protocolo de autenticación basado en contraseña segura (*secure passwor-based authentication protocol*)
SSL	Capa de zócalo segura (*secure socket layer*)
SSO	Firma única (*single sign-on*)
TCP/IP	Protocolo de control de transmisión/protocolo de Internet (*transmisión control protocol/Internet protocol*)
TLS	Seguridad de capa de transporte (*transport layer security*)
RGT	Red de gestión de las telecomunicaciones
UE	Equipo de usuario (*user equipment*)
UICC	Tarjeta de circuito integrado universal (*universal integrated circuit card*)
UIT-T	Sector de normalización de las telecomunicaciones de la Unión Internacional de Telecomunicaciones
USN	Red de sensores ubicuos (*ubiquitous sensor network*)
VoIP	Voz por IP (*voice over IP*)
VPN	Red privada virtual (*virtual private network*)
WAN	Red de área extensa (*wide area network*)
Wi-Fi	Fidelidad inalámbrica (*gíreles fidelity*) (marca de la alianza Wi-Fi para productos certificados basados en las normas IEEE 802.11)
XACML	Lenguaje de marcaje de control de acceso extensible (*extensible access control markup language*)
XML	Lenguaje de marcaje extensible (*extensible markup language*)
3G	Tercera generación (*3rd generation*)
3GPP	Proyecto de asociación de tercera generación (*3rd generation partnership project*)
3GPP2	Proyecto de asociación de tercera generación Nº 2 (*3rd generation partnership Project 2*)

Anexo C – Resumen de las Comisiones de Estudio del UIT-T relacionadas con la seguridad

Anexo C
Resumen de las Comisiones de Estudio del UIT-T relacionadas con la seguridad

El trabajo de la mayoría de las Comisiones de Estudio incluye por lo menos algunos aspectos de la seguridad de las telecomunicaciones y/o de las TIC. Cada Comisión de Estudio es responsable de tratar los estudios de seguridad dentro de su propio ámbito de responsabilidad, aunque la CE 17, que está centrada en la seguridad ha sido designada la Comisión de Estudio rectora sobre seguridad. El cuadro 8 resume las funciones de las Comisiones de Estudio con responsabilidades relativas a la seguridad y enumera sus respectivas responsabilidades como Comisión de Estudio rectora.

Cuadro 3 – Comisiones de Estudio con responsabilidades relacionadas con la seguridad

Comisión de Estudio	Título	Responsabilidades/función de seguridad
CE 2	Aspectos de explotación de la prestación de servicios y de la gestión de las telecomunicaciones	Comisión de Estudio rectora para la definición de servicios, la numeración y el encaminamiento Comisión de Estudio rectora sobre las telecomunicaciones para alertas y desastres Comisión de Estudio rectora sobre gestión de las telecomunicaciones
CE 5	Entorno y cambio climático	Comisión de Estudio rectora sobre compatibilidad electromagnética y efectos el entorno electromagnético Comisión de Estudio rectora sobre TIC y cambio climático
CE 9	Redes de cable integradas de banda ancha y transmisión de televisión y sonido	Comisión de Estudio rectora sobre redes de cable integradas de banda ancha y televisión
CE 11	Requisitos de señalización, protocolos y especificaciones de prueba	Comisión de Estudio rectora sobre señalización y protocolos Comisión de Estudio rectora sobre redes inteligentes Comisión de Estudio rectora sobre especificaciones de pruebas
CE 12	Calidad de funcionamiento, calidad de servicio y calidad de la experiencia	Comisión de Estudio rectora sobre calidad de servicio y calidad de experiencia
CE 13	Redes futuras incluidas la red móvil y las redes de la próxima generación	Comisión de Estudio rectora para futuras redes y NGN Comisión de Estudio rectora sobre gestión de movilidad y convergencia fijo-móvil
CE 15	Infraestructuras de las redes de transporte y de las redes de acceso ópticas	Comisión de Estudio rectora sobre transporte por redes de acceso Comisión de Estudio rectora sobre tecnología óptica Comisión de Estudio rectora sobre redes de transporte ópticas
CE 16	Codificación, sistemas y aplicaciones multimedios	Comisión de Estudio rectora sobre codificación, sistemas y aplicaciones multimedios Comisión de Estudio rectora sobre aplicaciones ubicuas ("e-everything", como la telemedicina) Comisión de Estudio rectora sobre accesibilidad a las telecomunicaciones/TIC para personas con discapacidades
CE 17	Seguridad	Comisión de Estudio rectora sobre seguridad de las telecomunicaciones Comisión de Estudio rectora sobre gestión de identidad Comisión de Estudio rectora sobre lenguajes y técnicas de descripción

