

Unión Internacional de Telecomunicaciones

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.1032**

(12/2010)

SERIE X: REDES DE DATOS, COMUNICACIONES  
DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la información y de las redes –  
Seguridad de las redes

---

**Arquitectura de interrelaciones externas  
para un sistema de seguridad de la red  
de telecomunicaciones IP**

Recomendación UIT-T X.1032

UIT-T



RECOMENDACIONES UIT-T DE LA SERIE X  
**REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD**

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
<b>Seguridad de las redes</b>	<b>X.1030–X.1049</b>
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

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

## Recomendación UIT-T X.1032

### Arquitectura de interrelaciones externas para un sistema de seguridad de la red de telecomunicaciones IP

#### Resumen

La Recomendación UIT-T X.1032 propone cuatro modelos que hacen posible examinar las interrelaciones entre un sistema de seguridad de la red de telecomunicaciones IP (TNSS) y varios grupos de objetos externos. Se considera cada objeto en cuanto a sus funciones principales y su probable efecto sobre la construcción del TNSS y los principios de funcionamiento. Esta Recomendación sirve de base para elaborar recomendaciones detalladas sobre seguridad de la red con respecto al efecto en objetos externos.

#### Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1032	2010-12-17	17

## 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/>.

© UIT 2011

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1	Ámbito ..... 1
2	Referencias ..... 2
3	Definiciones ..... 2
3.1	Términos definidos en otras Recomendaciones ..... 2
3.2	Términos definidos en esta Recomendación ..... 3
4	Abreviaturas y acrónimos ..... 3
5	Convenios ..... 3
6	Consideraciones generales ..... 3
7	Interrelaciones del TNSS con los sistemas de seguridad de los sistemas de información y estructura de la información ..... 4
7.1	Modelo de interrelaciones ..... 4
7.2	Funciones de los objetos externos y sus efectos sobre el TNSS ..... 4
8	Interrelaciones del TNSS con los objetos del sistema de telecomunicaciones ..... 5
8.1	Modelo de interrelaciones ..... 5
8.2	Funciones de los objetos externos y sus efectos en el TNSS ..... 5
9	Interrelaciones del TNSS con organizaciones externas ..... 7
9.1	Modelo de interrelaciones ..... 7
9.2	Funciones de organizaciones externas y su efecto en el TNSS ..... 7
10	Interrelaciones del TNSS con las fuentes que constituyen una amenaza para la seguridad ..... 8
10.1	Modelo de interrelaciones ..... 8
10.2	Funciones de objetos externos y su efecto en el TNSS ..... 8
	Apéndice I – Posible composición de las instalaciones técnicas de la red de telecomunicaciones IP ..... 10
	Bibliografía ..... 11



## Recomendación UIT-T X.1032

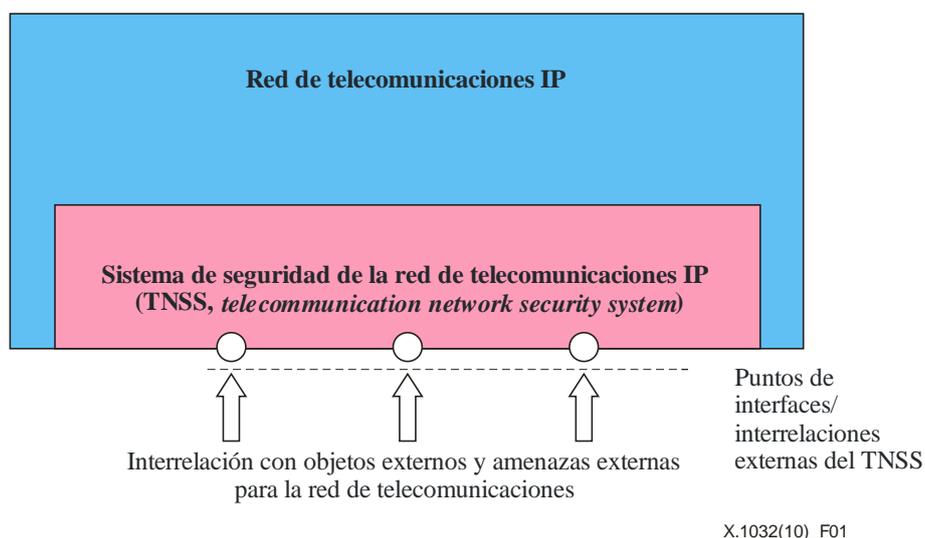
### Arquitectura de interrelaciones externas para un sistema de seguridad de la red de telecomunicaciones IP

#### 1 Ámbito

**1.1** En el estudio de cualquier objeto deben considerarse no sólo las interconexiones entre los distintos componentes situados en el interior del objeto sino también las interrelaciones externas del objeto. A través de estas interrelaciones externas el objeto lleva a cabo sus funciones en el contexto del sistema global. Además, estas interrelaciones pueden actuar como distintas amenazas que pueden llegar a perturbar el funcionamiento del objeto.

