Unión Internacional de Telecomunicaciones

# UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

# Y.2705

(03/2013)

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

Redes de la próxima generación – Seguridad

## Requisitos mínimos de seguridad para la interconexión del servicio de telecomunicaciones de emergencia (ETS)

Recomendación UIT-T Y.2705

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

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

| | |
|---|---|
| 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 |
| 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 |
| Televisión IP sobre redes de próxima generación | 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 |
| Redes basadas en paquetes | Y.2600–Y.2699 |
| **Seguridad** | **Y.2700–Y.2799** |
| Movilidad generalizada | Y.2800–Y.2899 |
| Entorno abierto con calidad de operador | Y.2900–Y.2999 |
| REDES FUTURAS | Y.3000–Y.3499 |
| COMPUTACIÓN EN LA NUBE | Y.3500–Y.3999 |

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

# Recomendación UIT-T Y.2705

## Requisitos mínimos de seguridad para la interconexión del servicio de telecomunicaciones de emergencia (ETS)


**Resumen**

El servicio de telecomunicaciones de emergencia (ETS) es un servicio nacional que da a los usuarios autorizados del ETS prioridad de acceso a los servicios de telecomunicaciones en caso de catástrofe y en situaciones de emergencia. En la Recomendación UIT-T Y.2705 se establecen los requisitos mínimos de seguridad para la interconexión entre redes del ETS. De este modo el ETS contará con la protección de seguridad necesaria entre redes nacionales, que hayan establecido acuerdos bilaterales y/o multilaterales, en caso de catástrofe y en situación de emergencia.



**Historia**

| Edición | Recomendación | Aprobación | Comisión de Estudio |
|---|---|---|---|
| 1.0 | ITU-T Y.2705 | 2013-03-01 | 13 |

**Palabras clave**

Capacidades y servicios prioritarios, seguridad de las NGN, servicio de telecomunicaciones de emergencia (ETS).

## 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 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

## Introducción

El servicio de telecomunicaciones de emergencia (ETS) es un servicio nacional que da a los usuarios autorizados de ETS prioridad de acceso a los servicios de comunicaciones en caso de catástrofe y en situaciones de emergencia. La implantación del ETS es responsabilidad de cada país. Sin embargo, las catástrofes/emergencias pueden traspasar las fronteras geográficas internacionales, por lo que es posible que los países/administraciones concluyan acuerdos bilaterales y/o multilaterales para vincular sus respectivos sistemas de ETS. De este modo los servicios de comunicaciones prioritarios (por ejemplo, voz, mensajería, vídeo y datos) pertenecientes al ETS podrían utilizar diferentes redes nacionales sujetas a acuerdos bilaterales y/o multilaterales en caso de catástrofe y en situación de emergencia.

La integridad, confidencialidad y disponibilidad del ETS entre redes nacionales interconectadas dependerán de la seguridad de cada red nacional participante en las comunicaciones de extremo a extremo. Para que la red asegure el ETS de extremo a extremo en distintas redes nacionales (es decir, países/administraciones) es necesario imponer unos requisitos de seguridad para la interconexión del ETS.

# Recomendación UIT-T Y.2705

## Requisitos mínimos de seguridad para la interconexión del servicio de telecomunicaciones de emergencia (ETS)

### 1 Alcance

En esta Recomendación se establecen los requisitos de seguridad mínimos para la interconexión entre redes del ETS. Los requisitos de seguridad comprenden la protección de la integridad, la confidencialidad y la disponibilidad de las comunicaciones ETS a través de las fronteras de red (es decir, en distintas redes nacionales).

El objetivo de esta Recomendación es establecer un conjunto de requisitos mínimos de seguridad que pueda utilizarse para facilitar el soporte del ETS en redes directa o indirectamente interconectadas.

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

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

[UIT-T M.3342] Recomendación UIT-T M.3342 (2006), *Directrices para la definición de plantillas de representación del SLA.*

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2010)**,** *Arquitectura y requisitos funcionales de las redes de próxima generación*.

[UIT-T Y.2205] Recomendación UIT-T Y.2205 (2011), *Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas.*

### 3 Definiciones

#### 3.1 Términos definidos en otros documentos

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

**3.1.1 autorización** [b-UIT-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

**3.1.2 disponibilidad** [b-UIT-T X.800]: Propiedad de ser accesible y utilizable sobre pedido por parte de una entidad autorizada.

**3.1.3 confidencialidad** [b-UIT-T X.800]: Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

**3.1.4 integridad de los datos** [b-UIT-T X.800]: Propiedad que garantiza que los datos no han sido alterados ni destruidos de una manera no autorizada.

**3.1.5 servicio de telecomunicaciones de emergencia (ETS, *emergency telecommunications service*)** [UIT-T E.107]: Servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios autorizados en situaciones de catástrofe y emergencia.

### 3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen el siguiente término:

**3.2.1 Proveedor de Servicio:** el Proveedor de Servicio (con mayúsculas) es un proveedor de servicios de telecomunicaciones públicas autorizado a prestar el ETS.

## 4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ANI Interfaz aplicación-red (*application network interface)*

CVE Vulnerabilidades y exposiciones comunes (*common vulnerabilities and exposures)*

CVE Vulnerabilidad y exposición comunes (*common vulnerability and exposure)*

CVSS Sistema de puntuación para las vulnerabilidades comunes (*common vulnerability scoring system*)

CWE Enumeración de debilidades comunes (*common weakness enumeration)*

CYBEX Intercambio de información de ciberseguridad (*cyber security information exchange)*

DDoS Denegación de servicio distribuida (*distributed denial of service)*

DNS Servidor de nombre de dominio (*domain name server)*

DoS Denegación de servicio (*denial of service)*

DSCP Punto de código Diffserv (*Diffserv code point)*

ETS Servicio de telecomunicaciones de emergencia (*emergency telecommunications service)*

IDS Sistema de detección de intrusiones (*intrusion detection system)*

IEPS Plan internacional de preferencias en situaciones de emergencia (*international emergency preference scheme)*

IP Protocolo Internet (*Internet protocol)*

IPS Sistema de prevención de intrusiones (*intrusion prevention system)*

IPsec Seguridad IP (*IP security)*

LAN Red de área local (*local area network)*

NE Elemento de red (*network element*)

NGN Red de la próxima generación (*next generation network)*

NNI Interfaz red-red (*network-network interface)*

IIP Información de identificación personal (*personally identifiable information)*

RTPC Red telefónica pública conmutada *(public switch telephone network)*

QoS Calidad de servicio (*quality of service)*

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

SNI Interfaz servicio-red (*service network interface)*

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

## 5 Convenios

En la presente Recomendación:

Se pone con mayúscula "Proveedor de Servicio" cuando este término se refiere a los "Proveedores de Servicios" de telecomunicaciones públicas autorizados a facilitar el ETS (véase 3.2.1).