Anexo D – Recomendaciones de seguridad referenciadas en este Manual

Anexo D
Recomendaciones de seguridad referenciadas en este manual

Este anexo incluye una lista completa de todas las Recomendaciones UIT-T referenciadas en este manual junto con un hipervínculo de forma que los lectores que estén utilizando una versión electrónica del texto pueden enlazar directamente para descargar las Recomendaciones. Como se indica en el texto, el UIT-T ha desarrollado muchas normas relacionadas con la seguridad en colaboración con otras organizaciones de normalización. También se incluyen en este cuadro las Recomendaciones comunes/gemelas publicadas actualmente relacionadas con la seguridad de las TIC. Se puede acceder al conjunto completo de las Recomendaciones UIT-T en línea en: www.itu.int/rec/T-REC/en. Las Recomendaciones UIT-T relacionadas con la seguridad están disponibles en la parte 2 (base de datos) de la hoja de ruta de normas de seguridad (www.itu.int/ITU-T/studygroups/com17/ict/index.html).

Recomendación	Título	Texto equivalente
E.408	Requisitos de seguridad para las redes de telecomunicaciones	
E.409	Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones	
G.827	Parámetros y objetivos de disponibilidad para trayectos digitales internacionales de extremo a extremo de velocidad binaria constante	
G.1000	Calidad de servicio de las comunicaciones: Marco y definiciones	
G.1030	Estimación de la calidad de funcionamiento de extremo a extremo en redes IP para aplicaciones de datos	
G.1050	Modelo de red para evaluar la calidad de la transmisión multimedia por el protocolo Internet	
G.1081	Puntos de control de calidad de funcionamiento de IPTV	
H.235.0	Marco de seguridad H.323: Marco de seguridad para sistemas multimedia 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	H.323 security framework: Voice encryption profile with native H.235/H.245 key management	
H.Imp235	Guía para diseñadores de H.235 V3: " Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245) "	
H.323	Sistemas de comunicación multimedios basados en paquetes	
H.350	Arquitectura de servicios de directorio para conferencia multimedios	
H.460.17	Utilización de la conexión de señalización de llamadas H.225.0 como transporte de mensajes RAS H.323	

Recomendación	Título	Texto equivalente
H.460.18	Paso de señalización H.323 a través de traductores de dirección de red y cortafuegos	
H.460.19	Paso de medios H.323 por traductores de dirección de red y cortafuegos	
H.510	Movilidad para sistemas y servicios multimedios H.323	
H.350	Arquitectura de servicios de directorio para conferencia multimedios	
H.530	Procedimientos de seguridad simétricos para movilidad de sistemas H.323 según la Recomendación H.510	
J.160	Arquitectura para la distribución de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable	
J.170	Especificación de la seguridad de IPCablecom	
J.360	Arquitectura general IPCablecom2 – Documento principal	
M.3010	Principios para una red de gestión de las telecomunicaciones	
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: Mecanismo de seguridad	
M.3016.4	Seguridad en el plano de gestión: Formulario de características	
M.3208.2	Servicios de gestión de la RGT para redes de circuitos especializados y reconfigurables: Gestión de conexiones de enlaces de servicio proporcionados previamente para formar un servicio de circuitos arrendados	
M.3210.1	Servicios de gestión de la RGT para la gestión de la seguridad de las telecomunicaciones móviles internacionales-2000 (IMT-2000)	
Q.816	Servicios de la red de gestión de las telecomunicaciones basados en CORBA	
Q.834.3	Descripción del lenguaje de modelado unificado para los requisitos de interfaz de gestión de redes ópticas pasivas de banda ancha	
Q.834.4	Especificación de interfaz de arquitectura de intermediario de petición de objeto común para las redes ópticas pasivas de banda ancha basada en los requisitos de interfaz del lenguaje de modelado unificado	
Q.1701	Marco para las redes de las telecomunicaciones móviles internacionales-2000 (IMT-2000)	
Q.1702	Visión a largo plazo de las características de las redes de sistemas posteriores a los sistemas de las telecomunicaciones móviles internacionales-2000 (IMT-2000)	
Q.1703	Marco de capacidades de servicio y de red desde la perspectiva de la red para los sistemas posteriores a las IMT-2000	
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	3GPP

