Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2701

(04/2007)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Seguridad

Requisitos de seguridad para las redes de la próxima generación, versión 1

Recomendación UIT-T Y.2701

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

DISPONIBLE	Y.1–Y.99
INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
Disponible	Y.900–Y.999
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Disponible	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Disponible	Y.2600–Y.2699
Seguridad	**Y.2700–Y.2799**
Movilidad generalizada	Y.2800–Y.2899
Disponible	Y.2900–Y.2999

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

Recomendación UIT-T Y.2701

Requisitos de seguridad para las redes de la próxima generación, versión 1

Resumen

La presente Recomendación dispone requisitos de seguridad para las redes de la próxima generación (NGN) y sus interfaces (por ejemplo, UNI, NNI y ANI) aplicando la Rec. UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*, a la Rec. UIT-T Y.2201, *Requisitos de la versión 1 de las redes de la próxima generación*, y a la Rec. UIT-T Y.2012, *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.

Estos requisitos consisten en proporcionar seguridad de red a las comunicaciones de usuario extremo a través de dominios administrativos de múltiples redes. La seguridad de los activos y la información de los clientes en el dominio de cliente (por ejemplo, red del usuario), y la utilización de aplicaciones par a par en los equipos del cliente quedan fuera del alcance de esta Recomendación.

En esta Recomendación se utiliza un modelo de confianza basado en los elementos de red (cajas físicas). Los proveedores NGN instalarán elementos de red que soporten las entidades funcionales definidas en la Rec. UIT-T Y.2012. La agregación de estas entidades funcionales con un elemento de red determinado variará, dependiendo del vendedor. Por consiguiente, el objetivo de esta Recomendación no es mostrar la relación estricta y fija entre las entidades funcionales lógicas y los elementos de red físicos.

Los requisitos que figuran en esta Recomendación deben considerarse como un conjunto mínimo de requisitos de seguridad y se anima a los proveedores de NGN a tomar cualquier otra medida además de las especificadas en las Recomendaciones para la seguridad de la NGN.

Orígenes

La Recomendación UIT-T Y.2701 fue aprobada el 27 de abril de 2007 por la Comisión de Estudio 13 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
1.1 Principios definidos en la Recomendación UIT-T X.805 2
1.2 Hipótesis 3
1.3 Resumen 3
2 Referencias 4
3 Definiciones y abreviaturas 4
3.1 Términos definidos en otros documentos 4
3.2 Términos definidos en esta Recomendación 4
3.3 Abreviaturas y acrónimos 6
4 Amenazas y riesgos contra la seguridad 7
5 Modelo de confianza de seguridad 9
5.1 Modelo de confianza de una sola red 9
5.2 Modelo de confianza de redes pares 11
6 Arquitectura de seguridad 11
6.1 Arquitectura funcional de referencia de la NGN 11
6.2 Correspondencia con la arquitectura funcional NGN 13
6.3 Identificación de recursos NGN para protección de seguridad 15
7 Objetivos y requisitos 19
7.1 Objetivos de seguridad generales 19
7.2 Objetivos para la seguridad a través de múltiples dominios de proveedores de red 20
7.3 Requisitos específicos para las dimensiones de seguridad 20
8 Requisitos específicos de seguridad 22
8.1 Requisitos de seguridad comunes para los elementos de las NGN 22
8.2 Requisitos de los elementos de red NGN en la zona fiable 26
8.3 Requisitos de los elementos frontera de la NGN en el dominio "fiable pero vulnerable" 26
8.4 Requisitos para los elementos frontera TE en el dominio "no fiable" 27
8.5 Recomendaciones de seguridad para el equipo terminal en el dominio "no fiable" 27
Apéndice I – Objetivos de seguridad y directrices para la interconexión de servicios de telecomunicaciones de emergencia 28
I.1 Antecedentes 28
I.2 Alcance/propósito 28
I.3 Objetivos generales 28
I.4 Capacidades de seguridad generales 30
I.5 Autenticación, autorización y control de acceso 30
I.6 Confidencialidad y privacidad 30

Página

I.7 Integridad de datos 31
I.8 Comunicación 31
I.9 Disponibilidad 31
Bibliografía 32

Recomendación UIT-T Y.2701

Requisitos de seguridad para las redes de la próxima generación, versión 1

1 Alcance

Esta Recomendación dispone requisitos para la protección de las redes de la próxima generación (NGN) contra las amenazas de seguridad. Dicha seguridad se logra aplicando los principios de la Rec. UIT-T X.805, *Arquitectura de seguridad para los sistemas de comunicaciones extremo a extremo*, a la Rec. UIT-T Y.2201, *Requisitos de la versión 1 de las redes de la próxima generación*, y a la Rec. UIT-T Y.2012, *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.

Estos requisitos pretenden proteger los siguientes elementos en un entorno multired:

- la infraestructura de la red y el proveedor de servicios y sus activos (por ejemplo, activos y recursos de las 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 las NGN (por ejemplo, servicios de voz, vídeo y datos);
- comunicaciones de información de usuario extremo (por ejemplo, información privada).

Los requisitos consisten en proporcionar seguridad basada en la red a las comunicaciones de usuario extremo a través de dominios administrativos multired. La seguridad de los activos e informaciones del cliente en el dominio de cliente (por ejemplo, red del usuario) y la utilización de aplicaciones par a par en los equipos del cliente quedan fuera del alcance de esta Recomendación.

Los requisitos especificados por la presente Recomendación se aplican a una NGN, incluidas las interfaces usuario-red (UNI, *user-to-network interfaces*), interfaces red-red (NNI, *network-to-network interfaces*) e interfaces aplicación-red (ANI, *application-to-network interface*) en un entorno multired.

Los proveedores de servicios NGN implantarán "elementos de red" que soporten las entidades funcionales definidas en [UIT-T Y.2012]. La vinculación de estas entidades funcionales a un elemento de red determinado variará, dependiendo del vendedor. Por consiguiente, no es el objetivo de esta Recomendación mostrar una relación estricta y fija entre entidades funcionales lógicas y elementos de red físicos.

Debe considerarse que los requisitos de esta Recomendación son un conjunto mínimo de requisitos para la seguridad de las NGN y no son exhaustivos, por lo que los proveedores de NGN habrán de adoptar otras medidas además de las ya especificadas en las Recomendaciones para la seguridad de las NGN.

Además, los requisitos de esta Recomendación abarcan algunos aspectos técnicos de lo que generalmente se conoce como IdM ("gestión de identidad"). La definición del trabajo de IdM es "gestión por parte de los proveedores de las NGN de atributos fiables de una entidad tales como un abonado, un dispositivo o un proveedor". Por tanto, no se pretende realizar una validación positiva de una persona.

Las administraciones pueden exigir a los proveedores de las NGN que tengan en cuenta los requisitos de los reglamentos y políticas nacionales al aplicar esta Recomendación.

1.1 Principios definidos en la Rec. UIT-T X.805

[UIT-T X.805] define las siguientes dimensiones de seguridad:

control de acceso;

autenticación;

no repudio;

confidencialidad de datos;

seguridad de las comunicaciones;

integridad de datos;

disponibilidad;

privacidad.

Se identifican asimismo las siguientes amenazas contra la seguridad:

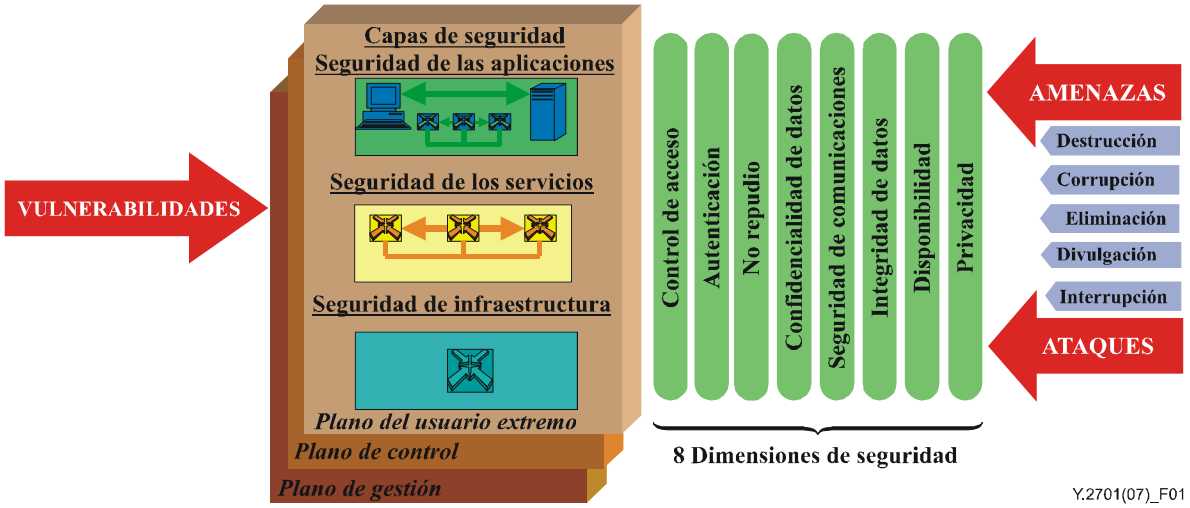

Figura 1 – Arquitectura de Seguridad de X.805 (figura 3/X.805)

Estas dimensiones y amenazas en materia de seguridad se consideran como la base de la presente Recomendación.

La presente Recomendación no define ni distingue la utilización de las capas de seguridad (aplicación, servicios o infraestructura) indicadas en la Rec. UIT-T X.805 y la conformidad a esta norma no requiere dicha distinción. Esta Recomendación hace referencia a una distinción entre el tráfico de los planos de gestión, control y usuario, pero advierte al lector que la utilización de esa clasificación varía según la capa de la pila de protocolos en consideración. Por consiguiente, será necesario hacer referencia a otras normas con objeto de determinar la conformidad a las distinciones indicadas. Esta norma formula recomendaciones con respecto a la aplicación de las dimensiones de seguridad pero no infiere que sean suficientes para evaluar la seguridad de las NGN.

1.2 Hipótesis

Esta Recomendación se basa en las siguientes hipótesis:

1) La vinculación de entidades funcionales, como se definen en [UIT-T Y.2012], con un elemento de red determinado variará, dependiendo del vendedor.

2) Los proveedores de las NGN tienen responsabilidades específicas dentro de su dominio en lo que respecta a seguridad. Por ejemplo, han de aplicar los servicios y prácticas de seguridad adaptados para:

   a) protegerse a sí mismos;

   b) garantizar que la seguridad de extremo a extremo no está comprometida dentro de su red; y

   c) garantizar una gran disponibilidad de las comunicaciones NGN.

3) Cada dominio de red establecerá y aplicará políticas para que los acuerdos de nivel de servicio (SLA) garanticen la seguridad de su dominio y de las interconexiones de red. Se supone que en los SLA se especificarán servicios, mecanismos y prácticas de seguridad que habrán de aplicarse para proteger las redes interconectadas y las comunicaciones (tráfico de señalización/control, tráfico de portador y tráfico de gestión) a través de las UNI, ANI y NNI.

4) Esta Recomendación trata de la seguridad en la red, cuya estructura está organizada en capas, que consiste en la seguridad del perímetro con respecto a los dominios fiables, la seguridad física del equipo del proveedor y la posible utilización de la encriptación.

1.3 Resumen

La presente Recomendación se organiza de la siguiente manera:

- Cláusula 2 (Referencias) – En esta cláusula se presentan las referencias normativas.
- Cláusula 3 (Definiciones y abreviaturas) – En esta cláusula se presentan las definiciones y abreviaturas que se utilizan en esta Recomendación.
- Cláusula 4 (Amenazas y riesgos contra la seguridad) – En esta cláusula se subrayan las amenazas y riesgos contra la seguridad que se suponen en el entorno de las NGN. Estas amenazas y riesgos se utilizan como guía para elaborar los requisitos de seguridad e identificar las capacidades y procedimientos de seguridad que han de soportarse.
- Cláusula 5 (Modelo de seguridad) – En esta cláusula se describe un modelo de confianza para la seguridad en las NGN. Éste puede utilizarse para elaborar relaciones de confianza entre las UNI, ANI y NNI y diseñar la arquitectura de seguridad.
- Cláusula 6 (Arquitectura de seguridad) – En esta cláusula se describe la relación entre la arquitectura NGN funcional definida en [UIT-T Y.2012] y las arquitecturas de seguridad compuestas.
- Cláusula 7 (Objetivos y requisitos) – En esta cláusula se describen los objetivos y requisitos generales de seguridad para las NGN que se utilizarán como base para definir los requisitos de seguridad de las mismas.
- Cláusula 8 (Requisitos específicos de seguridad) – En esta cláusula se presentan los requisitos específicos de seguridad que se definen en la cláusula 7.
- Apéndice I – Objetivos y requisitos de seguridad para la interconexión de implementaciones nacionales de los servicios de telecomunicaciones de emergencia.
- Bibliografía.

Esta Recomendación está definida para servir de base a la seguridad de las NGN. En el futuro se presentarán otras Recomendaciones relacionadas para las distintas esferas de seguridad específicas, por ejemplo, autenticación y autorización, gestión de certificados, gestión de identidad, etc.