La expresión "se exige" indica un requisito que debe cumplirse estrictamente, no permitiéndose desviación alguna si se pretende reclamar la conformidad con la presente Recomendación.

La expresión "se recomienda" indica un requisito recomendado pero que no se exige con carácter taxativo. Por ello no es necesario cumplir este requisito para reclamar la conformidad.

La expresión "se prohíbe" indica un requisito que debe cumplirse estrictamente, sin permitirse desviación alguna si se pretende reclamar la conformidad con la presente Recomendación.

La expresión "puede opcionalmente" indica un requisito opcional admisible que no reviste en absoluto el carácter de recomendación. Esta expresión no pretende dar a entender que la implementación del fabricante debe suministrar una opción o característica que puedan ser activadas opcionalmente por el operador de red o proveedor del servicio. Más bien significa que el fabricante puede proporcionar opcionalmente esta característica sin menoscabo de su derecho de reclamar la conformidad con la especificación.

En el cuerpo de la presente Recomendación y en sus anexos aparecen algunas veces verbos que expresan obligación, prohibición, recomendación y posibilidad, en cuyo caso deben interpretarse en dicho sentido. Cuando estas expresiones o términos aparecen en apéndices o en partes incluidas explícitamente a título informativo no deben interpretarse en su sentido normativo.

## 6 Amenazas y riesgos de seguridad

Las comunicaciones ETS pueden ser objeto de ataques de ciberseguridad dada su naturaleza crítica. Véase en [UIT-T E.107], [UIT-T Y.2205] y [b-UIT-T Sup57] la definición de ETS e información al respecto. Las amenazas o acciones malintencionadas de interrupción, utilización indebida, manipulación o daños de otro tipo al ETS pueden proceder de diversas fuentes, incluidas las redes interconectadas. Por ejemplo, pueden lanzarse ataques de ciberseguridad al ETS para:

- Interrumpir la capacidad de comunicación del personal participante en las operaciones de socorro.
- Obtener información sensible mediante escuchas ilícitas de las llamadas/sesiones ETS.

Una amenaza se considera una debilidad de seguridad o una posible vulnerabilidad que, de explotarse, podría menoscabar la disponibilidad, integridad o confidencialidad de las comunicaciones ETS.

La presente Recomendación se centra principalmente en las amenazas que supone la interconexión de redes para el ETS. Las amenazas relativas a la interconexión de redes son, entre otras, las siguientes:

- Amenaza de interconexión general: debilidades de seguridad o posibles vulnerabilidades asociadas con la conexión de la red (por ejemplo, NGN) a otras redes gestionadas o no gestionadas, como el Internet público.
- Amenaza de diseño y aplicación: debilidades de seguridad o posibles vulnerabilidades de la arquitectura de interconexión de redes y los diseños de aplicación.
- Amenaza interior, operativa y de gestión: debilidades de seguridad o posibles vulnerabilidades de las funciones de instrucción y control del ETS y de su infraestructura subyacente.

- Amenaza de transporte e instalaciones: debilidades de seguridad o posibles vulnerabilidades asociadas con la red de transporte subyacente (por ejemplo, encaminamiento, duplicación de la red, diversidad, resistencia), los sistemas de soporte (por ejemplo, alimentación eléctrica, medio ambiente) y protección física de los activos de la red.

## 7 Arquitectura de referencia de la seguridad de interconexión ETS

En la presente Recomendación se basa en la arquitectura funcional y el modelo de conexión de red definidos en [UIT-T Y.2012].

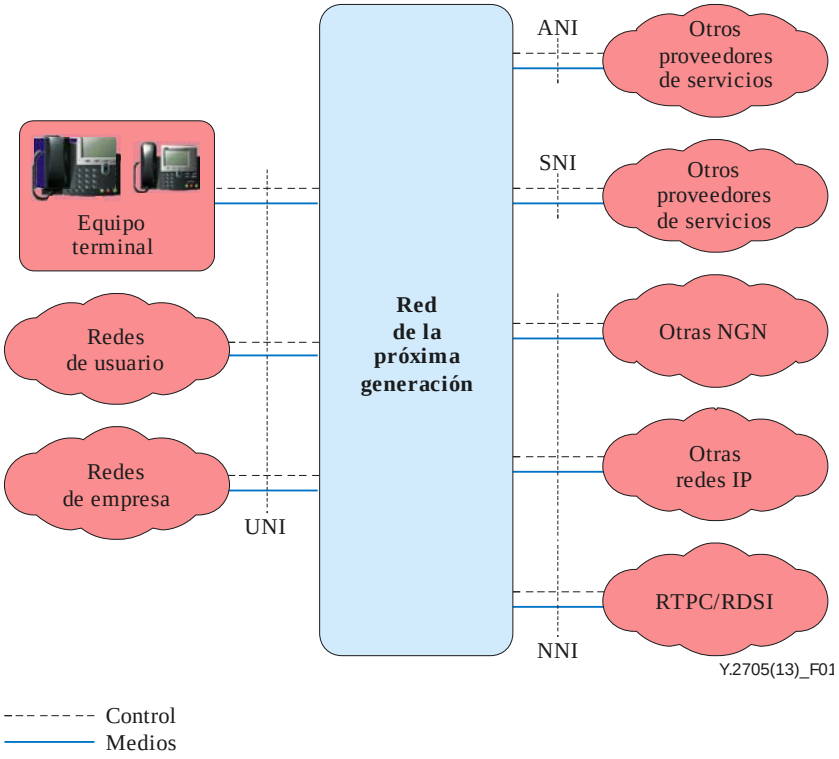



**Figura 1 – Conexión a las NGN [UIT-T Y.2012]**

Las interfaces mediante las que se interconecta la red son:

- Interfaz aplicación-red (ANI)
- Interfaz servicio-red (SNI)
- Interfaz red-red (NNI).

Véase en [UIT-T Y.2012] la descripción de ANI, SNI y NNI.

Para que distintas redes soporten las comunicaciones ETS a través de las fronteras de red, se necesitan medidas de seguridad específicas para proteger la integridad, confidencialidad y disponibilidad de las comunicaciones ETS dentro de cada red nacional y en la interconexión entre redes nacionales.