El estudio de estos objetos es especialmente importante para el sistema de seguridad de la red de telecomunicaciones IP (TNSS), que debe proteger la red de telecomunicaciones IP fundamentalmente contra las amenazas externas (véase la figura 1).

En el apéndice I aparece una posible composición de los componentes técnicos de una red de telecomunicaciones IP.



**Figura 1 – Interrelaciones entre el sistema de seguridad de la red de telecomunicaciones IP y los objetos externos**

**1.2** El TNSS no funciona como un sistema autónomo sino en estrecha interacción con un cierto número de sistemas externos.

Estos sistemas externos incluyen en primer lugar todas las propias redes de telecomunicaciones IP que protege el TNSS. Los principios de construcción del medio de transporte y de las plataformas de servicio determinan directamente los requisitos del TNSS y, por ende, los principios de construcción de dicho TNSS.

En segundo lugar, estos sistemas externos incluyen a los usuarios de la red de telecomunicaciones IP cuyos requisitos deben satisfacerse mediante una red de telecomunicaciones IP que incluya su TNSS.

Los principios de construcción del TNSS también pueden resultar afectados por otras organizaciones externas. Entre estas organizaciones cabe citar:

- autoridades de reglamentación nacional;

- terceras partes confiables que proporcionan servicios para el sistema de seguridad (bajo el principio "externalización");
- organizaciones que utilizan los servicios de la red de telecomunicaciones IP para la creación de redes de información;

A la larga, la tarea principal del TNSS consiste en proteger las redes de telecomunicaciones IP y la información transmitida a través de estas redes contra las diversas amenazas de seguridad externas existentes en el entorno en que funciona el TNSS.

La lista anterior indica que el TNSS tiene interrelaciones con muchos objetos externos que pueden subdividirse en varios grupos.

**1.3** Las interrelaciones del TNSS con objetos externos pueden afectar directa o indirectamente los requisitos del propio TNSS y de los principios de construcción de funcionamiento del TNSS. Por lo tanto, en el transcurso del desarrollo del TNSS deben tenerse en cuenta estas interconexiones. Existen Recomendaciones del UIT-T que abordan ciertos aspectos de este problema (por ejemplo, las Recomendaciones [UIT-T X.842] y [UIT-T X.843] consideran las interrelaciones con una tercera parte confiable). Sin embargo, muchos aspectos de las interrelaciones del TNSS con objetos externos aún no han sido considerados.

**1.4** Esta Recomendación cubre una arquitectura general de las interrelaciones del TNSS con objetos externos. Esta arquitectura puede aplicarse a diversos tipos de redes de telecomunicaciones IP y a varios sistemas de seguridad de las telecomunicaciones. La Recomendación tiene por objeto ofrecer una panorámica general de todas las interrelaciones externas del TNSS. La Recomendación puede servir de base para la elaboración de Recomendaciones detalladas sobre seguridad de la red con respecto a los efectos en los objetos externos.

## **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, estarán 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 decisiones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. La referencia a un documento en el marco de esta Recomendación no le confiere, como documento autónomo, carácter de Recomendación.

- [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 X.842] Recomendación UIT-T X.842 (2000) | ISO/CEI TR14516:2002, *Tecnología de la información – Técnicas de seguridad – Directrices sobre el uso y gestión de servicios a tercera parte confiable*.
- [UIT-T X.843] Recomendación UIT-T X.843 (2000) | ISO/CEI 15945:2002, *Tecnología de la información – Técnicas de seguridad – Especificación de servicios para soportar la aplicación de firmas digitales*.

## **3 Definiciones**

### **3.1 Términos definidos en otras Recomendaciones**

Ninguna.

## 3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

**3.2.1 sistema de seguridad:** Variedad de elementos de interrelación (ciertos principios, organización y medidas técnicas para la prestación de seguridad) que minimizan la vulnerabilidad de los activos y recursos.