2 Referencias

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

[UIT-T M.3016.0] Recomendación UIT-T M.3016.0 (2005), *Seguridad en el plano de gestión: Visión general*.

[UIT-T M.3016.1] Recomendación UIT-T M.3016.1 (2005), *Seguridad en el plano de gestión: Requisitos de seguridad*.

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

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

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.

[UIT-T Y.2201] Recomendación UIT-T Y.2201 (2007), *Requisitos de las redes de la próxima generación, versión 1*.

3 Definiciones y abreviaturas

3.1 Términos definidos en otros sitios

En esta Recomendación se utilizan los siguientes términos definidos en otros sitios:

3.1.1 servicio de telecomunicaciones de emergencia (ETS): Servicio nacional que proporciona telecomunicaciones prioritarias autorizadas para facilitar las tareas del personal de emergencia en situaciones de catástrofe. (Véase la Rec. UIT-T E.107).

3.1.2 usuario: Un usuario incluye usuario final (Rec. UIT-T Y.2091), persona, abonado, sistema, equipo, terminal (por ejemplo, fax, computadora personal), entidad (funcional), proceso, aplicación, proveedor o red institucional.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se utilizan los siguientes términos:

3.2.1 activo: Cualquier elemento de valor para la organización, sus actividades económicas, funcionamiento y continuidad.

3.2.2 elemento frontera: Elemento de red cuya función consiste en la conexión de diversos dominios de seguridad y administrativos.

3.2.3 red institucional: Red privada que admite numerosos usuarios y que puede estar situada en diversos lugares (por ejemplo, una empresa, una ciudad universitaria).

3.2.4 elemento frontera de dominio: Elemento frontera bajo control exclusivo del proveedor que proporciona funciones de seguridad con otros dominios de red.

3.2.5 elemento frontera de red: Elemento frontera bajo control exclusivo del proveedor de servicios que proporciona funciones de seguridad con equipos terminales.

3.2.6 dominio de seguridad: Conjunto de elementos, política de seguridad, autoridad de seguridad y conjunto de actividades relativas a la seguridad donde los elementos se gestionan de conformidad con la política de seguridad. La política estará administrada por la autoridad de seguridad. Un dominio de seguridad determinado puede abarcar múltiples zonas de seguridad.

3.2.7 zona de seguridad: En esta Recomendación se definen 3 zonas de seguridad:

1) fiable;

2) fiable pero vulnerable; y

3) no fiable.

Una zona de seguridad está definida por el control operativo, la ubicación y la conectividad con otros elementos de red/dispositivos.

3.2.8 elemento frontera de equipo terminal: Elemento frontera que proporciona funciones de seguridad entre el equipo en los locales del cliente y la red del proveedor de servicios.

3.2.9 confianza: Se dice que la entidad X confía en la entidad Y para la realización de un conjunto de actividades única y exclusivamente si la entidad X confía en que la entidad Y se va a comportar de una manera concreta con respecto a dichas actividades.

3.2.10 zona fiable pero vulnerable: Desde el punto de vista de un proveedor de NGN, zona de seguridad donde el proveedor de las NGN explota los elementos/dispositivos de red (configuración y mantenimiento). El equipo puede estar bajo control del cliente/abonado o del proveedor de la NGN. Además, el equipo puede estar ubicado dentro o fuera del dominio del proveedor de la NGN. La comunicación se establece con elementos tanto de la zona fiable como con elementos de la zona no fiable, por lo que se considera "vulnerable". La principal función de seguridad consiste en proteger los elementos de red de la zona fiable de los ataques de seguridad cuyo origen se encuentra en la zona no fiable de manera infalible.

3.2.11 zona fiable: Desde el punto de vista de un proveedor de NGN, dominio de seguridad donde se encuentran los elementos y sistemas de la red del proveedor de la NGN que nunca comunican directamente con los equipos del cliente. Las características comunes de los elementos de la red NGN en este dominio que están bajo control del proveedor de las NGN correspondiente, están ubicadas en los locales de dicho proveedor (lo que proporciona seguridad física), y establecen comunicación únicamente con elementos del dominio "fiable" y con elementos del dominio "fiable pero vulnerable".

3.2.12 zona no fiable: Desde el punto de vista de un proveedor de NGN, zona que incluye todos los elementos de red de las redes de cliente o, posiblemente, redes pares u otras zonas del proveedor fuera del dominio original, conectados a los elementos frontera del proveedor de NGN.

3.2.13 red de usuario: Red privada constituida por un equipo terminal que puede tener numerosos usuarios.

3.3 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos.

3G	3ª generación (*3rd generation*)
AGW	Pasarela de acceso (*access gateway)*
ANI	Interfaz aplicación-red (*application-to-network interface*)
B2BUA	Agente de usuario adosado (*back-to-back user agent*)
BE	Elemento frontera (*border element*)
CSC-FE	Entidad funcional de control de sesión de llamada (*call session control functional entity*)
DBE	Elemento frontera de dominio (*domain border element*)
DNS	Sistema de nombre de dominio *(domain name system*)
ETS	Servicio de telecomunicaciones de emergencia (*emergency telecommunications service*)
FE	Entidad funcional (*functional entity*)
GW	Pasarela (*gateway*)
I-CSC-FE	Entidad funcional de control de sesión de llamada interrogante (*interrogating call session control functional entity*)
IMS	Subsistema de multimedios IP (*IP multimedia subsystem*)
IP	Protocolo Internet (*Internet protocol*)
LAN	Red de área local (*local area network*)
MPLS	Conmutación para etiquetas multiprotocolo (*multi protocol label switching*)
MRP-FE	Entidad funcional de procesamiento de recurso de medios (*media resource processing functional entity*)
NAC-FE	Entidad funcional de control de acceso de red (*network access control functional entity*)
NAPT	Traducción de direcciones de red y puertos (*network address and port translation*)
NAT	Traducción de direcciones de red (*network address translation*)
NBE	Elemento frontera de red (*network border element*)
NE	Elemento de red (*network element*)
NGN	Red de próxima generación (*next generation network*)
NNI	Interfaz red-red (*network-to-network interface*)
OAMP	Operaciones, administración, mantenimiento y configuración (*operations, administration, maintenance and provisioning*)
P-CSC-FE	Entidad funcional de control de sesión de llamada intermediaria (*proxy call session control functional entity*)
POTS	Telefonía tradicional (*plain old telephone service*)
QoS	Calidad de servicio (*quality of service*)
RTPC	Red telefónica pública conmutada

RAC-FE Entidad funcional de control de recursos y admisión (*resource and admission control functional entity*)

RAN Red de acceso radioeléctrico (*radio access network*)

RDSI Red digital de servicios integrados

RTSP Protocolo de trenes en tiempo real (*real time streaming protocol*)

SAA-FE Entidad funcional de autenticación y autorización de servicio (*service authentication and authorization functional entity*)

S-CSC-FE Entidad funcional de control de sesión de llamada servidora (*serving call session control functional entity*)

SIM Módulo de entidad de abonado (*subscriber identity module*)

SIP Protocolo de inicio de sesión (*session initiation protocol*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SL-FE Entidad funcional de localizador de suscripción (*subscription locator functional entity*)

TAA-FE Entidad funcional de autenticación y autorización de transporte (*transport authentication and authorization functional entity*)

TE Equipo terminal (*terminal equipment*)

TE-BE Elemento frontera de equipo terminal (*terminal equipment border element*)

TMN Red de gestión de las telecomunicaciones (*telecommunication management network*)

UA Agente de usuario (*user agent*)

UICC Tarjeta de circuito integrado universal (*universal integrated circuit card*)

UNI Interfaz usuario-red (*user-to-network interface*)

VLAN LAN virtual (*virtual LAN*)

W-CDMA Acceso múltiple por división de código de banda ancha (*wideband code division multiple access*)

WLAN LAN inalámbrica (*wireless LAN*)

xDSL Línea de abonado digital x (*x digital subscriber line*)

4 Amenazas y riesgos contra la seguridad

En esta Recomendación se supone que los sistemas, componentes, interfaces, información, recursos, comunicaciones (es decir, tráfico de señalización, gestión y datos/portador), servicios que conforman las NGN estarán expuestos a diversas amenazas y riesgos en materia de seguridad. Estas amenazas y riesgos dependen de diversos factores. Además, los usuarios extremos también se verán expuestos a determinadas amenazas (por ejemplo, acceso no autorizado a información privada).

Las amenazas a las NGN son las siguientes:

- reconocimiento no autorizado, por ejemplo, análisis a distancia del sistema para determinar puntos débiles (entre ellos, exploración, barrido, interrogación al puerto, cuadro de rutas, etc.);
- interrupción/apropiación del dispositivo que da lugar a la pérdida de control del mismo y a anomalías y errores en las auditorías de configuración;

- destrucción de información y/o otros recursos;
- corrupción o modificación de información;
- robo, eliminación o pérdida de información y/o otros recursos;
- divulgación de información; e
- interrupción y negación del servicio.

Además, resulta evidente que las NGN funcionarán en un entorno distinto del entorno RTPC, por lo que podrán estar expuestas a distintos tipos de amenazas y ataques internos y externos. Las NGN tendrán conexión directa o indirecta con redes fiables y no fiables y equipos terminales, quedando así expuestas a riesgos y amenazas contra la seguridad relacionados con la conexión a redes y equipos en los locales del cliente no seguros. Por ejemplo, la NGN de un proveedor puede estar conectada directa o indirectamente (es decir, a través de otra red) a los siguientes elementos, como se muestra en la figura 2:

- otros proveedores de servicio y sus aplicaciones;
- otras NGN;
- otras redes IP;
- red telefónica pública conmutada (RTPC);
- redes institucionales;
- redes de usuarios;
- equipos terminales;
- otros dominios de transporte NGN.

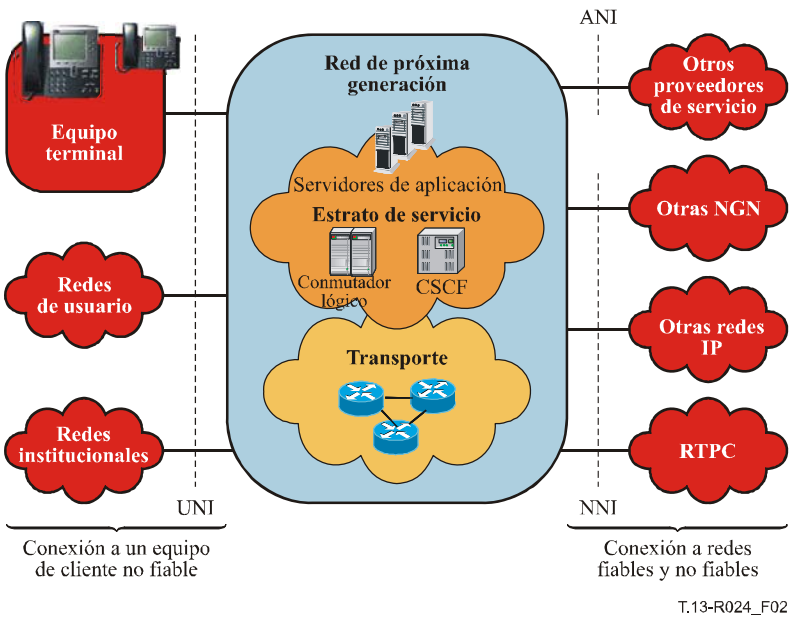

Figura 2 – Conexión con redes y usuarios

En un entorno evolutivo, la seguridad a través de múltiples dominios de proveedores de red depende de la combinación que los proveedores deciden hacer para proteger sus redes. El acceso no autorizado a la red de un proveedor puede fácilmente llevar a la explotación de una red interconectada y sus correspondientes servicios. Se trata esto de un ejemplo de explotación del enlace más débil que puede amenazar a la integridad y la continuidad del servicio de la red del proveedor además de una gran diversidad de ataques.

Cada proveedor de NGN es responsable de la seguridad dentro de su dominio. Cada proveedor de NGN es responsable de diseñar y aplicar soluciones de seguridad utilizando políticas de red específicas para las relaciones de confianza (cláusula 5) para colmar sus propias necesidades y contribuir a la consecución de los objetivos de seguridad de extremo a extremo globales a través de múltiples dominios de proveedores de red.

5 Modelo de confianza de seguridad

En esta cláusula se define el modelo de confianza de seguridad de las NGN.

La arquitectura funcional de referencia de las NGN define entidades funcionales (FE). No obstante, dado que los aspectos de la seguridad de la red dependen en gran medida en la manera en que estas FE están agrupadas, la arquitectura de seguridad de la NGN se basa en los elementos de red físicos (NE), es decir, cajas tangibles que contienen uno o más FE. La manera en que estas FE están agrupadas en las NE variará dependiendo del vendedor.

5.1 Modelo de confianza de una sola red

En esta subcláusula se definen tres zonas de seguridad:

1) fiable,

2) fiable pero vulnerable,

3) no fiable,

que dependen del control operativo, la ubicación y la conexión a otros elementos de red/dispositivos. Esas tres zonas se muestran en el modelo de confianza de seguridad de la figura 3.