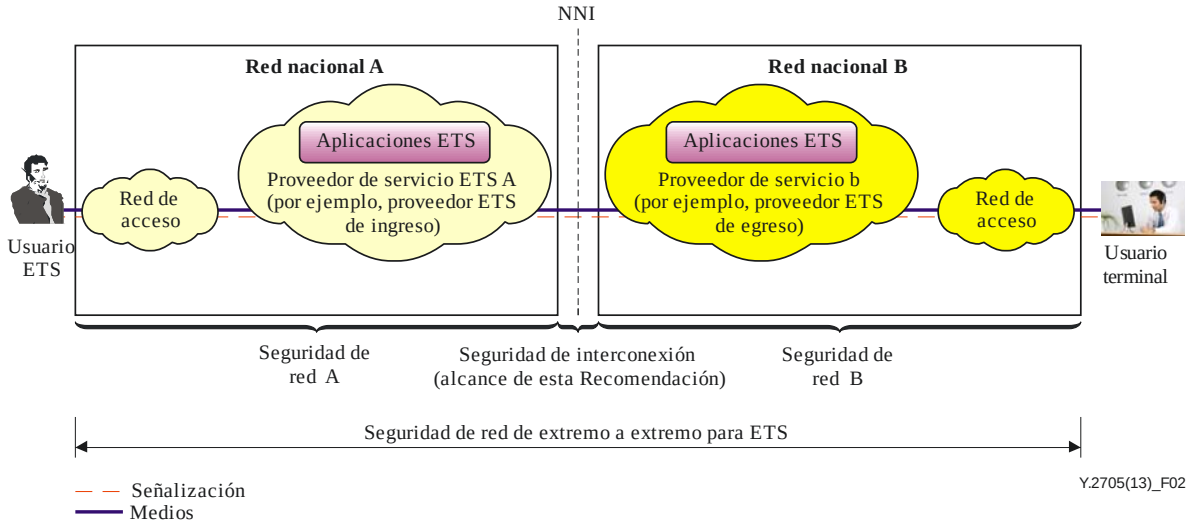



**Figura 2 – Seguridad de red de extremo a extremo para aplicaciones ETS**

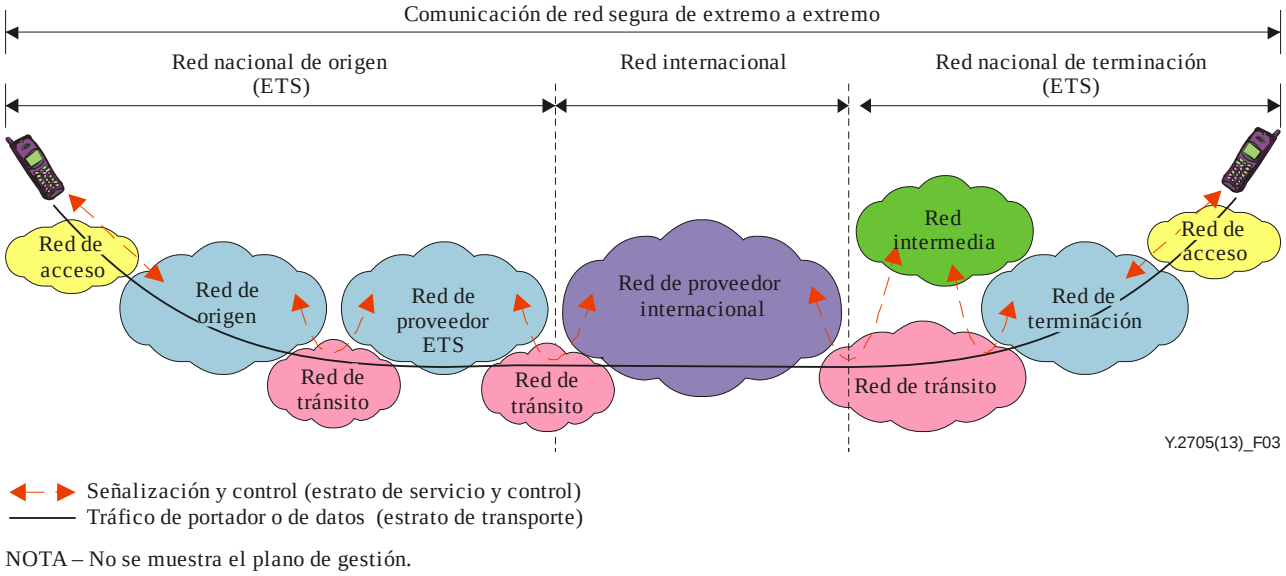
En la Figura 2 se ve que la seguridad de extremo a extremo de una comunicación ETS que atraviese múltiples redes (redes nacionales A y B) dependerá de las medidas de seguridad que se apliquen en cada una de las redes y de la protección de seguridad de la interconexión entre ambas redes.

La Figura 2 muestra que esta Recomendación se centra en la interconexión segura para ETS.

## 8 Objetivos de seguridad y directrices para la interconexión de ETS

### 8.1 Objetivos generales

El objetivo general es ofrecer protección de seguridad de red a las comunicaciones ETS de extremo a extremo que puedan atravesar distintos dominios de proveedor de red y redes internacionales (es decir, países/administraciones) siendo cada red responsable de la seguridad dentro de su dominio salto a salto.




NOTA – No se muestra el plano de gestión.

**Figura 3 – Ejemplo de comunicación de extremo a extremo entre diversos ETS nacionales**

En la Figura 3 se ilustran las comunicaciones ETS de extremo a extremo (por ejemplo, comunicaciones de voz, vídeo datos o mensajería prioritarias) con origen y terminación en dos redes nacionales diferentes. Este ejemplo muestra que la comunicación prioritaria de extremo a extremo del ETS puede atravesar múltiples segmentos de red y dominios administrativos (por ejemplo, red de acceso, red de origen, red de proveedor ETS, red de proveedor internacional, red intermedia y red de terminación). El objetivo general es que cada una de las redes interconectadas a lo largo del trayecto de la comunicación ETS de extremo a extremo ofrezca la protección de seguridad necesaria dentro de su dominio, incluida la interconexión con la red adyacente, de manera que no se pongan en peligro la integridad, confidencialidad y disponibilidad de la comunicación ETS de extremo a extremo.

## 8.2 Directrices generales

Las redes que se interconectan para el ETS han de establecer y aplicar un método estructurado a través de los acuerdos de nivel de servicio (SLA). Ese método comprenderá los siguientes elementos:

1) Evaluación de riesgos de seguridad: evaluación de riesgos de los activos ETS y análisis de amenazas y vulnerabilidades relacionadas con la interconexión ETS. Es fundamental que la evaluación de riesgos de seguridad se efectúe periódicamente y cuando se efectúen cambios en la tecnología, los servicios y las aplicaciones, o se introduzcan otros nuevos.