**3.2.2 sistema de seguridad de la red de telecomunicaciones IP (TNSS, *telecommunication IP-based network security system*):** Sistema de seguridad utilizado en una red de telecomunicaciones IP.

## 4 Abreviaturas y acrónimos

Esta Recomendación utiliza las siguientes abreviaturas y acrónimos:

TIC Tecnologías de la información y la comunicación (*information and communication technologies*)

TNSS Sistema de seguridad de la red de telecomunicaciones (*telecommunication IP-based network security system*)

## 5 Convenios

Ninguno.

## 6 Consideraciones generales

**6.1** La consideración de las interrelaciones del TNSS con objetos externos se complica por el elevado número de tales objetos y por los diversos tipos de relaciones e interfaces. Por consiguiente, un problema importante es la posibilidad de la descomposición (división) del conjunto de interrelaciones. Esta Recomendación propone cuatro tipos de interrelaciones externas:

- interrelaciones del TNSS con los sistemas de seguridad superpuestos a sistemas de información de infraestructura y las estructuras de información;
- interrelaciones del TNSS con los objetos del sistema de telecomunicaciones;
- interrelaciones del TNSS con otros objetos; es decir, organizaciones externas;
- interrelaciones del TNSS con las amenazas de seguridad, que pueden ser los objetos antes nombrados o nuevos objetos.

Estos tipos de interrelaciones se consideran a continuación en las cláusulas 7, 8, 9 y 10, respectivamente.

**6.2** Además, en las cláusulas 7, 8, 9 y 10 se utiliza el principio de descomposición. En primer lugar, se define un modelo de interrelaciones en forma gráfica. Este modelo contiene objetos externos y sus interrelaciones con el TNSS. A continuación, se describen las funciones de cada uno de estos objetos externos. Por último, a partir de estas funciones se evalúan brevemente:

- los posibles efectos de los objetos externos sobre el TNSS (por ejemplo, efectos sobre los requisitos del TNSS, efectos sobre los principio de construcción y funcionamiento del TNSS);
- los tipos posibles de interrelación (por ejemplo, una interfaz eléctrica, requisitos organizativos, influencia del medio ambiente externo).

## 7 Interrelaciones del TNSS con los sistemas de seguridad de los sistemas de información y estructura de la información

### 7.1 Modelo de interrelaciones

La figura 2 muestra las interrelaciones del TNSS con los sistemas de seguridad superpuestos a sistemas de información de infraestructura que, a su vez, tienen interfaces con los sistemas de seguridad de la estructura de la información.

### 7.2 Funciones de los objetos externos y sus efectos sobre el TNSS

**7.2.1** Los sistemas de información utilizan varios tipos de tecnologías de la información que emplean las telecomunicaciones. Las funciones de los sistemas de información incluyen, por ejemplo, recopilación, almacenamiento y extracción de la información, organización de las bases de datos y las direcciones de usuarios, apoyo técnico a la edición, conversión y otros tipos de procesamiento de la información. Los sistemas de información pueden realizar funciones de transferencia y distribución de la información a distancia utilizando los servicios de telecomunicaciones, (es decir, constituyendo redes de información-telecomunicación). Un ejemplo de red pública de información-telecomunicación es Internet.