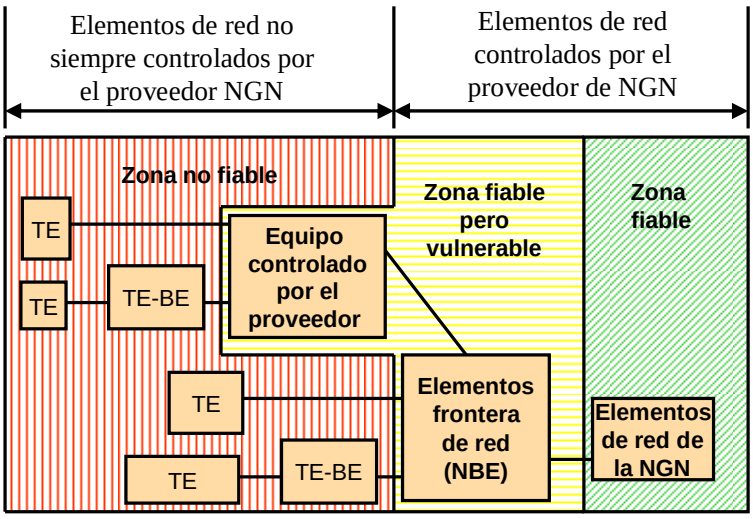

Figura 3 – Modelo de confianza en la seguridad

Una "zona de seguridad fiable en la red" o "zona fiable" es la zona donde se encuentran los sistemas y elementos de red del proveedor de NGN que nunca comunican directamente con los equipos de cliente u otros dominios. Las características comunes de los elementos de la NGN de esta zona es que están bajo control del proveedor de NGN, se encuentran en el dominio del proveedor de NGN, y comunican únicamente con elementos de la zona "fiable" y con elementos de la zona "fiable pero vulnerable". No se debería suponer que por ser fiable una zona es segura *per se*.

La zona "fiable" estará protegida por una combinación de diversos métodos. Pueden citarse como ejemplos la seguridad física de los elementos de red NGN, el refuerzo general de los sistemas, la utilización de la señalización segura, la seguridad para los mensajes OAMP de diversas VPN dentro de la red (MPLS/)IP para las comunicaciones dentro de la zona "fiable" y con los elementos de la NGN en la zona "fiable pero vulnerable". Pueden encontrarse más detalles al respecto en la cláusula 8.

Una "zona de seguridad fiable pero vulnerable en la red", o, en breve, "zona fiable pero vulnerable", es la zona donde el proveedor de NGN trabaja (configuración y mantenimiento) con los elementos/dispositivos de red. Los equipos pueden estar bajo control del cliente/abonado o del proveedor de NGN. Además, el equipo puede encontrarse dentro o fuera de los locales del proveedor de NGN y comunicar con elementos tanto de la zona fiable como con elementos de la zona no fiable, por lo que se considera que son "vulnerables". La principal función de seguridad consiste en proteger los NE de la zona fiable de los ataques a la seguridad originados en la zona no fiable.

Los elementos ubicados en el dominio del proveedor de NGN que tienen conexión con elementos de fuera de la zona fiable se consideran elementos frontera de red (NBE). Pueden citarse como ejemplos de elementos frontera los siguientes:

- Elementos frontera de red (NBE) en la UNI, que interactúan con los elementos de transporte o control de servicio del proveedor de NGN en la zona fiable para proporcionar acceso a los usuarios/abonados a la red de proveedor de NGN para servicios y/o transporte.
- Elemento frontera de dominio (DBE), que es el mismo tipo de equipo con elemento frontera de red a excepción de que reside en la frontera de los dominios.
- NBE de configuración y carga inicial de dispositivo (DCB-NBE) que está conectado con el sistema de configuración del dispositivo del proveedor de NGN en la zona fiable para configurar los dispositivos de los usuarios/abonados y los equipos del proveedor de NGN en la planta exterior.
- Los OAMP-NBE que están conectados con los sistemas OAMP del proveedor de NGN en la zona fiable para configurar y mantener los dispositivos de usuarios/clientes y los equipos del proveedor de NGN en la planta exterior.
- Los NBE de servidor de aplicación/servidor web (AS/WS-NBE) están conectados con los AS/WS-NBE del proveedor de NGN en la zona fiable para proporcionar acceso a usuarios/abonados a los servicios web.

A continuación se indican ejemplos de dispositivos/elementos explotados por el proveedor de NGN pero que no están ubicados en sus locales y que pueden estar o no bajo su control:

- equipo de la planta exterior en la red/tecnología de acceso;
- encaminadores opción base (BSR), un elemento de red que integra la estación base, el controlador de red radioeléctrica y las funcionalidades de encaminamiento;
- unidades ópticas (ONU) en los locales del usuario/abonado.

La zona "fiable pero vulnerable" comprende los NBE que se protegerán gracias a una combinación de diversos métodos, como por ejemplo, si la seguridad física de los elementos de la NGN, el refuerzo general de los sistemas, la utilización de señalización segura para todos los mensajes de señalización enviados a los elementos de la NGN en la zona "fiable", la seguridad de los mensajes OAMP y los filtros de paquetes y cortafuegos, según convenga. Pueden encontrarse más detalles al respecto en la cláusula 8.

Una "zona no fiable" incluye todos los elementos de red de las redes de cliente, o, posiblemente, redes pares u otros dominios del proveedor de NGN ubicados fuera del dominio original, que están conectados a elementos frontera de red del proveedor de NGN. El equipo terminal de la zona "no fiable" puede no estar bajo control del proveedor de NGN e incluso ser imposible obligar a los

usuarios a cumplir con la política de seguridad del proveedor. Aun así sigue siendo preferible intentar aplicar algunas medidas de seguridad y, con este fin, se recomienda asegurar la señalización, los medios y los OAM&P, y reforzar el TE-BE ubicado en la zona "no fiable". No obstante, debido a la falta de seguridad física, no se puede considerar que estas medidas sean absolutamente seguras. Pueden encontrarse más detalles al respecto en la cláusula 8.

5.2 Modelo de confianza de redes pares

Cuando una NGN está conectada a otra red, la confianza depende de los siguientes elementos:

- interconexión física, que puede ir desde la conexión directa en un edificio seguro hasta la conexión mediante instalaciones compartidas;
- modelo entre pares, en que el tráfico puede intercambiarse directamente entre dos proveedores de servicio de NGN a través de uno o más proveedores de transporte NGN;
- relaciones de empresa, donde puede encontrarse cláusulas de penalización en los acuerdos SLA y/o confiar en la política de seguridad del otro proveedor de NGN;
- en general, los proveedores de NGN deberían considerar no fiables a otros proveedores.

En la figura 4 se muestra un ejemplo de red conectada que se considera no fiable.

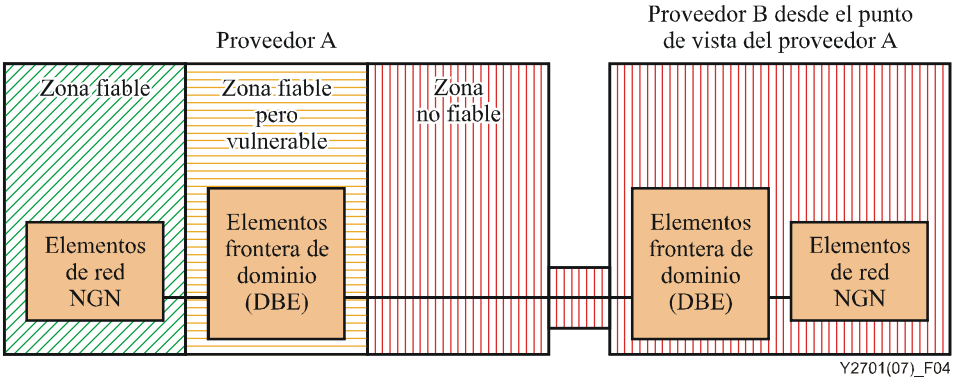

Figura 4 – Modelo de confianza entre pares

6 Arquitectura de seguridad

6.1 Arquitectura funcional de referencia de la NGN

La arquitectura NGN que se ajusta a [UIT-T Y.2201], *Requisitos de la versión 1 de la red de próxima generación*, se define en [UIT-T Y.2012], *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.

En la figura 5 se muestra un esquema funcional de la arquitectura NGN.

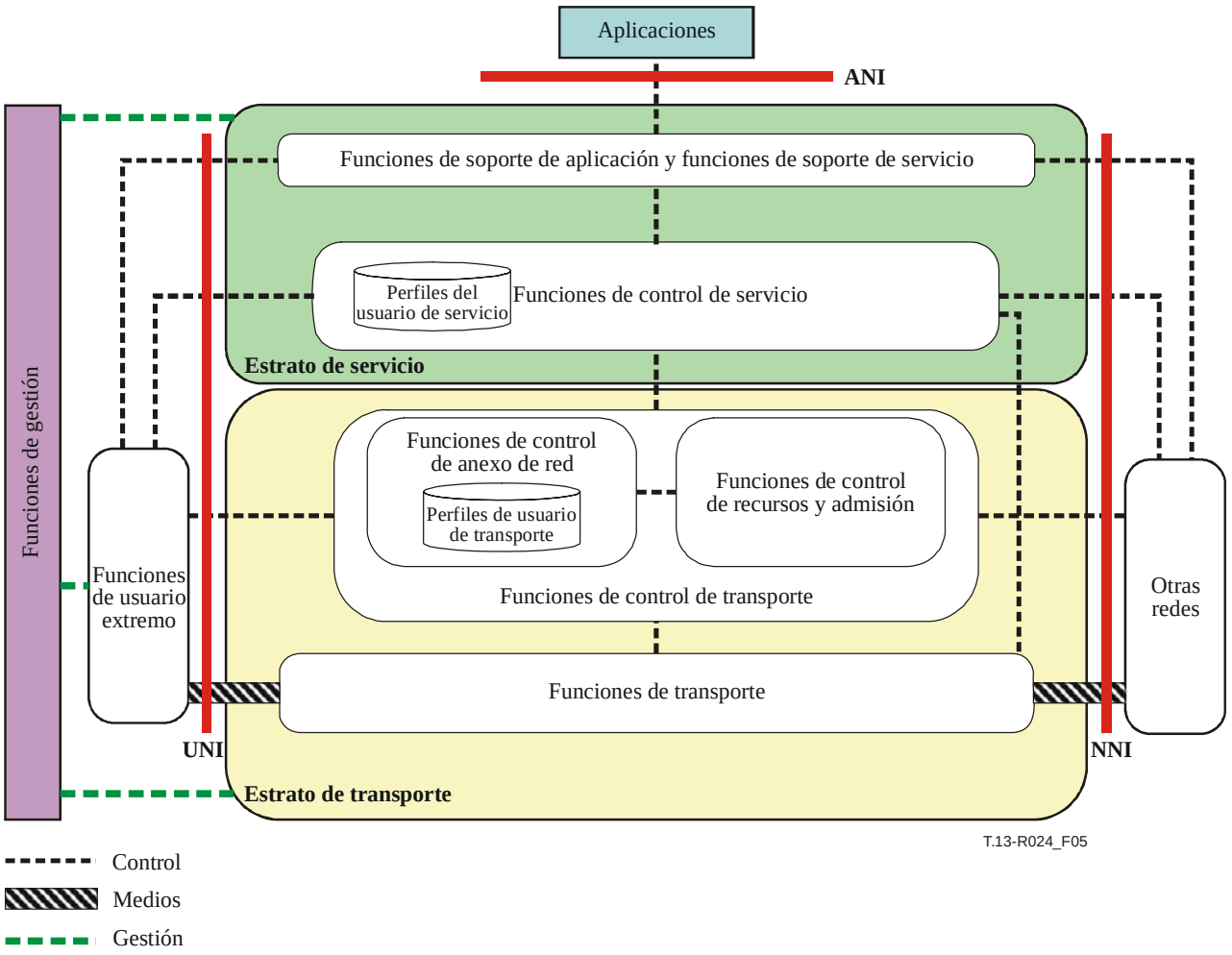

Figura 5 – Arquitectura general de la NGN (figura 1/Y.2012)

La NGN soporta un punto de referencia hacia las funciones de usuario extremo denominado interfaz usuario-red (UNI), y hacia otras redes, donde se denomina interfaz red-red (NNI). También soporta un punto de referencia hacia un grupo funcional de aplicaciones denominado interfaz aplicación-red (ANI), que permite la aplicación de capacidades NGN para crear y proporcionar aplicaciones para los usuarios de la NGN.

El estrato de transporte de la versión 1 de las NGN proporciona servicios de conexión IP a los usuarios de la NGN bajo el control de las funciones de control de transporte, incluidas las funciones de control de anexo de red (NACF) y las funciones de control de recursos y admisión (RACF).

El estrato de servicio proporciona servicios y aplicaciones a sus usuarios extremos utilizando las funciones de soporte de aplicación y las funciones de soporte de servicio y otras funciones de control relacionadas.

Las funciones de usuario extremo son aquellas conectadas a redes de acceso NGN y no se hacen aquí consideraciones sobre las diversas interfaces de usuario extremo y redes de usuario extremo.

Las funciones de gestión ofrecen la posibilidad de gestionar la NGN para proporcionar servicios con la calidad, seguridad y fiabilidad esperadas.

Pueden encontrarse más detalles al respecto en [UIT-T Y.2012].