2) Arquitectura y solución de seguridad: se ha de establecer una política de seguridad, un diseño de arquitectura de seguridad y una especificación de las soluciones para contrarrestar las amenazas al ETS identificadas. Esto comprende la conclusión de los SLA bilaterales o multilaterales necesarios para la seguridad del ETS (véase en [UIT-T M.3342] y [b-TMF GB917] información sobre los SLA). En los SLA para interconexión se han de abordar las políticas de seguridad, los requisitos, el diseño de arquitectura, el conocimiento de la situación, las herramientas forenses y la seguridad de la infraestructura.

3) Aplicación de seguridad: aplicación e implantación de la arquitectura y las soluciones de seguridad, en función de los SLA bilaterales o multilaterales, según proceda, para la seguridad de la interconexión ETS.

4) Operaciones de seguridad: se han de especificar y aplicar medidas operativas para la gestión de las soluciones de seguridad de la interconexión ETS. Por ejemplo, gestión de amenazas internas, gestión de parámetros configurables y valores por defecto, resistencia y operaciones de recuperación de fallos, pruebas de seguridad ETS, registro cronológico y auditoría de eventos de seguridad ETS.

## 8.3 Objetivos y requisitos comunes

En esta cláusula se presentan los requisitos y objetivos comunes.

R-1 El Proveedor de Servicio deberá proteger las comunicaciones ETS contra las intrusiones (por ejemplo, intercepción, pirateo y reproducción) que puedan poner en peligro la autenticidad, integridad, confidencialidad y disponibilidad del ETS, de conformidad con las prácticas idóneas en materia de seguridad disponibles en el mercado, cuando el tráfico ETS atraviese el dominio del Proveedor de Servicio.

En el requisito anterior, el dominio es un "segmento de red" físico o lógico del cual el Proveedor de Servicio es responsable del control, la gestión, el mantenimiento y la seguridad administrativos y operativos.

Se prevé que los proveedores de servicio soporten y utilicen una amplia gama de herramientas y capacidades de seguridad para proteger tanto al ETS como a la red en sí y a todas las aplicaciones soportadas. Es importante que se tomen las medidas adecuadas para garantizar que la utilización de

esas capacidades de seguridad no menoscaba el rendimiento del ETS o introduce brechas de seguridad imprevistas para el ETS.

R-2 La utilización de mecanismos de seguridad por parte del Proveedor de Servicio (por ejemplo, sistema de detección de intrusión y sistema de prevención de intrusión (IDS/IPS) y encriptación) no interferirá con los mecanismos de tratamiento de prioridades utilizados para el soporte de ETS (véase en [UIT-T Y.2205] la definición y descripción del mecanismo de tratamiento de prioridades).

O-1 Conviene que el Proveedor de Servicio utilice herramientas y capacidades de seguridad de tal manera que se minimicen las consecuencias negativas para la calidad de servicio (QoS) del ETS (por ejemplo, introducción de retardos innecesarios).

### 8.4 Autentificación, autorización y control de acceso al ETS

En esta cláusula se abordan:

- La autentificación y autorización de los usuarios del ETS.
- La autentificación de los usuarios del ETS y la autorización de proveedores de ETS.
- La autentificación de las fuentes de datos para el ETS.
- La autentificación y autorización mutua de proveedores de ETS.

#### 8.4.1 Autentificación mutua

La autentificación es el proceso mediante el cual se verifica la identidad declarada de una parte que participa en algún tipo de comunicación. La autentificación garantiza la validez de las identidades declaradas de las entidades que participan en la comunicación (por ejemplo, persona, dispositivo, servicio o aplicación) y asegura que esa entidad no intenta usurpar o reproducir sin autorización una comunicación anterior.

Una comunicación ETS de extremo a extremo puede involucrar a múltiples segmentos de red y dominios administrativos (por ejemplo, red de acceso de origen, red de Proveedor de Servicio ETS, red intermedia, red de acceso de terminación). Al recibir el tráfico ETS, el Proveedor de Servicio debe verificar la validez y autorización de la fuente (por ejemplo, la red) del tráfico recibido. Al entregar el tráfico ETS, el Proveedor de Servicio debe verificar la validez y autorización de la entidad a la que entrega el tráfico NGN (por ejemplo, la red). En la actualidad, las relaciones de confianza de seguridad para la interconexión sólo pueden verificarse mediante la interconexión física directa entre dos redes interconectadas.

R-3 Los proveedores de servicio se autentificarán mutuamente para el intercambio (es decir, entrega o recepción) de tráfico ETS. Esto comprende todo intercambio de tráfico de señalización o de medios ETS entre dos proveedores de servicio a través de NNI, ANI o SNI.

Esto puede efectuarse mediante la verificación de la interconexión física directa y de los acuerdos de nivel de servicio (SLA).

NOTA – El objetivo aquí no es la autentificación de cada llamada/sesión, sino introducir la noción de mecanismos para efectuar la autentificación periódicamente o cuando resulte necesario.

#### 8.4.2 Control de acceso

Se necesitan medidas de control de acceso para la protección de los recursos de red contra la utilización no autorizada, incluida la utilización de los recursos de manera no autorizada. El control de acceso garantiza que sólo los usuarios o dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones.

El control de acceso en la NNI implica la capacidad de la red receptora para aceptar o rechazar tráfico entrante específico procedente de una red vecina y para restringir el acceso a los recursos dentro de la red por parte de entidades exteriores a la red.

R-4 El Proveedor de Servicio establecerá normas y aplicará medidas de control de acceso para evitar que las comunicaciones ETS no autorizadas atraviesen las NNI. Concretamente, el Proveedor de Servicio sólo permitirá que atraviesen las NNI las comunicaciones entre NE que hayan sido identificadas y previamente autorizadas (por ejemplo, mediante SLA).

R-5 Al recibir el tráfico de señalización ETS de otro proveedor de servicio, el Proveedor de Servicio verificará las relaciones de confianza que mantiene con el proveedor de servicio del que recibe el tráfico.

R-6 Al recibir el tráfico de medios ETS de otro proveedor de servicio, el Proveedor de Servicio verificará las relaciones de confianza que mantiene con el proveedor de servicio del que recibe el tráfico ETS.

R-7 Al entregar el tráfico de señalización ETS a otro proveedor de servicio, el Proveedor de Servicio verificará las relaciones de confianza que mantiene con el proveedor de servicio al que entrega el tráfico ETS.

R-8 Al entregar el tráfico de medios ETS a otro proveedor de servicio, el Proveedor de Servicio verificará las relaciones de confianza que mantiene con el proveedor de servicio al que entrega el tráfico.