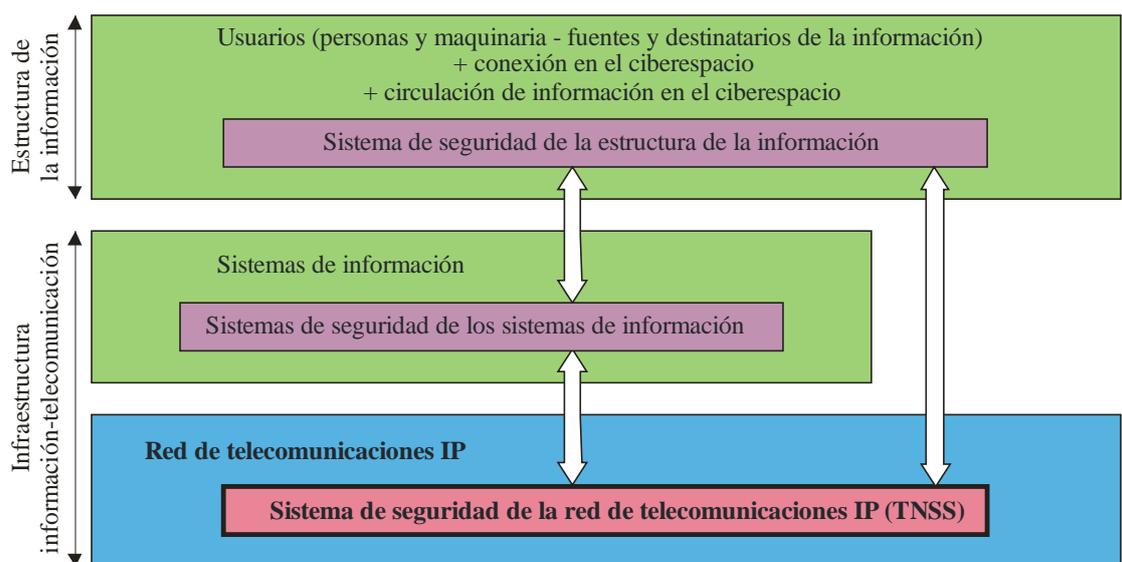
Los tipos tradicionales de comunicación (por ejemplo, comunicaciones telefónicas, comunicaciones facsímil) pueden realizarse con y sin la utilización de la red de información-telecomunicación.

Los sistemas de seguridad del sistema de información sirven para proteger los procesos técnicos de estos sistemas y la información almacenada y transferida dentro de estos sistemas. Los sistemas de seguridad del sistema de información pueden afectar al TNSS de las siguientes maneras:

- se suplementan durante la protección contra ciertas amenazas; por ejemplo, contra la divulgación de información; y
- introducen limitaciones en los protocolos de seguridad utilizados en el TNSS.

La interrelación externa del TNSS con los sistemas de seguridad del sistema de información puede ser:

- interfaces de hardware o software; o
- acuerdo contractual.



X.1032(10)\_F02

**Figura 2 – Modelo de interrelaciones del TNSS con los sistemas de seguridad de los sistemas de información y la estructura de la información**

**7.2.2** La estructura de la información garantiza que la información se utiliza en todas las esferas de la actividad humana. El sistema de seguridad de la estructura de información sirve para proteger a los usuarios del ciberespacio (autores, propietarios, fuentes, destinatarios y compradores de información) contra intrusiones en el ciberespacio que perturban el trabajo de los usuarios. Los usuarios del ciberespacio incluyen personas y maquinaria (elementos de detección, actuadores, dispositivos automáticos, etc.). Como ejemplos de intrusiones no deseadas pueden citarse a los virus, gusanos, correo basura y software dañino (malware) que existen en el ciberespacio. Una intrusión no deseada también puede incluir una denegación de servicio de la infraestructura de información y comunicación.

El sistema de seguridad de la estructura de la información puede afectar al TNSS directamente o a través de los sistemas de seguridad de la red de información; por ejemplo, puede imponer requisitos al TNSS para la protección del ciberespacio mediante herramientas técnicas que puedan soportar la ejecución de medidas jurídicas, administrativas y de organización utilizadas en el sistema de seguridad de la infraestructura de la información. Ese tipo de herramientas técnicas incluyen los medios de contrarrestar los virus y el correo basura.

La interrelación externa del TNSS con el sistema de seguridad de la estructura de la información puede establecerse mediante acuerdo contractual.

## **8 Interrelaciones del TNSS con los objetos del sistema de telecomunicaciones**

### **8.1 Modelo de interrelaciones**

La figura 3 muestra las interrelaciones del TNSS con sus propios objetos de la red de telecomunicaciones y con los sistemas de seguridad de otros objetos del sistema de telecomunicaciones; es decir, con los sistemas de seguridad de los equipos terminales de usuario y de las redes de telecomunicaciones vecinas.