6.2 Correspondencia con la arquitectura funcional NGN

En esta Recomendación se describe el método para lograr un nivel de seguridad utilizando el modelo de confianza que se muestra en la cláusula 5, es decir, una NGN compuesta por un dominio fiable (zona verde), un dominio no fiable (zona roja) y un dominio fiable pero vulnerable (zona amarilla) entre ambos.

Una de las cuestiones claves para lograr la seguridad con este modelo es el método de transmisión del tráfico de señalización, medios y OAMP del dominio no fiable al dominio fiable. Hay distintos métodos para lograrlo y el proveedor de NGN decide cuál de ellos considerar como su política. A continuación se presentan ejemplos de estos métodos.

a) Instalar NE para terminar el tráfico (B2BUA para señalizaciones SIP) entre la zona verde y la zona roja. Se recibe un paquete de la zona roja, se examina, se rechaza si no resulta adecuado y, si lo es, se copia la parte necesaria para reconstruir un paquete adecuado en la zona verde. En este caso, los NE donde termina el tráfico se convierten en los NE de la zona amarilla.

b) Se controla el tráfico en la capa intermedia (por ejemplo, abriendo y cerrando un puerto en concreto) (válvula) en el cortafuegos y se garantiza que únicamente los NE autorizados (y los usuarios) pueden enviar tráfico a los equipos de la zona verde. En este caso, los NE que controlan el tráfico se convierten en los NE de la zona amarilla.

c) Encriptación de extremo a extremo entre el emisor y el receptor.

En la arquitectura funcional que se muestra en [UIT-T Y.2012] (figura 6 de esta Recomendación), las señalizaciones SIP generada por la función de un usuario extremo (es generalmente no fiable puesto que el proveedor de las NGN no puede confirmar que la función no está falsificada) se transmite a S-2, P-CSC-FE. Por consiguiente, los NE que contienen P-CSC-FE se consideran los NE de la zona amarilla, o los NE de la zona verde debido a las funciones del cortafuegos. Si los NE que contienen S-1 (S-CSC-FE) están separados de los NE que contienen P-CSC-FE, se consideran como los NE de la zona verde.

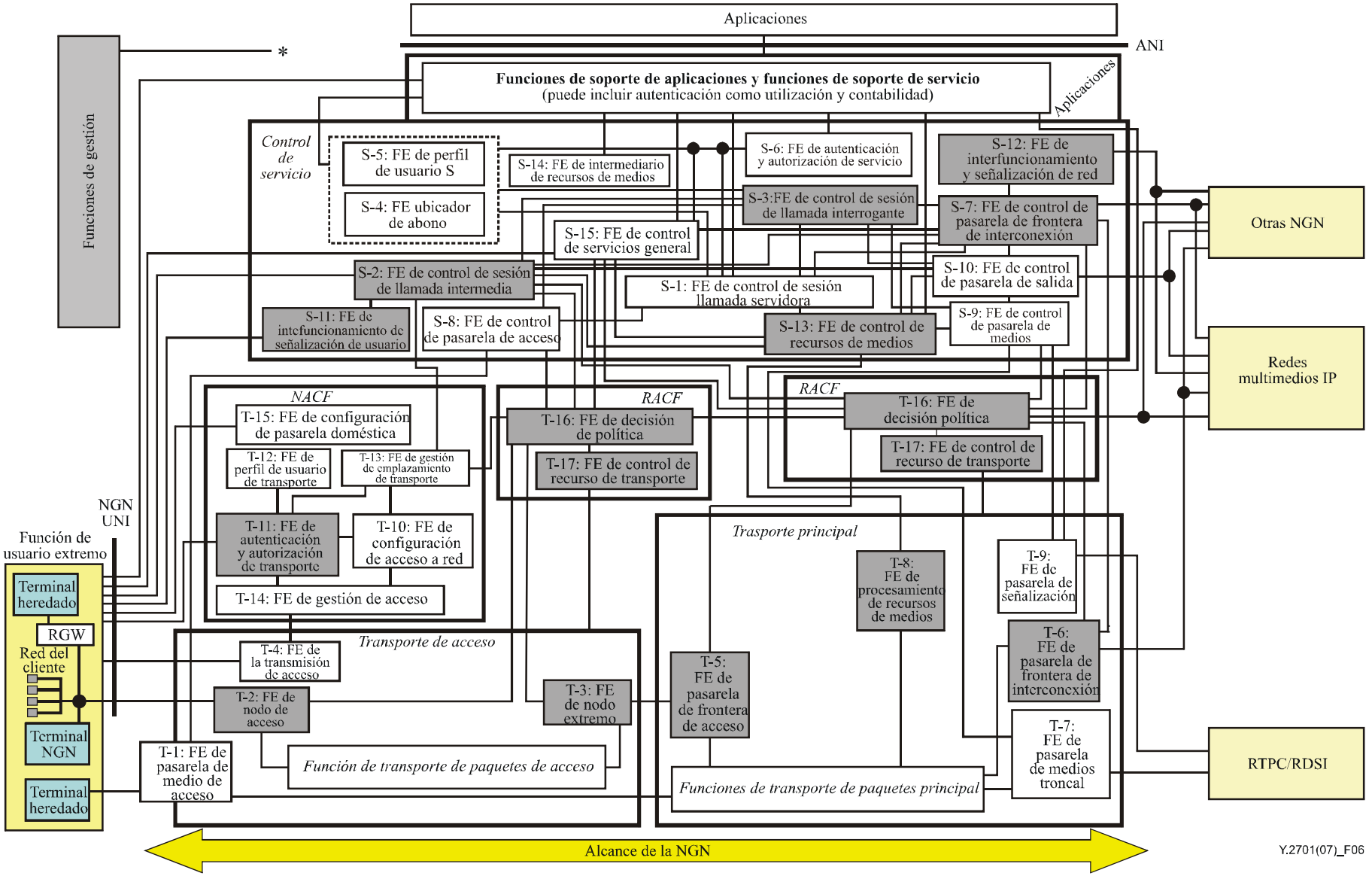

Figura 6 – Arquitectura funcional generalizada (figura 3/Y.2012)

6.3 Identificación de recursos NGN para protección de seguridad

Todos los proveedores de red deben identificar los activos como recursos con información interfaces de su red que han de protegerse así como las amenazas que han de contrarrestarse. Por ejemplo, los elementos de red, interfaces (UNI, ANI y NNI), sistemas de gestión y comunicaciones de señalización, gestión y medio/portador. Al identificar los recursos de NGN para protección de seguridad contra amenazas, ha de tenerse en cuenta la arquitectura por capas teórica definida en [UIT-T Y.2012] junto con la aplicación práctica de las entidades funcionales.

En los siguientes cuadros se presentan ejemplos de activos, recursos e interfaces de NGN para protección de seguridad contra amenazas, que se organizan de la siguiente manera:

- Cuadro 1 – Ejemplo de activos, recursos e información relacionados con la UNI.
- Cuadro 2 – Ejemplo de activos, recursos, información e interfaces del estrato de transporte.
- Cuadro 3 – Ejemplo de activos, recursos, información, interfaces del estrato de servicio.
- Cuadro 4 – Ejemplo de activos, recursos, información e interfaces de gestión.

Los ejemplos de los cuadros 1 a 4 no son exhaustivos.

Cuadro 1 – Ejemplo de activos, recursos e información relacionados con la UNI

Ejemplo	Objetivos y metas
Recursos de usuario extremo: • Dispositivos de usuario • Pasarelas de la red de usuario • Pasarelas de redes institucionales	a) Proteger el equipo de usuario extremo conectado a la red (por ejemplo, terminales, red de usuario y pasarelas de redes institucionales) contra los ataques originados en la red (por ejemplo, ataques para destruir, corromper y modificar el equipo de usuario). b) Proteger contra la interrupción de servicios (por ejemplo, ataques de denegación de servicio) y garantizar la disponibilidad del servicio. c) Proteger la red de acceso no autorizado (por ejemplo, usuarios y dispositivos de usuario no autorizados).
Información de usuario extremo: • Información de abono. • Información de identidad. • Información de ubicación.	a) Proteger contra la corrupción o modificación de la información. b) Proteger contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado a la información de ubicación).
Información de proveedor de NGN Información de identidad	a) Proteger contra la corrupción o modificación de la información. b) Proteger contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado a la información de ubicación).

Cuadro 1 – Ejemplo de activos, recursos e información relacionados con la UNI

Ejemplo	Objetivos y metas
Interfaces UNI	a) Estrato de transporte – Proporciona la protección de seguridad al tráfico de medios/portador que atraviese las interfaces UNI. b) Estrato de servicio (control de servicio) – Proporcionar protección de seguridad a la señalización y gestión en las interfaces UNI (por ejemplo, SIP, HTTP, RDSI y H.248). c) Estrato de servicio (soporte de aplicación y servicio) – Proporciona protección y seguridad a las funciones de control de aplicación de servicios en las interfaces UNI (por ejemplo, señalización en banda).

Cuadro 2 – Ejemplos de activos, recursos, información e interfaces del estrato de transporte

Ejemplos	Metas y Objetivos
Recursos del estrato de transporte: • Elementos de red de transporte (por ejemplo, encaminadores IP, nodos MPLS). • Enlaces de transmisión. • Información de encaminamiento (por ejemplo, servidores DNS). • Información del perfil de usuario de transporte (por ejemplo, bases de datos y almacén de datos de transporte).	a) Proteger todos los elementos, componentes y funciones de la red de transporte contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de la red de transporte. c) Proteger la disponibilidad de los elementos, componentes y funciones de la red de transporte. Protección contra la interrupción de los servicios (por ejemplo, contra ataques de denegación de servicio). d) Proteger contra la divulgación de cualquier tipo de información privada de usuario o red.
Comunicaciones internas del sistema en el estrato de transporte (comunicaciones dentro de la red de un proveedor de red).	a) Proporcionar protección de seguridad al tráfico de medios/portador entre sistemas dentro de una red de proveedor. b) Proporcionar protección de seguridad a la señalización y gestión del control de transporte (por ejemplo, OSPF) dentro de una red de proveedor. c) Proporcionar seguridad a la señalización entre sistemas en el estrato de servicio (por ejemplo, servidores de aplicación) y los sistemas en el estrato de transporte (por ejemplo, encaminadores IP).
Interfaces de transporte y comunicaciones.	a) Proporcionar protección de seguridad al tráfico de medios/portador en las interfaces UNI, NNI y ANI de transporte. b) Proporcionar protección de seguridad a la señalización del control de transporte (por ejemplo, OSPF) y gestión en las interfaces UNI, NNI y ANI.

Cuadro 3 – Ejemplos de activos, recursos, información e interfaces del estrato de servicio

	Ejemplos	Metas y objetivos
Estrato de servicio – Control de servicios	Estrato de servicios – Recursos o control de servicios. • Elementos de red de control de servicio (por ejemplo CSC-FE, SL-FE, MRP-FE, pasarelas, S/BC).	a) Proteger todos los elementos, componentes y funciones de red de control de servicio contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de red de control de servicio, incluida contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes y funciones de red de control de servicio. Proteger contra la interrupción de los servicios (por ejemplo, contra ataques de denegación de servicio).
	Estrato de servicio – Información de control de servicio. • Información de abonado (por ejemplo, bases de datos y depósito de datos que contienen los perfiles de usuario y los perfiles de servicio). • Información de proveedor de NGN (por ejemplo, bases de datos y depósito de datos que contiene la información de encaminamiento, numeración y direccionamiento).	a) Proteger contra la corrupción o modificación de datos e información. b) Proteger contra robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Proteger contra la divulgación (por ejemplo, acceso no autorizado e información privada de usuario y red).
	Estrato de servicio – Comunicación entre sistemas de control de servicio.	Proporcionar protección de seguridad en la señalización entre sistemas (por ejemplo SIP, RADIOS, Diameter) dentro de una red de un proveedor de red (por ejemplo, señalización CSCF a HSS).
	Interfaces y comunicaciones.	Proporcionar protección de seguridad a la señalización y gestión en las interfaces UNI, NNI y ANI.

Cuadro 3 – Ejemplos de activos, recursos, información e interfaces del estrato de servicio

	Ejemplos	Metas y objetivos
Estrato de servicio – Soporte de aplicaciones y servicios	Estratos de servicios – Recursos de soporte de aplicaciones y servicios: • Elementos y plataformas de red de soporte de aplicaciones y servicios (por ejemplo, servidores de aplicación, bases de datos, portales web).	a) Proteger todos los elementos, componentes y funciones de red de soporte de servicios contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes y funciones de red de soportes de servicios, incluido contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes y funciones de red de soporte de servicios. d) Protección contra la interrupción de los servicios (es decir, contra los ataques de denegación de servicio).
	Estrato de servicios – Información de soporte de aplicaciones y servicios: • Información de aplicaciones y servicios. • Información de abono.	a) Proteger contra la corrupción o modificación de datos e información. b) Protección contra el robo, eliminación o pérdida (por ejemplo, robo de identidad). c) Protección contra la divulgación (por ejemplo, acceso no autorizado a la información privada de usuario y red).
	Interfaces.	a) Proporcionar protección de seguridad a los elementos y recursos de red para cualquier tipo de acceso de proveedor de aplicación (por ejemplo, Parlay y pasarelas de Alianza Móvil Abierta). b) Proporcionar protección de seguridad a las interfaces UNI, NNI y ANI. c) Proporcionar protección de seguridad de la señalización y gestión del tráfico en las interfaces ANI.