NOTA – Lo anterior no pretende implicar la verificación por llamada/sesión.

La autorización es la concesión de privilegios, lo que comprende la concesión de acceso en función de los privilegios de acceso. La autorización se concede a una entidad tras su validación mediante un proceso de autentificación y control de acceso.

R-9 El Proveedor de Servicio debe otorgar protección de seguridad para evitar el acceso no autorizado al ETS.

Los medios por los que puede cumplirse con el R-9 son, entre otros, los siguientes (según proceda):

- Autentificación y autorización de usuarios extremos y dispositivos ETS.
- Autentificación y autorización de las fuentes de datos de las comunicaciones ETS (por ejemplo, fuente de mensaje o fuente de datos).
- 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 autentificación y los sistemas de gestión).

El control de acceso al sistema comprende medidas de seguridad para evitar el acceso no autorizado a elementos y sistemas de red y sus puntos de acceso asociados. Hay amenazas relacionadas con el acceso no autorizado a elementos y sistemas de red que soportan el ETS, por lo que se han de establecer y aplicar las medidas de control de acceso convenientes para evitar el acceso no autorizado.

R-10 Los Proveedores de Servicio impondrán normas y aplicarán medidas de control de acceso al sistema para impedir el acceso no autorizado a los elementos y sistemas de red que soportan el ETS. Esto comprende la protección de seguridad del acceso lógico y físico.

R-11 El Proveedor de Servicio otorgará protección contra el acceso no autorizado a los datos y recursos ETS (es decir, el Proveedor de Servicio sólo permitirá a los administradores autorizados acceder a los datos y recursos ETS [por ejemplo, ficheros, instrucciones, software] en los elementos y sistemas de red que soportan el ETS).

### 8.5 Integridad del ETS

Esta cláusula abarca:

- La protección de la integridad de la señalización ETS.
- La protección de la integridad de los medios ETS.

### 8.5.1 Integridad de la señalización

Es necesario proteger la integridad de la señalización ETS entre redes contra la intercepción, la corrupción y la manipulación (por ejemplo, supresión, creación o reproducción).

R-12 Los Proveedores de Servicio protegerán la integridad de todo el tráfico de señalización ETS entre redes que atraviese las NNI, ANI o SNI.

Las medidas que pueden tomarse para proteger la integridad del tráfico de señalización ETS son, entre otras, las siguientes:

a) medidas de seguridad física (por ejemplo, protección física de los elementos de red, los medios de transmisión y las instalaciones, y aplicación de las medidas de control de acceso pertinentes);

b) protección criptográfica;

c) definición y cumplimiento de los adecuados requisitos y objetivos de integridad definidos en los acuerdos de nivel de servicio;

d) supervisión de la integridad de la configuración de las NNI.

### 8.5.2 Integridad de los medios

Es necesario proteger los medios asociados a las comunicaciones ETS entre redes contra la intercepción, la corrupción y la manipulación (por ejemplo, supresión, creación o reproducción).

R-13 El Proveedor de Servicio protegerá la integridad de todo el tráfico de medios ETS entre redes que atraviese las NNI o SNI.

Las medidas que pueden adoptarse para proteger la integridad del tráfico de medios son, entre otras, las siguientes:

a) medidas de seguridad física (por ejemplo, protección física de los elementos de red, los medios de transmisión y las instalaciones, y aplicación de las medidas de control de acceso pertinentes);

b) protección criptográfica;

c) definición y cumplimiento de los adecuados requisitos y objetivos de integridad definidos en los acuerdos de nivel de servicio;

d) supervisión de la integridad de la configuración de las NNI.

## 8.6 Confidencialidad de las comunicaciones ETS y protección de la IIP

Es necesario proteger la confidencialidad de las comunicaciones ETS a través de las NNI, ANI y SNI a fin de impedir que entidades no autorizadas obtengan información sensible. La protección de la confidencialidad comprende:

- Control y señalización ETS.
- Tráfico de portadora ETS (por ejemplo, voz, video o datos).
- Información de identificación personal (IIP).

### 8.6.1 Confidencialidad de la señalización

Los Proveedores de Servicio deben proteger la señalización ETS entre redes a través de las NNI, ANI o SNI contra el acceso no autorizado. La información de señalización se ha de proteger contra las escuchas ilícitas a fin de reducir las posibilidades de que un análisis del tráfico de señalización revele información sensible que se pueda utilizar indebidamente (por ejemplo, patrones de llamada, información de ubicación e identidad de los usuarios).

R-14 El Proveedor de Servicio protegerá la confidencialidad de toda señalización ETS entre redes que atraviese las NNI, ANI o SNI.

Las medidas que pueden tomarse para proteger la confidencialidad del tráfico de señalización y de medios son, entre otras, las siguientes:

a) medidas de seguridad física (por ejemplo, protección física de los elementos de red, los medios de transmisión y las instalaciones, y aplicación de las medidas de control de acceso pertinentes);

b) protección criptográfica;

c) definición y cumplimiento de los adecuados requisitos y objetivos de confidencialidad definidos en los acuerdos de nivel de servicio.

Si bien la protección de la confidencialidad suele asociarse a mecanismos criptográficos, el requisito impuesto en esta cláusula de proteger la confidencialidad de la señalización entre redes no pretende implicar la utilización obligatoria de métodos criptográficos en todos los casos y para todos los flujos de señalización de extremo a extremo. El objetivo del requisito es que los Proveedores de Servicio dispongan y apliquen las medidas necesarias para garantizar que las comunicaciones de señalización a través de las NNI, ANI y SNI están protegidas contra las escuchas ilícitas. Esto supone que se ha de examinar cada interconexión a fin de determinar los mecanismos que conviene utilizar para proteger la confidencialidad, según determine la política de seguridad. Por ejemplo, se puede proteger la confidencialidad utilizando medios físicos y las operaciones conexas, en función de la configuración arquitectónica y física de la interconexión IP (por ejemplo, enlace físico dedicado).

### 8.6.2 Confidencialidad de los medios

Es necesario proteger los trenes de medios (por ejemplo, voz, video y datos) contra el acceso no autorizado porque la escucha ilícita de los trenes de medios ETS puede revelar información de seguridad sensible (es decir, transportada en la comunicación de medios).

R-15 El Proveedor de Servicio protegerá la confidencialidad de todo el tráfico de medios ETS entre redes que atraviese las NNI o SNI.

Las medidas que pueden adoptarse para proteger la confidencialidad del tráfico de señalización y de medios son, entre otras, las siguientes:

a) medidas de seguridad física (por ejemplo, protección física de los elementos de red, los medios de transmisión y las instalaciones, y aplicación de las medidas de control de acceso pertinentes);

b) protección criptográfica;

c) definición y cumplimiento de los adecuados requisitos y objetivos de confidencialidad definidos en los acuerdos de nivel de servicio.