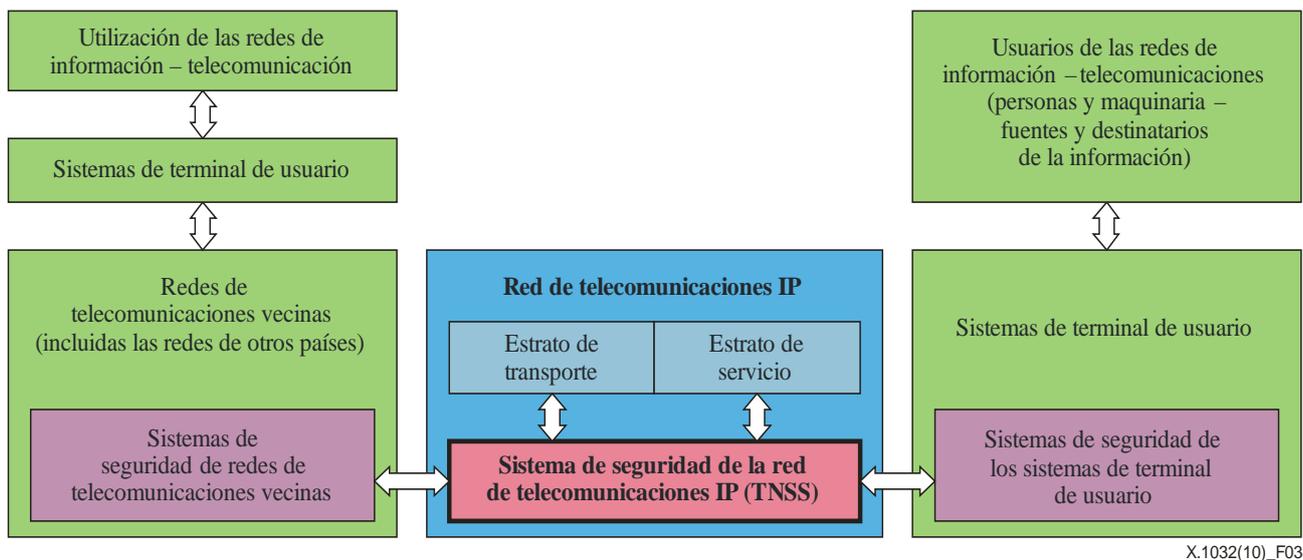
### **8.2 Funciones de los objetos externos y sus efectos en el TNSS**

**8.2.1** Los objetos internos de la red de telecomunicaciones (estrato de transporte y estrato de servicio) determinan la nomenclatura de los servicios de telecomunicaciones ofrecidos, así como las características cuantitativas y cualitativas de estos servicios. Dichos objetos afectan directamente al TNSS, en particular determinan:

- la lista de servicios sujetos a protección;
- las posibilidades de la red en cuanto a realización de mecanismos de seguridad.

Las interrelaciones externas del TNSS con el estrato de transporte y el estrato de servicio pueden ser

- interfaces de hardware o software; o
- acuerdo contractual.



X.1032(10)\_F03

**Figura 3 – Modelo de interrelaciones del TNSS con los objetos del sistema de telecomunicaciones**

**8.2.2** Los sistemas de terminal de usuario pueden contener algunos dispositivos terminales (aparatos telefónicos, receptores de televisión, ordenadores y otros tipos de terminales) y las pertinente conexiones a la red doméstica/empresarial (véanse en el apéndice I más detalles al respecto). Los sistemas de seguridad de los sistemas de terminal de usuario llevan a cabo funciones de protección para los dispositivos terminales y la red doméstica/empresarial contra amenazas a la seguridad. Estas amenazas pueden proceder de la red de telecomunicaciones misma o de fuentes internas (por ejemplo, el sistema del terminal de usuario). Además, los sistemas de seguridad de los sistemas de terminal de usuario emplean mecanismos para proteger la información de usuario transmitida a la red de telecomunicaciones.

Los sistemas de seguridad de los sistemas de terminal de usuario pueden afectar al TNSS, en particular pueden:

- soportarse mutuamente durante la protección de la información de usuario contra ciertas amenazas, por ejemplo criptando los datos transmitidos;
- determinar los requisitos del nivel de seguridad objetivo que debe garantizar el TNSS.

Las interrelaciones externas del TNSS con los sistemas de seguridad de los sistemas del terminal de usuario pueden expresarse como:

- una interfaz eléctrica; o
- requisitos y limitaciones organizativos.

**8.2.3** Las redes de telecomunicaciones vecinas (incluidas las redes de otros países) realizan un intercambio de tráfico con la red de telecomunicaciones considerada. Los sistemas de seguridad de las redes de telecomunicaciones vecinas llevan a cabo funciones de protección de estas redes y de la información transmitida a través de dichas redes contra amenazas de seguridad. Estos sistemas pueden afectar al TNSS, en particular, pueden:

- suplementarse durante la protección de información de usuario contra ciertas amenazas; por ejemplo, contra la corrupción o modificación de la información; y
- introducir limitaciones para utilizar ciertos mecanismos de seguridad del TNSS o modos de funcionamiento de estos mecanismos.