Cuadro 4 – Ejemplo de activos, recursos, información interfaces de gestión

Ejemplo	Metas y objetivos
Recursos de gestión • Sistemas de gestión del estrato de transporte (por ejemplo, gestión de elementos de red, sistemas de gestión de red y de gestión de servicios). • Sistemas de gestión de estratos de servicios (por ejemplo, gestión de elementos de red, sistemas de gestión de red y de gestión de servicios).	a) Proteger todos los elementos, componentes, funciones e interfaces de red de gestión contra el acceso no autorizado. b) Proteger la integridad de los elementos, componentes, funciones interfaces de red de gestión, incluida la protección contra la corrupción o modificación de la información. c) Proteger la disponibilidad de los elementos, componentes, funciones interfaces de red de gestión. Protección contra la interrupción de los servicios (es decir, contra los ataques de denegación de servicio).

Cuadro 4 – Ejemplo de activos, recursos, información interfaces de gestión

Ejemplo	Metas y objetivos
Comunicaciones entre sistemas dentro de la red de un proveedor de red.	a) Proporciona protección de seguridad al tráfico de gestión entre sistemas de gestión dentro de una red (por ejemplo, estrato de servicios). b) Proporciona la protección de seguridad al tráfico de gestión entre la red del usuario y el estrato de transporte y el estrato de servicio de un proveedor de red.
Interfaces y comunicaciones entre sistemas.	a) Proporciona seguridad a las interfaces de gestión de red internas y cualquier interfaz de gestión UNI, NNI y ANI. b) Proporciona la protección de seguridad al tráfico de gestión en las interfaces UNI, ANI y NNI.

7 Objetivos y requisitos

7.1 Objetivos de seguridad generales

A continuación se presenta una lista de los objetivos de seguridad generales utilizados para determinar los requisitos de esta Recomendación.

- Las características de seguridad de las NGN deben ser extensibles y suficientemente flexibles para satisfacer distintos niveles de necesidad.
- Los requisitos de seguridad deben tener en cuenta la calidad de funcionamiento, la posibilidad de uso, la escalabilidad y las restricciones de costes de las NGN.
- Los métodos de seguridad deben basarse en normas de seguridad existentes y bien conocidas, según sea conveniente.
- La arquitectura de seguridad de las NGN debe ser globalmente escalable (dentro de los dominios de proveedor de red, a través de múltiples dominios de proveedor de red, en la configuración de seguridad).
- La arquitectura de seguridad de las NGN debe respetar las separaciones lógicas o físicas del tráfico de señalización y control, el tráfico de usuario y el tráfico de gestión.
- La seguridad de las NGN debe configurarse y gestionarse de manera segura.
- Las NGN deben proporcionar seguridad desde todos los puntos de vista: servicio, proveedor de red y abonado.
- Los métodos de seguridad no deben afectar normalmente a la calidad de los servicios proporcionados.
- La seguridad debe tener unas características de configuración y prestación simples y seguras para abonados y proveedores (plug & play).
- Deben mantenerse niveles de seguridad adecuados incluso cuando se utilice la funcionalidad de multidifusión.
- Las capacidades de descubrimiento de servicio deberán soportar diversos criterios (por ejemplo, ubicación, costos, etc.) para ser suficientemente escalables y disponer de los mecanismos adecuados para garantizar la seguridad y la privacidad.
- El sistema de resolución de dirección debe ser un sistema especial utilizado únicamente por esta red y se necesitarán determinadas medidas de seguridad. Este sistema puede utilizar bases de datos internas o externas de un dominio.

- Habrán de seguirse principios y objetivos de seguridad generales aplicables a la gestión de la RGT como se indica en la cláusula 7 de [UIT-T M.3016.0].

7.2 Objetivos para la seguridad a través de múltiples dominios de proveedores de red

El objetivo general es proporcionar seguridad de red a las comunicaciones de extremo a extremo a través de múltiples dominios de proveedor. Esto se consigue proporcionando seguridad a las comunicaciones de extremo a extremo salto por salto a través de distintos dominios de proveedor. En la figura 7 se muestra el concepto general de seguridad de red para las comunicaciones de extremo a extremo entre usuarios extremos. Cada segmento de la red tiene responsabilidades de seguridad específicas dentro de su zona de seguridad para facilitar la seguridad y disponibilidad de las comunicaciones NGN a través de múltiples redes.

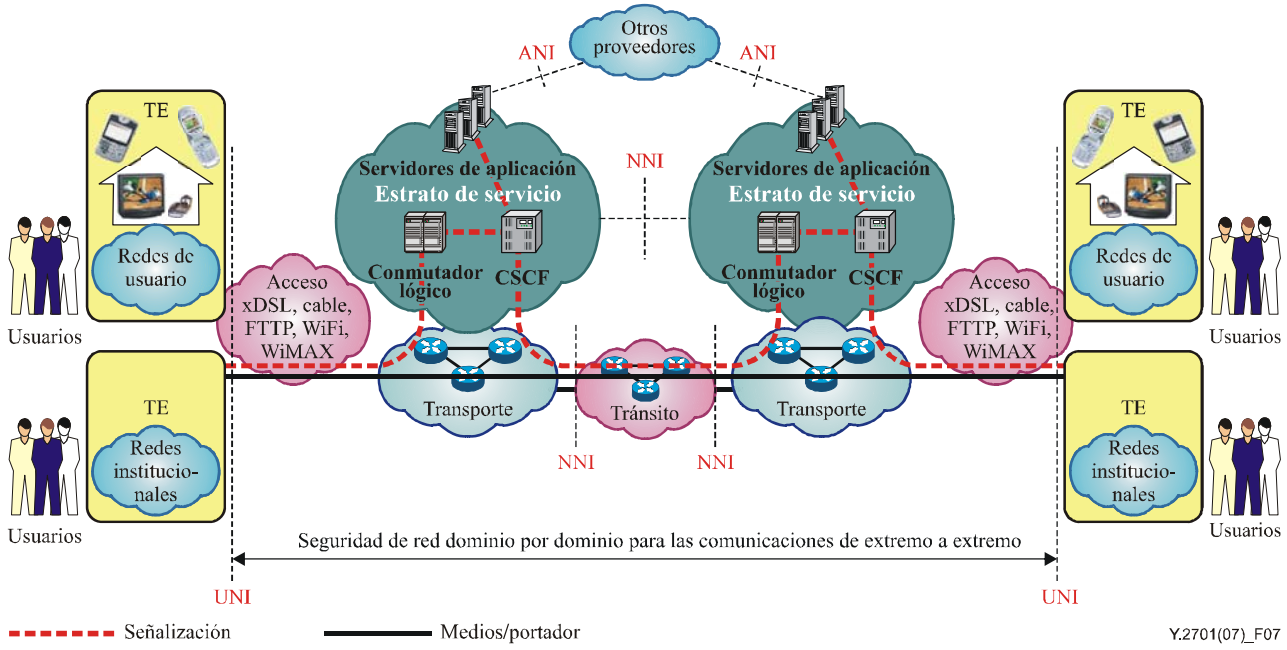

Figura 7 – Seguridad de las comunicaciones a través de múltiples redes

Como se indica en la cláusula 5.2, el modelo de confianza entre NGN interconectadas depende de diversos aspectos, por ejemplo las interconexiones físicas, los modelos entre pares y las relaciones de empresa.

7.3 Requisitos específicos para las dimensiones de seguridad

Los objetivos que aquí se indican son específicos a cada dimensión de seguridad en concreto, como la autenticación. Son comunes para todas las interfaces.

7.3.1 Control de acceso

Los proveedores de NGN deben restringir el acceso a abonados autorizados. El proveedor que facilita el acceso u otros proveedores pueden conceder la autorización una vez efectuada la validación mediante los procesos de autenticación y control de acceso.

Las NGN deben impedir el acceso no autorizado como, por ejemplo, el de intrusos que se hacen pasar por usuarios autorizados.

7.3.2 Autenticación

Los proveedores de NGN deben admitir capacidades destinadas a autenticar a los abonados, a los equipos, a los elementos de red y a otros proveedores, lo que incluye la admisión, aunque no únicamente, de lo siguiente:

1) Capacidades para autenticar a los usuarios para el acceso a la red de transporte (por ejemplo, autenticación y autorización de dispositivos de usuario extremo, pasarela de red de usuario o pasarela de red institucional para obtener acceso o conexión a la red de transporte).
2) Capacidades para autenticar a los usuarios para el acceso a servicios antes y durante la prestación del servicio (por ejemplo, autenticación de un usuario, un dispositivo o una combinación usuario/dispositivo cuando se aplica la autenticación al acceso a servicios/aplicaciones de la NGN).
3) Capacidades para que el usuario de una NGN autentique al proveedor de la NGN en cada estrato (por ejemplo, el usuario autentique la identidad del proveedor de la NGN conectada o el proveedor de servicios), si así lo requiere la política de seguridad.
4) Capacidades para permitir la autenticación par a par de usuario (por ejemplo, autenticación del usuario llamado, la entidad de origen, el origen de los datos) como servicios o características de la red.
5) Capacidades para permitir la autenticación bilateral entre dos proveedores de NGN en cada estrato para el intercambio de tráfico de señalización, gestión y medios/portador (por ejemplo, autenticación de redes remotas y directamente interconectadas a través de interfaces NNI).
6) Capacidades para permitir la autenticación de otros proveedores de servicios en las interfaces ANI. Han de soportarse los enfoques SIM y/o no SIM.

NOTA – La autenticación de una entidad no prevé indicar la validación positiva de una persona.

7.3.3 No repudio

Esta Recomendación no define ningún requisito de seguridad asociado al no repudio.

7.3.4 Confidencialidad de datos

Los proveedores de NGN deben proteger la confidencialidad del tráfico de abonado con medios criptográficos o de otro tipo.

Los proveedores de NGN deben proteger la confidencialidad de los mensajes de control con medios criptográficos o de otro tipo, si así lo requiere la política de seguridad.

Los proveedores de NGN deben proteger la confidencialidad del tráfico de gestión con medios criptográficos o de otro tipo.

7.3.5 Seguridad de la comunicación

Las NGN deben proporcionar mecanismos para garantizar que la información no se desvía o intercepta ilegalmente.

7.3.6 Integridad de datos

Los proveedores de NGN deben proteger la integridad del tráfico de abonado con medios criptográficos o de otro tipo.

Los proveedores de NGN deben proteger la integridad de los mensajes de control con medios criptográficos o de otro tipo, si así lo requiere la política de seguridad.

Los proveedores de NGN deben proteger la integridad del tráfico de gestión con medios criptográficos o de otro tipo.

7.3.7 Disponibilidad

Las NGN deberán proporcionar capacidades de seguridad para que los proveedores NGN puedan prevenir o cortar las comunicaciones con equipos de usuario extremo no conformes, por ejemplo, con miras a contrarrestar los ataques de denegación de servicio, la expansión de virus o gusanos, u otro tipo de ataques. Estas capacidades pueden dejarse en suspenso para permitir las telecomunicaciones de emergencia. También los elementos internos de la NGN pueden sufrir las consecuencias de virus, gusanos u otros ataques. Se deben aplicar medidas similares para poner en cuarentena los componentes de la red.

La NGN deberá contar con capacidades de seguridad para que un proveedor NGN pueda filtrar los paquetes y el tráfico considerados perjudiciales por la respectiva política de seguridad.

La NGN deberá proporcionar capacidades para soportar funciones y procedimientos de recuperación en caso de catástrofe. Los requisitos específicos a este respecto quedan fuera del alcance de esta Recomendación.

7.3.8 Privacidad

La NGN deberá proporcionar capacidades para proteger la información privada del abonado, tal como la ubicación de los datos, las identidades, los números de teléfono, las direcciones de red o los datos de contabilidad de llamadas conforme a la legislación y reglamentación nacionales. Los requisitos específicos que atañen a la privacidad son de ámbito nacional y quedan fuera del alcance de esta Recomendación.

8 Requisitos específicos de seguridad

En esta cláusula se tratan los requisitos específicos de seguridad de cada elemento de la red dentro de la infraestructura de la NGN. No obstante, dado que muchas necesidades de seguridad serán idénticas para distintos tipos de elementos de red, se especifican en primer lugar los requisitos de seguridad generales en la cláusula 8.1.

Los elementos frontera pueden integrarse o separarse, de conformidad con la infraestructura que se elija.

8.1 Requisitos de seguridad comunes para los elementos de las NGN

Estos requisitos se aplican a los elementos de las NGN de la zona fiable y la zona fiable pero vulnerable. Es de esperar que los dispositivos de la zona no fiable se ajusten a estos requisitos.

A continuación se presenta una lista de los requisitos de seguridad generales:

Los distintos elementos de las NGN deben soportar la interoperabilidad, en concreto entre los distintos mecanismos de seguridad NGN. En todo el mundo deben estar disponibles unas características de seguridad normalizadas mínimas.

La autenticación y autorización se ejercerán tanto en el estrato de servicio como en el estrato de transporte (usuario-red, red-usuario, red-red), lo que también debería ser posible en presencia de la NAPT transversal.

Los elementos de una NGN deberán proporcionar medidas de seguridad contra el acceso no autorizado a los recursos de red, los dispositivos, los servicios y los datos de abonado (perfil), por ejemplo, para bloquear el tráfico no autorizado.