Recomendación	Título	Texto equivalente
Q.1742.1	Referencias IMT-2000 a la red medular desarrollada ASNI-41 con red de acceso cdma2000	3GPP2
T.4	Normalización de los terminales facsímil del grupo 3 para la transmisión de documentos	
T.36	Capacidades de seguridad para su utilización con terminales facsímil del grupo 3	
T.37	Procedimientos para la transferencia de datos facsímil en modo almacenamiento y retransmisión por Internet	
T.38	Procedimientos para la comunicación facsímil en tiempo real entre terminales facsímil del grupo 3 por redes con protocolo Internet	
T.563	Características de terminal para aparatos facsímil del grupo 4	
X.500	El directorio: Visión de conjunto de conceptos, modelos y servicios	ISO/CEI 9594-1
X.501	El directorio: Modelos	ISO/CEI 9594-2
X.509	El directorio: Marcos para certificados de claves públicas y atributos	ISO/CEI 9594-8
X.511	El directorio: Definición de servicio abstracto	ISO/CEI 9594-3
X.518	El directorio: Procedimientos para operación distribuida	ISO/CEI 9594-4
X.519	El directorio: Especificaciones de protocolo	ISO/CEI 9594-5
X.520	El directorio: Tipos de atributos seleccionados	ISO/CEI 9594-6
X.521	El directorio: Clases de objeto seleccionadas	ISO/CEI 9594-7
X.525	El directorio: Replicación	ISO/CEI 9594-9
X.530	El directorio: Utilización de la gestión de sistemas para la administración del directorio	ISO/CEI 9594-10
X.711	Protocolo común de información de gestión: Especificación	ISO/CEI 9596-1
X.736	Gestión de sistemas: Función señaladora de alarmas de seguridad	ISO/CEI 10164-7
X.740	Gestión de sistemas: Función de pista de auditoría de seguridad	ISO/CEI 10164-8
X.741	Gestión de sistemas: Objetos y atributos para el control de acceso	ISO/CEI 10164-9
X.780	Directrices de la RGT para la definición de objetos gestionados mediante arquitectura de intermediario de petición de objeto común	
X.780.1	Directrices de la RGT para la definición de interfaces de objetos gestionados mediante arquitectura de intermediario de petición de objeto común de de granularidad gruesa	
X.780.2	Directrices de la TMN para definir objetos CORBA de gestión orientados al servicio y objetos CORBA de fachada	
X.781	Requisitos y directrices para los formularios de declaración de conformidad de implementación asociados con sistemas basados en CORBA	
X.790	Función de gestión de dificultades para aplicaciones del UIT-T	
X.800	Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT	ISO/CEI 7498-2
X.802	Modelo de seguridad de capas más bajas	ISO/CEI TR 13594
X.803	Modelo de seguridad de capas superiores	ISO/CEI 10745
X.805	Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo	ISO/CEI 18028-2
X.810	Marcos de seguridad para sistemas abiertos: Visión general	ISO/CEI 10181-1

Recomendación	Título	Texto equivalente
X.811	Marcos de seguridad para sistemas abiertos: Marco de autenticación	ISO/CEI 10181-2
X.812	Marcos de seguridad para sistemas abiertos: Marco de control de acceso	ISO/CEI 10181-3
X.813	Marcos de seguridad en sistemas abiertos: Marco de no rechazo	ISO/CEI 10181-4
X.814	Marcos de seguridad para sistemas abiertos: Marco de confidencialidad	ISO/CEI 10181-5
X.815	Marcos de seguridad para sistemas abiertos: Marco de integridad	ISO/CEI 10181-6
X.816	Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad	ISO/CEI 10181-7
X.830	Seguridad genérica de las capas superiores: Sinopsis, modelo y notación	ISO/CEI 11586-1
X.831	Seguridad genérica de las capas superiores: Definición del servicio basado en el elemento de intercambio de seguridad	ISO/CEI 11586-2
X.832	Seguridad genérica de las capas superiores: Especificación del protocolo de elemento de servicio de intercambio de seguridad	ISO/CEI 11586-3
X.833	Seguridad genérica de las capas superiores: Especificación de la sintaxis de transferencia de protección	ISO/CEI 11586-4
X.834	Seguridad genérica de las capas superiores: Formularios de declaración de conformidad de implementación del protocolo del elemento de servicio de intercambio de seguridad	ISO/CEI 11586-5
X.835	Seguridad genérica de las capas superiores: Formulario de declaración de conformidad de implementación de protocolo de la sintaxis de transferencia de protección	ISO/CEI 11586-6
X.841	Técnicas de seguridad – Objetos de información de seguridad para control de acceso	ISO/CEI 11586
X.842	Técnicas de seguridad – Directrices sobre el uso y gestión de servicios a tercera parte confiable	ISO/CEI TR 15416
X.843	Técnicas de seguridad – Especificación de servicios de tercera parte confiable para soportar la aplicación de firmas digitales	ISO/CEI 15945
X.Sup3 aX.800-X.849	Suplemento sobre directrices para la implementación de la seguridad entre sistemas y redes	
X.1031	Cometidos de los usuarios finales y de las redes de telecomunicaciones en la arquitectura de seguridad	
X.1034	Directrices sobre la autentificación y la gestión de claves basadas en el Protocolo de Autentificación Extensible en una red de comunicación de datos	
X.1035	Protocolo de intercambio de claves con autentificación mediante contraseña	
X.1036	Marco para la creación, almacenamiento, distribución y ejecución de políticas para la seguridad de las redes	
X.1051	Técnicas de seguridad – Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones	ISO/CEI 27011
X.1055	Guía para la gestión de riesgos y el perfil de riesgos	
X.1056	Directrices para la gestión de incidentes de seguridad en organizaciones de telecomunicaciones	