Las relaciones externas del TNSS con los sistemas de seguridad de las redes de telecomunicaciones vecinas pueden ser:

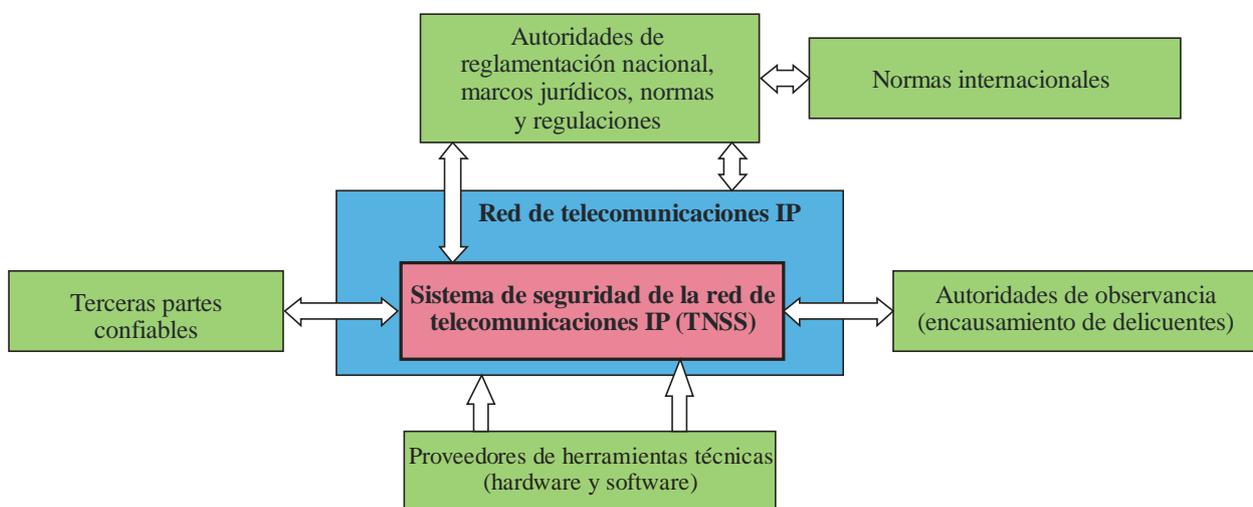
- una interfaz eléctrica; o
- disposiciones organizativas acordadas de forma bilateral.

## 9 Interrelaciones del TNSS con organizaciones externas

### 9.1 Modelo de interrelaciones

La figura 4 muestra interrelaciones del TNSS con varias organizaciones externas (para la red de telecomunicaciones) incluidas:

- las autoridades de reglamentación;
- las terceras partes confiables;
- las autoridades encargadas del cumplimiento de la ley; y
- proveedores de herramientas técnicas (hardware y software).



X.1032(10)\_F04

**Figura 4 – Modelo de interrelaciones del TNSS con organizaciones externas**

### 9.2 Funciones de organizaciones externas y su efecto en el TNSS

**9.2.1** Las autoridades de reglamentación definen las políticas generales en el campo de las telecomunicaciones; en particular, se ocupan de la elaboración y aplicación de normas internacionales, reglamentos y leyes, colaborando a la vez en la elaboración de normas nacionales.

**9.2.2** En cumplimiento de acuerdos bilaterales con un operador de la red de telecomunicaciones, las terceras partes pueden realizar ciertas funciones para garantizar el funcionamiento del TNSS.

La lista de estas funciones y principios de interacción entre terceras partes y el TNSS viene determinada por el operador de la infraestructura que incorpora el TNSS determinado.

Las interrelaciones externas del TNSS con terceras partes pueden ser:

- interfaces de hardware o software;
- acuerdos contractuales.

**9.2.3** Las autoridades encargadas del cumplimiento de ley (procesamiento de delincuentes) actúan en contra de las violaciones de la ley nacional en el campo de las redes de la información y las telecomunicaciones. En concreto, han de detener a los infractores responsables. Las autoridades encargadas del cumplimiento de la ley y el TNSS se suplementan, lo que mejora la seguridad de las telecomunicaciones.

Habida cuenta de la importancia de las tecnologías de la información y la comunicación (TIC) en todas las esferas de la sociedad humana, la legislación es y seguirá siendo fundamental en el camino hacia la sociedad de la información. En último término, esta tendencia dará mayor relieve a la función de las autoridades encargadas del cumplimiento de la ley pertinentes.