### 8.6.3 Protección de la IIP

Es necesario proteger la información de identificación personal (IIP) asociada al ETS contra la observación o divulgación no autorizadas (por ejemplo identidades de los usuarios extremos del ETS, identidades de las entidades comunicantes, información de abono ETS y ubicación de usuarios extremos del ETS).

R-16 El Proveedor de Servicio permitirá a los usuarios del ETS seleccionados utilizar el ETS anónimamente.

R-17 El Proveedor de Servicio protegerá la confidencialidad de la identidad de los usuarios del ETS seleccionados.

R-18 El Proveedor de Servicio protegerá la confidencialidad de la ubicación de los usuarios del ETS seleccionados.

La protección de la información de utilización del ETS (por ejemplo, patrones de uso, como volumen de tráfico ETS, ubicaciones, horas, frecuencia, etc.) contra la observación no autorizada es

necesaria. Esto comprende el soporte y la utilización de capacidades de seguridad para proteger la información sensible derivada de la observación de las actividades de la red, como los sitios web que ha visitado un usuario extremo, la ubicación geográfica del usuario extremo y las direcciones IP y nombres de servidor de nombres de dominio (DNS de los dispositivos en una red de proveedor de servicio.

O-2 Es conveniente que el Proveedor de Servicio proteja la información de utilización del ETS contra la observación o divulgación no autorizadas (por ejemplo, observación de actividades de la red, como los sitios web visitados por un usuario del ETS, las direcciones IP del usuario del ETS, o los patrones de uso, como el volumen de tráfico ETS, las ubicaciones, horas y frecuencia).

## 8.7 Transporte IP entre redes

### 8.7.1 Generalidades

La interconexión IP-IP entre dos Proveedores de Servicio tendrá variaciones arquitectónicas y físicas de la interconexión con diferentes repercusiones de seguridad.

La integridad y disponibilidad de la interconexión IP-IP entre dos Proveedores de Servicio dependerán de factores como la arquitectura, la conectividad física y los acuerdos de nivel de servicio.

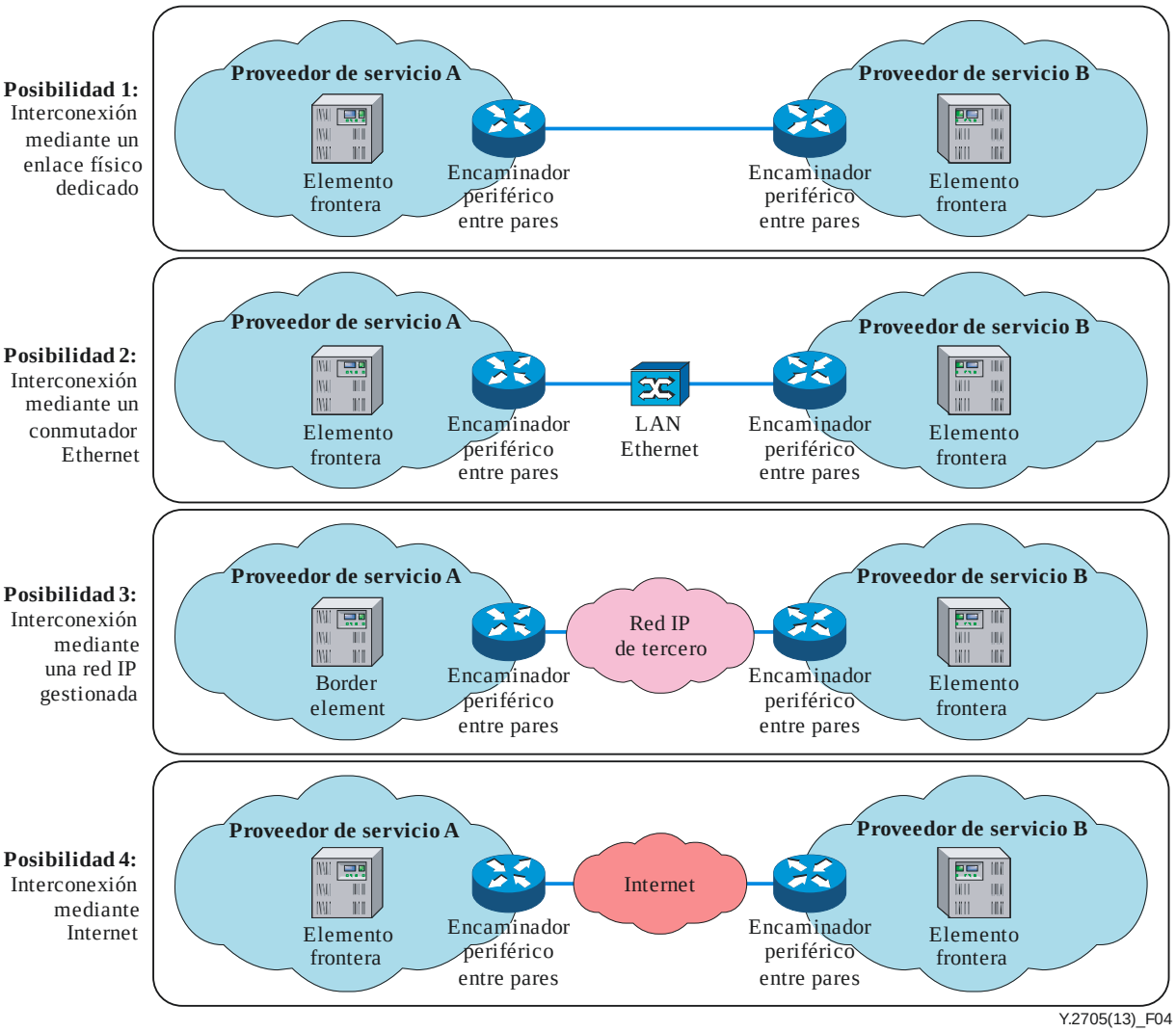



**Figura 4 – Configuraciones de interconexión IP-IP**

En la Figura 4 se muestran algunas de las posibles configuraciones de interconexión IP-IP:

1) Interconexión mediante un enlace físico dedicado: en esta configuración, se utiliza un enlace físico dedicado para conectar el encaminador periférico entre pares del Proveedor de Servicio A al encaminador periférico entre pares del Proveedor de Servicio B.

2) Interconexión mediante un conmutador Ethernet: en esta configuración, el encaminador periférico entre pares del Proveedor de Servicio A y el encaminador periférico entre pares del Proveedor de Servicio B están conectados físicamente por un conmutador Ethernet de una red de área local (LAN).