Recomendación	Título	Texto equivalente
X.1081	Marco para la especificación de los aspectos de la telebiometría relativos a protección y seguridad	
X.1082	Telebiometría relativa a fisiología humana	ISO/CEI 80000-14
X.1083	Biométrica – Protocolo para el interfuncionamiento con interfaces de programación de aplicaciones de tecnologías biométricas	ISO/CEI 24708
X.1084	Mecanismo del sistema de telebiometría – Parte 1: Protocolo general de autenticación biométrica y características de un modelo de sistema para sistemas de telecomunicaciones	
X.1086	Procedimientos de protección telebiométrica – Parte 1: Guía sobre las medidas técnicas y de gestión para la protección de la seguridad de los datos biométricos	
X.1088	Marco de claves digitales de telebiometría (TDK) – Un marco de generación y protección de claves digitales biométricas	
X.1089	Infraestructura de autenticación de telebiometría (TAI)	
X.1111	Marco de tecnologías de la seguridad para redes domésticas	
X.1112	Perfil del certificado de dispositivos de la red doméstica	
X.1113	Directrices sobre los mecanismos de autenticación de usuarios para servicios de la red doméstica	
X.1114	Marco de autorización para la red doméstica	
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	
X.1123	Servicio diferenciado de seguridad para comunicaciones de datos móviles seguras de extremo a extremo	
X.1124	Arquitectura de autenticación para comunicaciones móviles de extremo a extremo	
X.1125	Sistema de reacción correlativo en comunicaciones móviles de datos	
X.1141	Lenguaje de etiquetas de aserción de seguridad (SAML 2.0)	OASIS SAML 2.0
X.1142	Lenguaje de etiquetas de control de acceso extensible (XACML 2.0)	OASIS XACML 2.0
X.1143	Arquitectura de seguridad para seguridad de mensajes en servicios móviles de la web	
X.1151	Guía sobre protocolos seguros de autenticación con intercambio de claves	
X.1152	Técnicas de comunicación segura de datos de extremo a extremo que utilizan servicios fiables de terceros	
X.1161	Marco para comunicaciones seguras entre pares	
X.1162	Arquitectura y operaciones de seguridad para redes entre pares	
X.1171	Amenazas y requisitos para la protección de información identificable personalmente en las aplicaciones que utilizan la identificación basada en las etiquetas	
X.1191	Requisitos funcionales y arquitectura de los aspectos relativos a la seguridad de la TVIP	
X.1205	Aspectos generales de la ciberseguridad	

Recomendación	Título	Texto equivalente
X.1206	Marco independiente del proveedor para la notificación automática de información relacionada con la seguridad y para la difusión automática de actualizaciones	
X.1207	Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado	
X.1231	Estrategias técnicas contra el correo basura	
X.1240	Tecnologías utilizadas contra el correo basura	
X.1241	Marco técnico contra el correo basura	
X.1242	Sistema de filtrado de correo basura en el servicio de mensajes cortos (SMS) basado en reglas especificadas por el usuario	
X.1244	Aspectos globales para contrarrestar el correo basura en las aplicaciones multimedias en las redes IP	
X.1250	Capacidades básicas para una confiabilidad y una interoperabilidad mejoradas de la gestión de identidad global	
X.1251	Marco para el control por el usuario de la identidad digital	
X.1303	Protocolo de alerta común (CAP 1.1)	OASIS CAP v1.1
X.Sup6	Serie ITU-T X.1240 – Suplemento sobre cómo contrarrestar el correo basura y otras amenazas asociadas	
X.Sup7	Serie ITU-T X.1250 – Suplemento sobre la visión general de la gestión de identidad en el contexto de la ciberseguridad	
X.2001	Visión general de las redes de próxima generación	
X.2701	Requisitos de seguridad para las redes de próxima generación	
	Otras publicaciones	
	Tecnologías de planta externa y microprocesadores para la construcción, instalación y protección de cables de telecomunicaciones	

Impreso en Suiza
Ginebra, 2010