A fin de ejecutar las funciones mencionadas, es necesario que las autoridades encargadas del cumplimiento de la ley reciban puntualmente de los operadores de la red de telecomunicaciones información sobre los incidentes de seguridad que constituyan violaciones de la ley. El TNSS ha de ocuparse de la adquisición, almacenamiento y análisis de la información que permita recopilar y enviar los mensajes correspondientes a las autoridades encargadas del cumplimiento de la ley. La posibilidad de transferir información sobre los incidentes de seguridad de las organizaciones de telecomunicaciones a las autoridades encargadas del cumplimiento de la ley viene indicada, por ejemplo, en [b-UIT-T E.409], [b-UIT-T X.1051] y [b-UIT-T X.1056].

Las interrelaciones externas del TNSS con las autoridades encargadas del cumplimiento de la ley pueden ser:

- una interfaz eléctrica u otros servicios de telecomunicaciones o servicios postales; y
- disposiciones organizativas acordadas de forma bilateral.

## **10 Interrelaciones del TNSS con las fuentes que constituyen una amenaza para la seguridad**

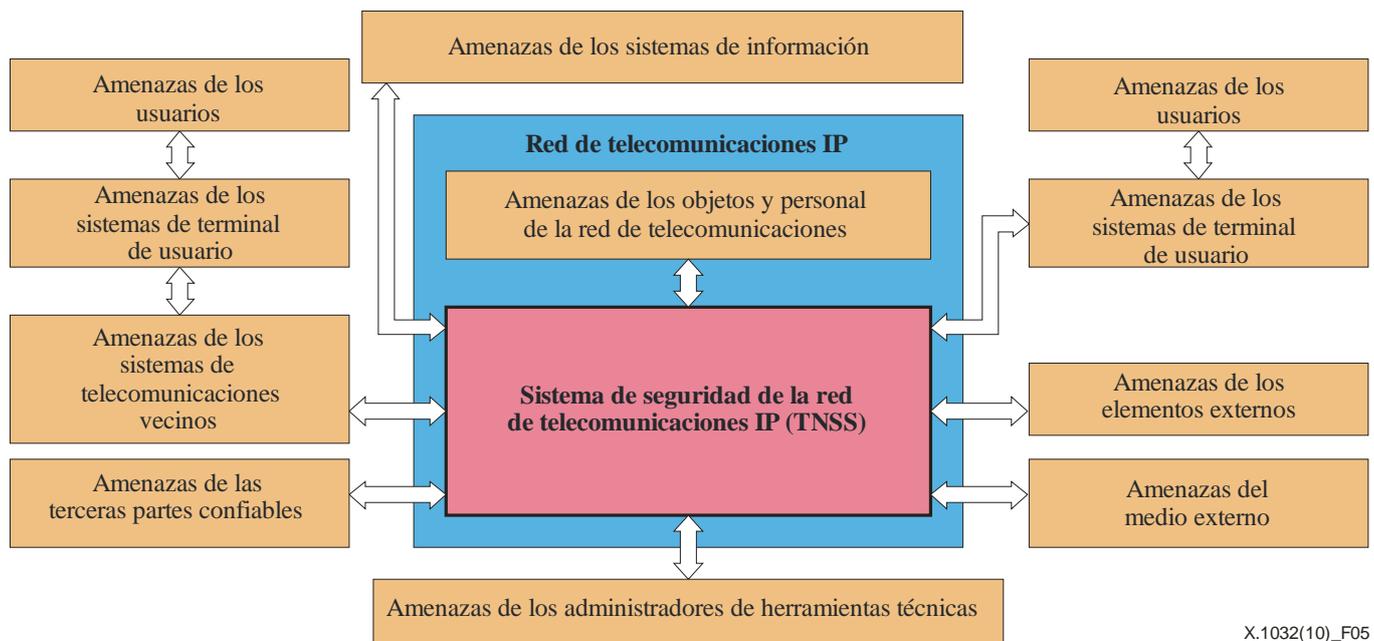
### **10.1 Modelo de interrelaciones**

La figura 5 representa un modelo de interrelaciones del TNSS con diversas fuentes que amenazan la seguridad e incluye:

- usuarios y sus sistemas terminales conectados a la red de telecomunicaciones considerada;
- elementos de exteriores (no usuarios) y medio externo;
- objetos y personal de la red de telecomunicaciones;
- redes de telecomunicaciones vecinas incluidos los usuarios pertinentes y los sistemas de terminal de usuario;
- sistemas de información conectados;
- terceras partes confiables; y
- suministradores de herramientas técnicas.