3) Interconexión mediante una red IP gestionada: en esta configuración, la interconexión IP entre el Proveedor de Servicio A y el Proveedor de Servicio B se efectúa mediante una red IP gestionada, que puede ser la red IP gestionada de un proveedor tercero.

4) Interconexión mediante Internet: en esta configuración, la interconexión IP entre el Proveedor de Servicio A y el Proveedor de Servicio B se efectúa mediante Internet abierto.

Cada una de las posibilidades ilustradas en la Figura 4 tiene consecuencias de seguridad para el ETS diferentes.

En esta Recomendación no se define ni restringe la interconexión IP empleada para conectar a los Proveedores de Servicio. El objetivo general es que depende del Proveedor de Servicio soportar y aplicar, en función de la configuración IP-IP que utilice, las medidas de seguridad adecuadas para proteger la interconexión e impedir que el servicio se vea afectado por los daños que pudiera ocasionar la interconexión IP.

R-19 El Proveedor de Servicio protegerá la red de transporte IP entre dos redes de Proveedores de Servicio interconectadas contra las intrusiones (por ejemplo, intercepción, pirateo y reproducción) que pudieran poner en peligro la autenticidad, integridad, confidencialidad y disponibilidad del ETS de conformidad con las prácticas idóneas en materia de seguridad disponibles en el mercado.

Para cumplir este requisito, el Proveedor de Servicio debe definir y aplicar normas para proteger la red de transporte IP entre redes de Proveedor de Servicio interconectadas, y documentar tales normas en los SLA.

R-20 El Proveedor de Servicio protegerá la integridad de los mecanismos de prioridad del tráfico IP, las capacidades funcionales y los datos de protocolo conexos (por ejemplo, puntos de código Diffserv) utilizados para el soporte del ETS en la interconexión de redes IP entre Proveedores de Servicio.

NOTA – Esto comprende la protección de la integridad de todos los datos o parámetros configurados del ETS relacionados con la interconexión IP, así como toda correspondencia establecida (por ejemplo, correspondencia de los puntos de código Diffserv basada en el esquema utilizado por cada Proveedor de Servicio interconexión).

CR-1 Si la señalización ETS atraviesa un segmento de red de transporte IP no fiable (por ejemplo, transporte IP de tercero), el Proveedor de Servicio recurrirá a la encriptación (por ejemplo, IPsec) para proteger la integridad y la confidencialidad.

CR-2 Si los medios ETS atraviesan un segmento de red de transporte IP no fiable (por ejemplo, transporte IP de tercero), el Proveedor de Servicio recurrirá a la encriptación (por ejemplo IPsec) para proteger la integridad y la confidencialidad.

### 8.7.2 Utilización de la encriptación

La utilización de mecanismos de seguridad (por ejemplo, encriptación) no interferirá con los mecanismos de tratamiento prioritario, ni los obstaculizará.

Cuando se utilicen túneles IPsec para el tráfico ETS entre redes (es decir, al atravesar las NNI, ANI y SIN), se cumplirán los siguientes requisitos:

R-21 El Proveedor de Servicio definirá y aplicará normas para alimentar y proteger la integridad de la información prioritaria (por ejemplo, valores DSCP) cuando se utilicen túneles IPsec para el tráfico ETS entre redes. Concretamente, se definirán en los SLA normas para la inclusión de valores de punto de código Diffserv (DSCP) del encabezamiento interno en el encabezamiento del túnel IPsec en el punto de ingreso IPsec, y se aplicarán para permitir el tratamiento prioritario entre los puntos IPsec de ingreso y de egreso.

## 8.8 Disponibilidad del ETS

### 8.8.1 Objetivo general

Para garantizar una mayor disponibilidad del ETS es necesario mantener al mínimo los fallos de cada sistema de servicio (que soporte el ETS), y la recuperación del servicio ha de ser rápida (tras un corte o fallo). Los fallos derivados de brechas de seguridad se tendrán en cuenta en la planificación y diseño de disponibilidad general del ETS. En el contexto de la seguridad, el objetivo general de disponibilidad del ETS es el siguiente:

O-3 Es conveniente que los Proveedores de Servicio tengan en cuenta los posibles fallos o interrupciones del servicio debidos a eventos de seguridad que afecten a la interconexión entre redes en la planificación y el diseño de la disponibilidad de servicio de extremo a extremo del ETS (es decir, las llamadas/sesiones ETS que atraviesen múltiples redes de Proveedor de Servicio). Esto incluye medidas de recuperación rápida en caso de fallos debidos a eventos de seguridad.

### 8.8.2 Protección de la disponibilidad

Es necesario proteger el ETS contra los ataques de denegación de servicio (DoS), de denegación de servicio distribuida (DDoS) y contra ataques de otro tipo que puedan afectar a la disponibilidad del ETS. Esto comprende la protección contra ataques que afecten a la disponibilidad del ETS para usuarios ETS individuales, grupos de usuarios del ETS, usuarios del ETS en emplazamientos o sitios concretos (por ejemplo, emplazamiento de red de empresa de una agencia estatal), usuarios del ETS en zonas geográficas o regiones concretas, o del ETS en su totalidad.

R-22 El Proveedor de Servicio protegerá la disponibilidad del ETS (por ejemplo, protección contra ataques DoS, DDoS y ataques de otro tipo que afecten a la disponibilidad del ETS), de conformidad con las prácticas idóneas en materia de seguridad disponibles en el mercado. Esto incluirá la protección contra ataques DoS, DDoS y ataques de otro tipo que afecten a la disponibilidad del ETS para usuarios del ETS individuales, grupos de usuarios del ETS, usuarios del ETS en emplazamientos o sitios concretos (por ejemplo, emplazamiento de red de empresa de una agencia estatal), usuarios del ETS en zonas geográficas o regiones concretas, o del ETS en su totalidad.

Las medidas que pueden tomarse para proteger la disponibilidad del ETS son, entre otras, las siguientes:

a) utilización de mecanismos de control de admisión y de regulación de eventos;

b) utilización de herramientas y funciones de mitigación de DoS y DDoS;

c) utilización de sistemas de detección de intrusiones y de sistemas de prevención de intrusiones (IDS/IPS);

d) utilización de herramientas de supervisión de seguridad;

e) utilización de herramientas de conocimiento de la situación.

R-23 Los Proveedores de Servicio utilizar herramientas y capacidades de seguridad para proteger la disponibilidad (por ejemplo, mecanismos DoS y DDoS), incluidas las medidas convenientes para impedir la denegación involuntaria de llamadas/sesiones ETS legítimas (por ejemplo, que se bloquee o impida la compleción de llamadas/sesiones ETS legítimas o que se descarten paquetes ETS legítimos).