La infraestructura de las NGN debe permitir que los proveedores limiten la visibilidad de la topología de red y los recursos a las entidades autorizadas.

La infraestructura de las NGN debe soportar múltiples zonas de seguridad. Es posible que se requiera el aislamiento en términos de seguridad de las distintas zonas de seguridad.

La infraestructura de las NGN garantizará la confidencialidad, así como la integridad de los flujos de señalización/control y de los flujos de gestión que transporta.

La infraestructura de las NGN debe garantizar la confidencialidad y la integridad de los flujos de medios que transporta.

Las NGN deberán asegurar cuidadosamente la seguridad de los elementos de red vinculados a recursos de gestión (OSS, base de datos, etc.) y recursos de servicio.

Los requisitos de seguridad para la gestión de la RGT segura deben seguir los definidos en la cláusula 10.1 de [UIT-T M.3016.0], detallados más a fondo en la cláusula 6 de [UIT-T M.3016.1].

Se aplicará una funcionalidad de seguridad en los elementos frontera de red (NBE o TE-BE, es decir, los NE en la zona fiable pero vulnerable), lo que incluye funciones tales como el control de acceso a los paquetes de datos y la información de señalización de acuerdo con las políticas especificadas, por ejemplo, denegación de tráfico a partir de aplicaciones a usuarios particulares.

Los elementos de la NGN sensibles, especialmente los elementos frontera de red, podrán aplicar una separación lógica y/o física de los trayectos de transporte de acuerdo con las políticas de seguridad vigentes, por ejemplo, la separación de los flujos de control y/o gestión de los flujos de medios utilizando interfaces distintas en el plano lógico o distintos planes de direccionamiento, y utilizando redes de transporte reales o virtuales distintas en el plano físico (virtuales como las RPV y VLAN).

Las NGN deberán almacenar de manera segura los datos relacionados con la seguridad (por ejemplo, identidad y credenciales). Este almacenamiento deberá ser distinto del depósito de datos general que contiene la información de abonados relacionado con los servicios. Las NGN dispondrán de una política de seguridad que incluya un conjunto de normas que determine qué tráfico ha de protegerse dependiendo de, por ejemplo, los contratos, el tipo de protección que se utiliza, la frecuencia de cambio de claves, y las reglas que determinan el cumplimiento de la seguridad de un dispositivo.

Las NGN deberán admitir la capacidad de supervisar el tráfico de la red y establecer los eventos básicos de la red que deberían considerarse normales.

Las NGN deberán estar en condiciones de detectar, informar y eliminar la aparición de eventos anormales en la red.

8.1.1 Política de seguridad

La política de seguridad es un conjunto de reglas establecidas por una autoridad de seguridad que rige el uso y la prestación de servicios e instalaciones de seguridad. Los proveedores de NGN prepararán una política de seguridad adecuada y serán responsables de su aplicación en todos los NE y dispositivos bajo su control.

8.1.2 Refuerzo e inhabilitación del servicio

Todos los elementos de las NGN deberán poder configurarse para soportar un mínimo de servicios necesarios para el soporte de la infraestructura NGN de los proveedores de NGN. Todo puerto de capa de transporte o de servicio que no se requiera para el funcionamiento correcto de un elemento de la NGN deberá inhabilitarse en todos los sistemas y elementos de la red. Además, las aplicaciones se ejecutarán con un mínimo de privilegios (por ejemplo, en las aplicaciones de plataforma UNIX/Linux no se ejecutarán como raíz, si no son indispensables en los privilegios de raíz). El sistema operativo de base (OS) que soporta cualquier elemento de la NGN deberá poder configurarse específicamente para proporcionar seguridad y reforzarse adecuadamente. No están autorizadas "puertas traseras" (acceso de software que pueda evitar cualquier mecanismo de control de acceso habitual) en los elementos de las NGN.

Además del refuerzo, deberán aplicarse controles de acceso físicos y lógicos para ajustarse a las prácticas idóneas de la industria.

8.1.3 Auditoría, interrogación y registro cronológico

Todos los elementos de las NGN deberán estar en condiciones de crear un rastro de auditoría que mantenga un registro de los eventos de seguridad, de acuerdo con la política de seguridad del proveedor de NGN. Tendrá que haber mecanismos para evitar cualquier modificación no autorizada o no detectada.

El rastro de auditoría deberá poder gestionarse y permitir el traslado de los datos en otros medios, por ejemplo, medios extraíbles, para su almacenamiento a largo plazo. Esta interfaz debe permitir a los administradores autorizados trasladar datos antiguos fuera del registro de auditoría e incorporarlos en medios extraíbles. Esta capacidad debe protegerse mediante una autorización específica para la gestión de la auditoría.

Pueden encontrarse más detalles relativos a la seguridad del registro cronológico y la auditoría en la cláusula 10.1.2.6.3 de [UIT-T M.3016.0] y las cláusulas 6.6 y 6.7 de [UIT-T M.3016.1].

8.1.4 Indicación de tiempo y fuente temporal

Todo elemento de la NGN soportará la utilización de una fuente de tiempo fiable tanto para el reloj del sistema como para la indicación de elementos de auditoría. Fuente temporal fiable en este caso significa una fuente temporal que puede verificarse como resistente a cualquier modificación no autorizada. Puede aceptarse una confianza transitoria, es decir, una fuente temporal que depende de una fuente temporal fiable es en sí misma una fuente temporal fiable aceptable.

8.1.5 Asignación de recursos y tratamiento de excepciones

Los elementos de la NGN tendrán la capacidad de limitar la cantidad de sus propios recursos importantes (por ejemplo, asignación de memoria), que asigna a las peticiones de servicio. Estos límites pueden minimizar los efectos negativos de los ataques de denegación de servicio. Los recursos utilizados para las peticiones de servicios entran en competencia con otras peticiones de utilización de recursos del sistema. Además, cada aplicación de NGN específica tendrá la capacidad de limitar su propia utilización de recursos importantes que asigna para satisfacer las peticiones.

El objetivo de este requisito es limitar los efectos de las ráfagas de actividad de manera que no afecten a otras peticiones de servicio. También permitirá/soportará la aplicación (y el OS) tengan la capacidad de señalar a los sistemas de vigilancia que la aplicación y/o su plataforma pueden estar sufriendo un ataque de denegación de servicio. Todo elemento de la NGN proporcionará una interfaz para supervisar la utilización de recursos.

Los elementos de la NGN descartarán de manera silenciosa cualquier paquete no conforme con el protocolo o formato esperados y, de acuerdo con la política de seguridad, serán capaces de generar una entrada en el registro cronológico para cada uno de estos eventos. El "descarte silencioso" consiste en interrogar y hacer un registro cronológico del paquete recibido y descartarlo sin responder con una indicación de descarte (por ejemplo, respuesta a error).

El objetivo de lo anterior es limitar los posibles ataques mediante paquetes maliciosos o incorrectos. Es decir, si la utilización de recursos de registro cronológico es tan grande que interfiere con el funcionamiento de otros elementos, la solución obvia es que el registro cronológico deje de funcionar hasta que la utilización de recursos vuelva a un nivel aceptable.

NOTA – Esto forma parte de los recursos internos de gestión que se mencionan anteriormente.

8.1.6 Integridad de código y sistema y de supervisión

Los elementos de red deberán poder supervisar 1) su configuración y software; y, 2) cualquier modificación para detectar cambios no autorizados, ambas basadas en la política de seguridad. Cualquier cambio no autorizado debe crear una entrada en el registro cronológico y generará una

alarma. De acuerdo con la política de seguridad, el elemento de red hará lo siguiente. El elemento será capaz de explorar periódicamente sus recursos y software para detectar el software malicioso, como por ejemplo un virus. Los elementos generarán una alarma si se descubre durante una exploración un software malicioso.

Es necesario controlar la supervisión para que no afecte el funcionamiento de las comunicaciones en tiempo real sensibles al retardo ni desactive innecesariamente las conexiones.

Pueden encontrarse otros requisitos de seguridad para la integridad del sistema en la cláusula 10.1.2.6.4 de [UIT-T M.3016.0].

8.1.7 Parches, "hotfixes" y códigos suplementarios

Para confiar en las señales generadas por los elementos de la NGN del proveedor de NGN dentro de redes no fiables como por ejemplo, un terminal, es indispensable que el software del sistema no se ponga en entredicho. Esto garantiza que no se telecargan en los elementos de la NGN o el OS subyacente "caballos de Troya[1]" (que llaman a casa),"gusanos" (que generan tráfico inútil o transforman el sistema en "zombies") y otro tipo de virus. Estos virus pueden poner en peligro la integridad del sistema, la confidencialidad y/o la disponibilidad de los datos.

Los elementos de red y sistemas del proveedor de NGN deben tener la capacidad de verificar y auditar todo su software. Los resultados de la auditoría tendrán que ser accesibles para cualquier OSS, lo que permite un análisis de la situación de seguridad de la infraestructura NGN del proveedor de NGN y orienta a los administradores y proveedores con respecto a las medidas que es necesario adoptar.

Deben obtenerse parches de seguridad de los vendedores de equipos e instalarlos de manera puntual una vez que el proveedor NGN los ha certificado.

En la cláusula I.5.2 de [UIT-T M.3016.1] pueden encontrarse más consideraciones sobre el proceso de parcheado, y en la cláusula I.5.3.9 de [UIT-T M.3016.1] sobre las premisas de seguridad del sistema operativo.

8.1.8 Acceso a las funciones OAMP en los dispositivos

Para salvaguardar la infraestructura OAMP, todo elemento de la NGN interno se gestionará mediante direcciones IP distintas asignadas a partir de bloques de direcciones distintos. Todos los elementos de la NGN internos deberán disponer de una interfaz separada física o lógicamente para uso exclusivo de este tráfico OAMP. Cuando se utilice esta interfaz aislada, el elemento de la NGN descartará de manera silenciosa todos los paquetes recibidos en la interfaz OAMP con direcciones fuente distintas de la dirección OAMP. Los elementos de la NGN descartarán de manera silenciosa todos los paquetes recibidos en una interfaz no OAMP cuya dirección de fuente estén asignadas al tráfico OAMP.

El acceso a las funciones OAMP podrá estar controlado mediante autenticación. Una vez que el usuario se haya autenticado entre un sistema, el elemento de la NGN interno rastreará todas las modificaciones que se aporten y ofrecerá la oportunidad de volver atrás.

Toda autorización relacionada con la seguridad se registrará cronológicamente en la auditoría. En concreto, todos los intentos de acceso, tengan o no éxito, a tal elemento se registrarán cronológicamente en la auditoría.

---

[1] Muchos caballos de Troya actúan como dispositivos de software de control remoto para el pirata que los envía. Cuando se instalan de manera segura en el sistema objetivo inician una conexión de vuelta al pirata para informarle de que ya están dispuestos para ser utilizados.

El tráfico OAMP debe protegerse de manera segura. Si este tráfico (incluido SNMP y NTP) atraviesa una red no fiable, habrá de estar seguramente protegido (por ejemplo, mediante IPSec o una MPLS, etc.).

8.2 Requisitos de los elementos de red NGN en la zona fiable

Se asignará una dirección IP del bloque reservado a los elementos de la NGN internos a los elementos de la versión 1 de la NGN de la zona "fiable". Toda la señalización utilizará esta dirección. También se asignará al elemento de la versión 1 de la NGN una dirección IP del bloque reservado para OAMP y todas las funciones OAMP utilizarán esta dirección.

Para preservar la confidencialidad e integridad de la comunicación de clientes deberá protegerse el tráfico de señalización y de medios, efectuando la encriptación del transporte o garantizando que el tráfico se cursa únicamente a través de un dominio protegido.

8.3 Requisitos de los elementos frontera de la NGN en el dominio "fiable pero vulnerable"

Los elementos frontera de red son la principal defensa contra ataques exteriores, es decir, ataques precedentes de dispositivos/elementos de red de la zona no fiable. Todo el tráfico de los elementos de red/dispositivos de la zona "no fiable" se envían en primer lugar a un elemento frontera de red, donde se validan antes de transmitirlos a su destino en el domino "fiable". Se utilizan las capacidades de separación física/lógica de las redes para prohibir al tráfico de un elemento de red/dispositivo de la zona no fiable a alcanzar cualquier elemento del dominio "fiable".

Los elementos frontera de red (NBE) son la principal defensa contra los ataques de señalización. Todo el tráfico de señalización procedente de un TE o un TE-BE en la zona no fiable se procesa en su NBE asignado, que lo retransmite a los equipos de red de la zona fiable. La capacidad de separar física/lógicamente las redes en el NBE se utiliza para prohibir a los TE/TE-BE de la zona no fiable que alcancen cualquier elemento de red de la zona fiable, excepto sus NBE asignados.

Como ocurre con la señalización, los elementos frontera de red (NBE) también son la principal defensa contra los ataques de medios. Todo el tráfico de medios procedente de un TE/TE-BE se procesa en el NBE y éste retransmite los medios. El NBE encamina paquetes de medios hacia su destino a través del dominio fiable únicamente si estos paquetes pueden asociarse con una sesión autorizada en curso. Los paquetes de medios no asociados con una petición de sesión no son válidos, no procede su curso y se descartan. Además, el NBE verifica la fuente del tren de medios y que la velocidad de paquetes es compatible con la sesión establecida. Los medios se transfieren dentro de las instalaciones del proveedor NGN a una pasarela RTPC (para una conexión RTPC) o a otro NBE. El segundo NBE procesa los medios y los retransmite al TE de destino.