### **10.2 Funciones de objetos externos y su efecto en el TNSS**

Las fuentes que amenazan la seguridad pueden atacar a las redes de telecomunicaciones. El sistema de seguridad de la red de telecomunicaciones IP (TNSS) se utiliza para prevenir, detectar y neutralizar tales ataques. Por lo tanto, puede decirse que las amenazas contra la seguridad están directamente relacionadas con el TNSS, como se ilustra en la figura 5.



X.1032(10)\_F05

**Figura 5 – Modelo de interrelaciones del TNSS con las fuentes de amenaza contra la seguridad**

Las amenazas se clasifican en cinco tipos, como indica las Recomendaciones [UIT-T X.800] y [UIT-T X.805]:

- destrucción de la información y otros recursos;
- corrupción o modificación de la información;
- robo, supresión o pérdida de información y de otros recursos;
- revelación de la información; y
- interrupción de los servicios.

La política de seguridad en la red de telecomunicaciones puede utilizarse para contrarrestar todas las amenazas o solamente algunas de ellas. De la forma correspondiente, en el transcurso de la elaboración del TNSS se seleccionan las dimensiones de seguridad requerida. En el cuadro 1 de la Recomendación [UIT-T X.805], aparece la correspondencia entre las amenazas contra la seguridad y las dimensiones de seguridad.

Las interrelaciones externas del TNSS con las fuentes de amenazas contra la seguridad pueden ser:

- interfaces eléctricas;
- acciones de las personas;
- ataques utilizando medios técnicos por la red de comunicaciones y medios técnicos externos;
- influencias medioambientales externas;
- medidas técnicas para contrarrestar los ataques; y
- medidas organizativas para contrarrestar los ataques.

## Apéndice I

### Posible composición de las instalaciones técnicas de la red de telecomunicaciones IP

(Este apéndice no forma parte integrante de la presente Recomendación.)

**A.1** Esta Recomendación utiliza el término "red de telecomunicaciones" para referirse a las siguientes instalaciones de los operadores de telecomunicaciones:

- instalaciones de suministradores de infraestructura (es decir, nodos de red, sus circuitos de conexión, redes de acceso, etc.);
- instalaciones de proveedores de servicio (es decir, servidores de servicio y otros); el cometido del suministrador de servicio puede desempeñarlo el suministrador de infraestructura; de no ser así, el suministrador de servicio puede funcionar dentro de la red independientemente;
- instalaciones de los proveedores de aplicaciones (es decir, servidores de aplicaciones y otros); un cometido del proveedor de aplicaciones puede desempeñarlo el proveedor de servicio; de no ser así, el proveedor de aplicaciones puede funcionar dentro de la red independientemente;
- conexión, conectando al usuario con el operador de telecomunicaciones (es decir, con el proveedor de infraestructura/servicios/aplicaciones); y
- información transferida y almacenada en las instalaciones explotadas por los suministradores de infraestructura/servicios/aplicaciones.

**A.2** La red de telecomunicaciones no incluye el término "sistemas de terminal de usuario". Tales sistemas contienen:

- terminales de abonado en telecomunicaciones (junto con su software para llevar a cabo las funciones de un usuario de infraestructura, un usuario de servicio y un usuario de aplicaciones, incluida la ejecución de ciertas funciones locales; por ejemplo, preparación y edición de mensajes);
- servidores de aplicación, si el usuario realiza las funciones de un proveedor de servicios de aplicación externo a la estructura de red;
- una red empresarial/local/doméstica (si está presente);
- un cortafuegos/pasarela (si está presente); y
- información de usuario, transmitida, recibida y almacenada.

## Bibliografía

- [b-UIT-T E.409] Recomendación UIT-T E.409 (2004), *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones.*
- [b-UIT-T X.1051] Recomendación UIT-T X.1051 (2008) | ISO/CEI 27011:2008, *Tecnología de la información – Técnicas de seguridad – Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones.*
- [b-UIT-T X.1056] Recomendación UIT-T X.1056 (2009), *Directrices para la gestión de incidentes de seguridad en organizaciones de telecomunicaciones.*





## 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
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
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