### 8.9 Seguridad de la gestión y las operaciones

En esta cláusula se tratan temas relacionados con:

- La seguridad de las operaciones de gestión (por ejemplo, parámetros configurables y por defecto relacionados con la configuración de la interconexión ETS).
- Registro cronológico de los eventos de seguridad ETS.
- Alertas y alarmas en caso de brecha de seguridad posible o real.

#### 8.9.1 Integridad de los datos ETS

Se ha de proteger la integridad de los datos ETS almacenados para impedir toda corrupción o manipulación de los datos que pueda afectar a la integridad o disponibilidad del ETS.

R-24 El Proveedor de Servicio protegerá la integridad de los datos ETS configurados. Esto comprende todos los datos ETS específicos, como los datos de abono, que se configuren.

#### 8.9.2 Parámetros configurables y valores por defecto

Hay muchas amenazas de seguridad relacionadas con la gestión de los parámetros configurables y los valores por defecto definidos por los fabricantes y proveedores de equipos. Por ejemplo, los valores por defecto de diversos parámetros configurables, tal y como los define el fabricante, se han de ajustar para adaptarse a los requisitos del Proveedor de Servicio. Los parámetros configurables se han de asignar adecuadamente y mantener actualizados a fin de que funcionen satisfactoriamente. El administrador humano ha de estar debidamente autorizado para realizar la administración de la seguridad.

R-25 El Proveedor de Servicio debe definir y aplicar normas para la administración de los parámetros configurables y los valores por defecto para el soporte del ETS. Se han de imponer y aplicar medidas de control de acceso a fin de que la ejecución de esas funciones esté reservada exclusivamente al administrador autorizado (es decir, que se denegará este permiso a todos los demás usuarios).

#### 8.9.3 Gestión de amenazas internas

Cualquier persona (por ejemplo, un empleado, un contratista o un trabajador) puede obtener acceso de gestión no autorizado o utilizar indebidamente su acceso de gestión a elementos y sistemas de red que soportan el ETS. Por consiguiente, es necesario minimizar las amenazas internas.

R-26 El Proveedor de Servicio impondrá y aplicará procesos de seguridad para minimizar las amenazas internas al ETS.

Como ejemplos de mitigación pueden citarse los siguientes:

- Controles de autentificación, privilegios por funciones, separación de funciones y métodos de acceso seguro para el acceso a los sistemas distantes, centralizados, manuales y automatizados.
- Registro cronológico de los eventos de seguridad relacionados con actividades de gestión.
- División de la información, las aplicaciones y el acceso ETS para sistemas y aplicaciones compartidos
- Auditoria de datos configurados en elementos de red y bases de datos (por ejemplo, perfiles de abono) para el registro y la detección de modificaciones no autorizadas.

### 8.9.4 Colaboración para el intercambio de información de ciberseguridad

Los Proveedores de Servicio entablaran relaciones de colaboración con sus socios para compartir información sobre eventos de ciberseguridad (incluido el intercambio de información en tiempo real durante un ataque de ciberseguridad). El intercambio de información sobre incidentes de ciberseguridad puede reportar beneficios a todas las partes y puede emplearse para anticipar las amenazas que se ciernen sobre el ETS poniendo al Proveedor de Servicio en situación de aplicar contramedidas efectivas.

O-4 Es conveniente que los Proveedores de Servicio impongan y apliquen procesos operativos y de gestión suficientes para entablar relaciones de colaboración para la compartición y el intercambio de información sobre eventos de seguridad. Los procesos deben tener en cuenta las funciones de análisis para que la información resulte útil a fin de tomar medidas y contramedidas de seguridad para proteger el ETS.

En las siguientes Recomendaciones UIT-T se puede encontrar más información sobre el intercambio de información de ciberseguridad:

- [b-UIT-T X.1500]
- [b-UIT-T X.1500.1]
- [b-UIT-T X.1520]
- [b-UIT-T X.1521]
- [b-UIT-T X.1524]
- [b-UIT-T X.1570].

### 8.9.5 Gestión de la intervención en caso de incidentes y la recuperación en caso de evento de seguridad

La disponibilidad del ETS depende de los procedimientos operativos implantados para la recuperación y la restauración del servicio tras un evento de seguridad. Es fundamental que esos procedimientos se definan, documenten y apliquen claramente, lo que implica que han de existir las necesarias políticas y prácticas para la recuperación y restauración del servicio dentro de un domino de Proveedor de Servicio y entre dominios para la interconexión y los servicios entre redes. Es necesario proteger la documentación procesal operativa y su aplicación contra los intrusos y las amenazas internas.

R-27 El Proveedor de Servicio debe disponer de un plan de recuperación e intervención en caso de incidentes documentado donde se describan las políticas y las medidas, procesos y procedimientos operativos y de gestión para la recuperación y restauración del servicio tras un evento de seguridad. Esto incluye las necesarias políticas y prácticas para la recuperación y restauración del servicio dentro de un dominio de Proveedor de Servicio y entre dominios para la interconexión y los servicios entre redes.

# Bibliografía


[b-UIT-T Q-Sup.57] Suplemento 57 a la serie de Recomendaciones UIT-T Q (2008), *Requisitos de señalización para el soporte del servicio de telecomunicaciones de emergencia (ETS) en las redes IP*

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

[b-UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Técnicas para el intercambio de información en materia de ciberseguridad.*

[b-UIT-T X.1500.1] Recomendación UIT-T X.1500.1 (2012), *Procedimientos de registro de arcos bajo el arco de identificador de objetos (OID) para el intercambio de información sobre ciberseguridad.*

[b-UIT-T X.1520] Recomendación UIT-T X.1520 (2011), *Vulnerabilidades y exposiciones comunes*.

[b-UIT-T X.1521] Recomendación UIT-T X.1521 (2011), *Sistema común de puntuación de vulnerabilidades*.

[b-UIT-T X.1524] Recomendación UIT-T X.1524 (2012), *Lista de puntos débiles comunes*.

[b-UIT-T X.1570] Recomendación UIT-T X.1570 (2011), *Mecanismos de descubrimiento en el intercambio de información de ciberseguridad*.

[b-TMF GB917] GB 917 (2012), *SLA Management Handbook*, Release 3.1, TM Forum.

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie D | Principios generales de tarificación |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y 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 | Terminales y métodos de evaluación subjetivos y objetivos |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos, comunicaciones de sistemas abiertos y seguridad |
| **Serie Y** | **Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación** |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2013