NOTA – El término "sesión" alude a cualquier tipo de flujo de medios, independientemente de la convención utilizada para establecer la sesión.

El elemento frontera de red debe soportar múltiples direcciones IP o múltiples interfaces de red. Se asignará una dirección IP (dirección "interna") del bloque reservado a los elementos de la versión 1 de la NGN internos. Todo el tráfico de señalización y medios procedente y dirigido a otros elementos de la versión 1 de la NGN internos utilizarán esta dirección (o esta interfaz). Se asignará una dirección IP (dirección "externa") que debe ser accesible desde el equipo TE. Todo el tráfico de señalización y medios procedente o dirigido al TE utilizará esta dirección (o esta interfaz). Se asignará una dirección IP ("dirección OAMP") del bloque reservado a la función OAMP, que es accesible desde los servidores OAMP.

Para preservar la confidencialidad de la comunicación de cliente contra escuchas malintencionadas del tráfico de señalización, transporte de señalización de todos los mensajes de señalización se asegurarán en los elementos de red NGN de las zonas "fiable" o "fiable pero vulnerable". Todas las conexiones iniciadas por un NBE utilizado para transferir la información de señalización a estos

elementos NGN se establecerán utilizando canales seguros con autenticación. Todos los mensajes de señalización recibidos por un NBE en su dirección NGN "interna" a través de canales no seguros se descartarán silenciosamente.

Los trenes de medios deben protegerse efectuando la encriptación del transporte o garantizando que el tráfico se cursa únicamente a través de una red protegida. Además, la garantía de dirección de origen en el borde de la red garantizará que los paquetes procedentes del exterior no reclamen tener origen en el bloque de dirección NGN interno.

Los paquetes de medio recibidos por un NBE en su dirección externa se verificarán para una sesión activa (basada en un intercambio de señalización), para comprobar la dirección de fuente esperada (basada en la descripción de sesión que contiene el intercambio de señalización). El NBE descartará silenciosamente cualquier paquete de medio recibido que no corresponda con la sesión activa. El NBE verificará asimismo que la velocidad de paquetes es compatible con los parámetros de sesión negociados. El NBE puede verificar que el tamaño de los paquetes es compatible con la sesión establecida. Los paquetes de medio recibidos de una dirección IP fuente que no se considera originador de medios válido para este NBE se descartarán silenciosamente.

El NBE autenticará todas las peticiones, si así lo requiere el acuerdo de servicio establecido con el cliente. Cuando se recibe una petición a través de una conexión no encriptada, cada una de las peticiones deberá ser autenticada. Cuando la petición se reciba a través de una conexión encriptada creada sin autenticación de cliente, se autenticará la primera petición de dicha conexión. Cuando se recibe una petición a través de una conexión encriptada creada con autenticación, no es necesario aplicar más autenticaciones. Cabe señalar que las peticiones enviadas a través de un TE-BE no requerirán autenticación del dispositivo, ya que este elemento estará utilizando una conexión encriptada hacia el NBE. Si la petición procede de una dirección IP fuente que no se considera originador de peticiones válido para este NBE, la petición se descartará silenciosamente. También se descartan silenciosamente las peticiones de canal seguro procedentes de direcciones IP fuentes que no se consideran originadores de petición válidos para este NBE.

8.4 Requisitos para los elementos frontera TE en el dominio "no fiable"

La seguridad física es un problema para los equipos situados en los locales del cliente. En último término, debe aceptarse que, en gran medida, la seguridad de estos dispositivos depende del cliente. Dicho esto, cada dispositivo deberá adoptar precauciones razonables para contrarrestar ataques, peligros o injerencias. Para preservar la confidencialidad de la comunicación de cliente contra escuchas malintencionadas en el tráfico de señalización, los mensajes de señalización utilizarán una conexión de señalización segura entre el TE-BE y el NBE. El TE-BE puede ejercer la función de retransmisión de medios.

8.4.1 Funciones OAMP

Todas las funciones entre TE-BE y el proveedor de NGN se protegerán contra determinadas escuchas malintencionadas. Dado que la función OAMP puede existir en banda y fuera de banda, estas dos modalidades se tratan por separado.

8.5 Recomendaciones de seguridad para el equipo terminal en el dominio "no fiable"

Los equipos terminales (TE) generalmente están fuera del control del proveedor de NGN, por lo cual éste no deberá establecer requisitos en cuanto a características o políticas de seguridad, ya que esta función corresponde mejor a los diversos elementos frontera de red para adaptarse a las políticas que elija el cliente y proporcionar el mejor servicio en tales condiciones.

Las funcionalidades de seguridad reales de los elementos frontera de red del proveedor de NGN deben ser objeto de más estudio.

Ha de protegerse el tráfico de medios de las escuchas malintencionadas o la modificación.

Apéndice I

Objetivos de seguridad y directrices para la interconexión de servicios de telecomunicaciones de emergencia

(Este apéndice no es parte integrante de la presente Recomendación)

I.1 Antecedentes

El servicio de telecomunicaciones de emergencia (ETS) es un servicio nacional que proporciona servicios de telecomunicaciones prioritarias a los usuarios ETS autorizados en caso de catástrofes y emergencias. La aplicación del ETS es de ámbito nacional. No obstante, las catástrofes/emergencias pueden trascender las fronteras geográficas, por lo que es posible que los países/administraciones lleguen a acuerdos bilaterales y/o multilaterales para vincular sus respectivos sistemas ETS, lo que situaría al servicio de telecomunicaciones prioritarios (por ejemplo, voz, mensajería, vídeo y datos) que forman parte del ETS bajo el mandato de distintas redes nacionales en el marco de acuerdos bilaterales y/o multilaterales en caso de catástrofes y emergencias.

Los servicios de telecomunicaciones ETS entre distintas redes nacionales (es decir, países/administraciones) han de protegerse contra las amenazas en materia de seguridad. Para proporcionar seguridad de red a los servicios de telecomunicaciones ETS de extremo a extremo entre distintas redes nacionales (es decir, países/administraciones), se necesitan objetivos y requisitos de seguridad comunes. La seguridad y disponibilidad de los servicios de telecomunicaciones ETS dependerá de la seguridad de cada una de las redes participantes en la comunicación de extremo a extremo.

I.2 Alcance/propósito

En este apéndice se fijan objetivos y requisitos de seguridad comunes y se dan orientaciones para el soporte de la seguridad de red de los servicios de telecomunicaciones ETS en distintas redes nacionales (es decir, países/administraciones).

No se incluye en el alcance de este apéndice la función de seguridad par a par de usuario extremo cuando se utilicen funciones de seguridad del equipo del usuario extremo especiales. El alcance de este apéndice se limita a la seguridad de red de los servicios y telecomunicaciones ETS a través de múltiples redes con un enfoque salto a salto. No obstante, convendría que la NGN pudiera soportar de manera transparente estas funciones par a par.

Este apéndice no pretende imponer condiciones a los sistemas ETS nacionales. Su principal objetivo es proporcionar seguridad de red a los servicios de telecomunicaciones ETS (es decir, comunicaciones seguras prioritarias de voz, vídeo, datos y mensajería).

I.3 Objetivos generales

El objetivo general es que las redes puedan proporcionar seguridad a los servicios de telecomunicaciones ETS (es decir, comunicaciones seguras prioritarias de voz, vídeo, datos y mensajería) a través de distintas redes nacionales (es decir, países/administraciones) y proteger la disponibilidad del ETS. Esto conlleva a la seguridad de las comunicaciones de extremo a extremo que pueden atravesar diversos dominios de proveedor de red en redes nacionales e internacionales (es decir, países/administraciones) donde cada red es responsable de la seguridad dentro de su dominio.

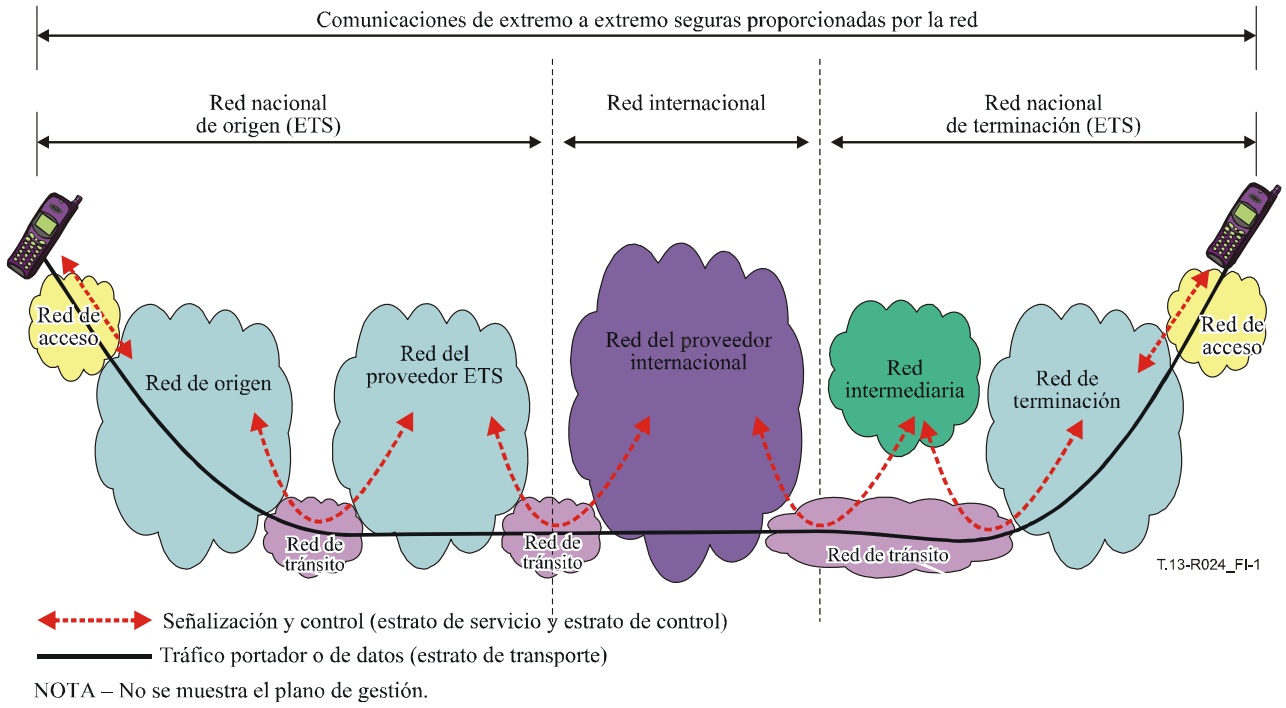

Figura I-1 – Ejemplo de comunicación de extremo a extremo a través de distintos sistemas ETS nacionales

En la figura I-1 se muestra un ejemplo del servicio de telecomunicaciones de extremo a extremo (por ejemplo, comunicación prioritaria de voz, vídeo, datos o mensajería) entre dos redes nacionales distintas. En este ejemplo se observa que la comunicación prioritaria de extremo a extremo del ETS puede involucrar múltiples segmentos de red y dominios administrativos (por ejemplo, red de acceso, red de origen, red de proveedor ETS, red de proveedor internacional, red intermediaria y red de terminación).

Cada segmento de red tendrá responsabilidades de seguridad específicas en el marco de su dominio para facilitar la seguridad y disponibilidad de extremo a extremo de los servicios de telecomunicaciones ETS.

A continuación se expone un conjunto mínimo de directrices generales y planificaciones de seguridad para proteger la señalización, el tráfico de portador y datos, y los datos de información relacionados con la gestión (por ejemplo, información del perfil de usuario) en el marco del ETS:

- Cada dominio de red establecerá y aplicará políticas de seguridad así como capacidades de soluciones de problemas para el ETS dentro de su dominio. Específicamente se recomienda que estas capacidades de soluciones de problemas y prácticas de seguridad que superen las de los servicios de aplicación general se identifiquen y apliquen para las comunicaciones prioritarias ETS. Por ejemplo, estas capacidades y prácticas se diseñarán para evitar el uso de recursos ETS por parte usuarios no autorizados y para evitar ataques de denegación de servicio y otro tipo.
- Cada dominio de red establecerá relaciones de confianza, métodos y procedimientos para identificar los servicios de telecomunicaciones ETS y para la gestión de identidad y de autenticación de usuarios extremos y redes en múltiples dominios administrativos de red. Por ejemplo, los acuerdos del nivel de servicio (SLA) establecerán una política de seguridad para la autenticación en cada dominio al entregar y recibir servicios de telecomunicaciones ETS.

- Cada dominio administrativo de red establecerá y aplicará políticas de seguridad para proteger los datos e información de gestión ETS (por ejemplo, información de perfil de usuario).

I.4 Capacidades de seguridad generales

Se recomienda que el ETS soporte las siguientes capacidades:

- Capacidades de seguridad para proteger los servicios de telecomunicaciones ETS de extremo a extremo a través de múltiples dominios de red.
- Capacidades de seguridad para proteger la disponibilidad de los servicios de telecomunicaciones ETS a través de múltiples dominios de red.
- Capacidades de seguridad para proporcionar gestión de la identidad y autenticación de los usuarios extremos y redes a través de múltiples dominios administrativos de red. Es preferible que el usuario interactúe con el servicio ETS únicamente cuando los mecanismos de seguridad han aceptado las credenciales del usuario extremo de un dominio administrativo a otro.

I.5 Autenticación, autorización y control de acceso

Se recomienda que el ETS soporte, como mínimo, las siguientes capacidades de autenticación, autorización y control de acceso:

- Capacidades de seguridad para proteger los mecanismos utilizados para autenticar y autorizar a los usuarios extremos y dispositivos ETS.
- Capacidades de seguridad para proteger los mecanismos utilizados para vincular a los usuarios extremos ETS con los dispositivos asociados.
- Capacidades de seguridad para proteger los mecanismos utilizados para compartir la información de autenticación (por ejemplo, confirmación de que un usuario extremo sea autenticado) a través de múltiples dominios de red.
- Capacidades de seguridad para proteger los mecanismos utilizados para la autenticación bilateral de usuarios extremos y entidades. Esto incluye los mecanismos para que un usuario ETS autentique a la parte llamada o a las entidades comunicantes (por ejemplo, sitio web, servidor de contenido, etc.).
- Capacidades de seguridad para proteger los mecanismos utilizados por una red para autenticar a otra. Esto incluye los mecanismos utilizados para autenticar la entrega por parte de la red de servicios de telecomunicaciones ETS (por ejemplo, red de origen) y para autenticar la red receptora de los servicios de telecomunicaciones ETS (por ejemplo, red intermedia o red de terminación).
- Capacidades de seguridad para proteger contra el acceso no autorizado a la información y los recursos ETS (por ejemplo, información de usuario en los servidores de autenticación y sistemas de gestión).

I.6 Confidencialidad y privacidad

Se recomienda soportar, como mínimo, las siguientes capacidades de confidencialidad:

- Capacidades de seguridad para proporcionar protección de confidencialidad a la señalización y control del ETS.
- Capacidades de seguridad para proporcionar protección de confidencialidad al tráfico portador y de datos ETS (por ejemplo, voz, vídeo de datos).
- Capacidades de seguridad para proporcionar protección y confidencialidad a los usuarios extremos ETS y las entidades comunicantes así como la información de abono.

- Capacidades de seguridad para proporcionar protección de confidencialidad a la ubicación del usuario extremo ETS.

Se recomienda soportar, como mínimo, las siguientes capacidades de privacidad:

- Capacidades de seguridad para proporcionar protección de privacidad a la información ETS (por ejemplo, información derivada de la observación de actividades de red, como sitios web que el usuario extremo ha visitado, la ubicación geográfica del usuario extremo y las direcciones IP y nombres DNS de los dispositivos en una red de proveedor de servicios).
- Capacidades de seguridad para proporcionar protección de privacidad contra la observación no autorizada de información de utilización ETS (por ejemplo, patrones de utilización como el volumen de tráfico ETS, las ubicaciones, el tiempo, la frecuencia, etc.).

I.7 Integridad de datos

Se recomienda soportar, como mínimo, las siguientes capacidades de integridad de datos:

- Mecanismos de seguridad para proporcionar protección de integridad a los servicios de telecomunicaciones ETS (por ejemplo, protección contra la modificación, eliminación, creación o reproducción no autorizada). Esto incluye los mecanismos para la notificación de información sobre manipulación o modificación.
- Mecanismos de seguridad para proporcionar protección de integridad a la información ETS (por ejemplo, marcas de prioridad, voz, datos y vídeo).
- Mecanismos de seguridad para proporcionar protección de integridad de los datos de configuración específicos de ETS (por ejemplo, información prioritaria almacenada en las funciones de decisión de políticas, el nivel de prioridad de usuarios, etc.)

I.8 Comunicación

Se recomienda soportar, como mínimo, las siguientes capacidades:

- Mecanismos de seguridad para proteger los servicios de telecomunicaciones ETS de un usuario extremo ETS autorizado contra las intrusiones (por ejemplo, mecanismos para prevenir la intercepción ilegal, el pirateo o la reproducción de tráfico de señalización o portador/datos ETS).

I.9 Disponibilidad

Se recomienda soportar, como mínimo, las siguientes capacidades:

- Mecanismos de seguridad para proteger la disponibilidad de los servicios de telecomunicaciones ETS (por ejemplo, protección del tráfico de señalización y control ETS y de portador/datos contra ataques de denegación de servicio o de otro tipo).
- Mecanismos de seguridad para proteger la disponibilidad de recursos específicos e información específicos de ETS (bases de datos de autenticación/autorización, información prioritaria almacenada en una función de decisión de política, recursos de red dedicados contra la denegación de servicio y otro tipo de ataques).

Bibliografía

Recomendaciones UIT-T

[b-UIT-T E.106] Recomendación UIT-T E.106 (2003), *Plan internacional de preferencias en situaciones de emergencia para actuaciones frente a desastres.*

[b-UIT-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de telecomunicaciones de emergencia (ETS) y marco de interconexión para implantaciones nacionales del ETS.*.

[b-UIT-T E.115] Recomendación UIT-T E.115 (2007), *Asistencia informatizada sobre directorios.*

[b-UIT-T M.3016.2] Recomendación UIT-T M.3016.2 (2005), *Seguridad en el plano de gestión: Servicios de seguridad.*

[b-UIT-T M.3016.3] Recomendación UIT-T M.3016.3 (2005), *Seguridad en el plano de gestión: Mecanismo de seguridad.*

[b-UIT-T M.3016.4] Recomendación UIT-T M.3016.4 (2005), *Seguridad en el plano de gestión: Formulario de características.*

[b-UIT-T M.3060] Recomendación UIT-T M.3060/Y.2401 (2006), *Principios para la gestión de redes de próxima generación.*

[b-UIT-T X.1121] Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

[b-UIT-T X.1122] Recomendación UIT-T X.1122 (2004*), Directrices para la implementación de sistemas móviles seguros basados en la infraestructura de claves públicas.*

[b-UIT-T Y.1271] Recomendación UIT-T Y.1271 (2004), *Requisitos y capacidades de red generales necesarios para soportar telecomunicaciones de emergencia en redes evolutivas con conmutación de circuitos y conmutación de paquetes.*

[b-UIT-T Y.2000-Sup.1] Suplemento 1 a las Recomendaciones de la serie Y.2000 (2006), *Alcance de la versión 1 de la red de próxima generación.*

[b-UIT-T Y.2111] Recomendación UIT-T Y.2111 (2006), *Funciones del control de recursos y de admisión en las redes de la próxima generación.*

Documentos ETSI TISPAN

[b-ETSI TR 187.002] ETSI TR 187 002 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis*.

[b-ETSI TS 187.001] ETSI TS 187 001 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements*.

[b-ETSI TS 187.003] ETSI TS 187 003 V.1.1.1 (2006), *Telecommunications and Internet converged services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture*.

Documentos ETSI/3GPP

[b-3GPP TS 33.102] 3GPP TS 33.102 (2007), *3G security; Security architecture*.

[b-3GPP TS 33.103] 3GPP TS 33.103 (2001), *3G security; Integration guidelines*.

[b-3GPP TS 33.110] 3GPP TS 33.110 (2007), *Key establishment between a UICC and a terminal*.

[b-3GPP TS 33.120] 3GPP TS 33.120 (2001), *Security Objectives and Principles*.

[b-3GPP TS 33.200] 3GPP TS 33.200 (2004), *3G security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-3GPP TS 33.203] 3GPP TS 33.203 (2007), *3G security; Access security for IP-based services*.

[b-3GPP TS 33.204] 3GPP TS 33.204 (2007), *3G security; Network Domain Security (NDS); TCAP user security*.

[b-3GPP TS 33.210] 3GPP TS 33.210 (2007), *3G security; Network Domain Security; IP network layer security*.

[b-3GPP TS 33.220] 3GPP TS 33.220 (2007), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-3GPP TS 33.310] 3GPP TS 33.310 (2007), *Network Domain Security (DNS; Authentication Framework (AF)*.

[b-3GPP TR 33.901] 3GPP TR 33.901 (2001), *Criteria for cryptographic algorithm design process*.

[b-3GPP TR 33.902] 3GPP TR 33.902 (2001), *Formal Analysis of the 3G Authentication Protocol*.

[b-3GPP TR 33.908] 3GPP TR 33.908 (2001), *3G Security; General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-3GPP TR 33.909] 3GPP TR 33.909 (2001), *3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-3GPP TR 33.918] 3GPP TR 33.918 (2007), *Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)*.

[b-3GPP TR 33.919] 3GPP TR 33.919 (2007), *3G Security; Generic Authentication Architecture (GAA); System description*.

[b-3GPP TR 33.920] 3GPP TR 33.920 (2007), *SIM card based Generic Bootstrapping Architecture (GBA); Early implementation feature*.

[b-3GPP TR 33.980] 3GPP TR 33.980 (2007), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)*.

[b-ETSI TR 133.901] ETSI TR 133.901 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security – Criteria for cryptographic Algorithm design process*.

[b-ETSI TR 133.902] ETSI TR 133.902 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); Formal Analysis of the 3G Authentication Protocol*.

[b-ETSI TR 133.908] ETSI TR 133.908 (2001), *Universal Mobile Telecommunications System (UMTS); Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms*.

[b-ETSI TR 133.909] ETSI TR 133.909 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions*.

[b-ETSI TR 133.919] ETSI TR 133.919 V6.2.0 (2005), *Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); System description*.

[b-ETSI TS 133.102] ETSI TS 133 102 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture*.

[b-ETSI TS 133.103] ETSI TS 133 103 V4.2.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines*.

[b-ETSI TS 133.120] ETSI TS 133 120 V4.0.0 (2001), *Universal Mobile Telecommunications System (UMTS); 3G Security; Security Principles and Objectives*.

[b-ETSI TS 133.200] ETSI TS 133 200 V6.1.0 (2005), *Universal Mobile Telecommunications System (UMTS); 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security*.

[b-ETSI TS 133.203] ETSI TS 133 203 V6.10.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services*.

[b-ETSI TS 133.210] ETSI TS 133 210 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS).*

[b-GPP TS 133.220] ETSI TS 133 220 V7.8.0 (2007), *Digital cellular telecommunications system; (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-ETSI TS 133.310] ETSI TS 133 310 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF)*.

Documentos ATIS/3GPP2

[b-GPP2 S.S0086] 3GPP2 S.S0086 (2004), *IMS Security Framework*.

RFC de IETF relacionados con IPsec

[b-IETF RFC 2085] IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay Prevention*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2709] IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains*.

[b-IETF RFC 2857] IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH*.

[b-IETF RFC 3526] IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE).*

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3664] IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*.

[b-IETF RFC 4109] IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1).*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[b-IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP).*

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).*

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).*

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[b-IETF RFC 4309] IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP).*

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use With IPsec*.

RFC de IETF relacionados con S/MIME

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification*.

[b-IETF RFC 2312] IETF RFC 2312 (1998), *S/MIME Version 2 Certificate Handling*.

[b-IETF RFC 3565] IETF RFC 3565 (2003), *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS).*

[b-IETF RFC 3657] IETF RFC 3657 (2004), *Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS).*

[b-IETF RFC 3850] IETF RFC 3850 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*.

[b-IETF RFC 3851] IETF RFC 3851 (2004), *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*.

[b-IETF RFC 3852] IETF RFC 3852 (2004), *Cryptographic Message Syntax*.

[b-IETF RFC 4134] IETF RFC 4134 (2005), *Examples of S/MIME Messages*.

RFC de IETF relacionados con TLS

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2817] IETF RFC 2817 (2000), *Upgrading to TLS Within HTTP/1.1*.

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.

[b-IETF RFC 3268] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

Otras RFC de IETF sobre seguridad

[b-IETF i-d.SIPUAP] IETF internet-draft work in progress, draft-ietf-sipping-config-framework-08.txt (March 6, 2006), *A Framework for Session Initiation Protocol User Agent Profile Delivery*.

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3715] IETF RFC 3715 (2004), *IPsec-Network Address Translation (NAT) Compatibility Requirements*.

[b-IETF RFC 3847] IETF RFC 3847 (2004), *Restart Signaling for Intermediate System to Intermediate System (IS-IS)*.

[b-IETF RFC 3948] IETF RFC 3948 (2005), *UDP Encapsulation of IPsec ESP Packets*.

RFC de IETF relacionados con DNS

[b-IETF RFC 4033] IETF RFC 4033 (2005), *DNS Security Introduction and Requirements*.

[b-IETF RFC 4034] IETF RFC 4034 (2005), *Resource Records for the DNS Security Extensions*.

[b-IETF RFC 4035] IETF RFC 4035 (2005), *Protocol Modifications for the DNS Security Extensions*.

Documentos de TIA

[b-TIA-683-D] TIA Standard TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

[b-TIA-1053] TIA Standard TIA-1053 (2005), *Broadcast/Multicast Security Framework*.

[b-TIA-1091] TIA Standard TIA-1091 (2006), *IMS Security Framework*.

Documentos de ARIB

[b-ARIB-SS0078] ARIB STD-T64 S.S0078-0 v1.0 (2002), *Common Security Algorithms*.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2008