UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.805

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(10/2003)

SERIE X: REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

Seguridad

Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

Recomendación UIT-T X.805

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1–X.19
Interfaces	X.20–X.49
Transmisión, señalización y conmutación	X.50–X.89
Aspectos de redes	X.90–X.149
Mantenimiento	X.150–X.179
Disposiciones administrativas	X.180–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200–X.209
Definiciones de los servicios	X.210–X.219
Especificaciones de los protocolos en modo conexión	X.220–X.229
Especificaciones de los protocolos en modo sin conexión	X.230–X.239
Formularios para declaraciones de conformidad de implementación de protocolo	X.240–X.259
Identificación de protocolos	X.260–X.269
Protocolos de seguridad	X.270–X.279
Objetos gestionados de capa	X.280–X.289
Pruebas de conformidad	X.290–X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300–X.349
Sistemas de transmisión de datos por satélite	X.350–X.369
Redes basadas en el protocolo Internet	X.370–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	
Gestión de redes	X.600–X.629
Eficacia	X.630–X.639
Calidad de servicio	X.640–X.649
Denominación, direccionamiento y registro	X.650–X.679
Notación de sintaxis abstracta uno	X.680–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Marco y arquitectura de la gestión de sistemas	X.700–X.709
Servicio y protocolo de comunicación de gestión	X.710–X.719
Estructura de la información de gestión	X.720–X.729
Funciones de gestión y funciones de arquitectura de gestión distribuida abierta	X.730–X.799
SEGURIDAD	**X.800–X.849**
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Compromiso, concurrencia y recuperación	X.850–X.859
Procesamiento de transacciones	X.860–X.879
Operaciones a distancia	X.880–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999

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

Recomendación UIT-T X.805

Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

Resumen

En esta Recomendación se definen los elementos de seguridad generales de la arquitectura, que pueden garantizar la seguridad de red extremo a extremo si son empleados correctamente.

Orígenes

La Recomendación UIT-T X.805 fue aprobada el 29 de octubre de 2003 por la Comisión de Estudio 17 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) 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.

ÍNDICE

Introducción

Las industrias de las telecomunicaciones y las tecnologías de la información necesitan soluciones de seguridad completas y rentables. Para ofrecer una red segura es necesaria una protección contra ataques malintencionados o imprevistos, y garantizar condiciones de alta disponibilidad, tiempo de respuesta apropiado, fiabilidad, integridad y adaptación a otra escala, y también proporcionar información exacta para facturación. Las capacidades de seguridad en los productos son esenciales para la seguridad general de la red (que incluye las aplicaciones y los servicios). Ahora bien, ha aumentado el número de productos que se combinan para ofrecer una solución global, y la compatibilidad entre productos determinará si la solución es satisfactoria. No es suficiente considerar la seguridad separadamente para cada producto o servicio, más bien como una combinación de capacidades de seguridad en la solución extremo a extremo global. La integración de distintos proveedores exige una norma de arquitectura de seguridad de red para lograr una solución satisfactoria.

Recomendación UIT-T X.805

Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo

1 Alcance

Esta Recomendación define una arquitectura de seguridad de red que garantiza la seguridad de comunicaciones extremo a extremo. Esta arquitectura puede aplicarse a distintas clases de redes en las que hay que garantizar la seguridad extremo a extremo, siendo indiferente la tecnología de red subyacente. En esta Recomendación se definen los elementos de seguridad generales de la arquitectura que son necesarios para garantizar la seguridad extremo a extremo. El objetivo es hacer de esta Recomendación una base para redactar Recomendaciones detalladas para la seguridad de red extremo a extremo.

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. Las ediciones indicadas estaban en vigor en la fecha de publicación. Los usuarios deben tener presente que todas las Recomendaciones y otras referencias son objeto de revisiones, y deben comprobar si es pertinente aplicar 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.

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

3 Términos y definiciones

En esta Recomendación se utilizan los siguientes términos de la Rec. UIT-T X.800:

– control de acceso;
– disponibilidad;
– autenticación;
– confidencialidad;
– integridad de los datos;
– no repudio;
– privacidad.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

AAA Autenticación, autorización y contabilidad (*authentication, authorization and accounting)*

ASP Proveedor de servicio de aplicación *(application service provider)*

ATM Modo de transferencia asíncrono *(asynchronous transfer mode)*

DHCP Protocolo dinámico de configuración de anfitrión *(dynamic host configuration protocol)*

DNS Servicio de nombres de dominio *(domain name service)*

DoS Denegación de servicio *(denial of service)*

DS-3 Señal digital de nivel 3 *(digital signal level 3)*

FTP Protocolo de transferencia de ficheros *(file transfer protocol)*

IP Protocolo Internet *(Internet protocol)*

IPSec Protocolo de seguridad IP *(IP security protocol)*

OAM&P Operaciones, administración, mantenimiento y configuración *(operations, administration, maintenance & provisioning)*

OSI Interconexión de sistemas abiertos *(open systems interconnection)*

PVC Circuito virtual permanente *(permanent virtual circuit)*

QoS Calidad de servicio *(quality of service)*

RPV Red privada virtual

RTPC Red telefónica pública conmutada

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

SMTP Protocolo de transferencia de correo simple *(simple mail transfer protocol)*

SNMP Protocolo de gestión de red simple *(simple network management protocol)*

SONET Red óptica síncrona *(synchronous optical network)*

SS7 Sistema de señalización N.º 7 *(signalling system No. 7)*

SSL Capa de zócalo segura (protocolo de criptación y autenticación [*secure socket layer (encryption and authentication protocol)*]

VoIP Voz sobre el protocolo Internet *(voice over IP)*

5 Arquitectura de seguridad

La arquitectura de seguridad responde a las exigencias generales de seguridad de los proveedores de servicio, las empresas y los consumidores, y es válida para redes de voz, de datos y convergentes de tecnología inalámbrica, óptica o de cable. Esta arquitectura de seguridad integra las consideraciones de gestión, control y utilización de la infraestructura, los servicios y las aplicaciones de red. La arquitectura de seguridad proporciona una visión global, de arriba abajo y extremo a extremo, de la seguridad de red y puede aplicarse a elementos de red, servicios y aplicaciones para detectar, estimar y remediar vulnerabilidades de seguridad.

La arquitectura de seguridad divide lógicamente una serie compleja de características de seguridad de red extremo a extremo, en distintos componentes de arquitectura. Esta segmentación permite considerar la seguridad de extremo a extremo de forma sistemática, lo que permite planificar nuevas soluciones de seguridad y evaluar la seguridad de las redes actuales.

La arquitectura de seguridad integra tres consideraciones esenciales para la seguridad extremo a extremo:

1) ¿Qué tipo de protección se necesita, y contra qué amenazas?

2) ¿Cuáles son los diferentes conjuntos de equipos e instalaciones de red que es necesario proteger?

3) ¿Cuáles son las diferentes actividades de red que es necesario proteger?

Para responder a estas preguntas hay que considerar tres componentes de la arquitectura: dimensiones de seguridad, capas de seguridad y planos de seguridad.

Los principios descritos por la arquitectura de seguridad se pueden aplicar a una gran diversidad de redes, siendo indiferente la tecnología de red y la posición en la jerarquía de protocolos.

En las siguientes cláusulas se describen en detalle los elementos de la arquitectura y sus funciones frente a las principales amenazas para la seguridad.

6 Dimensiones de seguridad

Una dimensión de seguridad es un conjunto de medidas de seguridad que responden a un determinado aspecto de la seguridad de red. En esta Recomendación se identifican ocho conjuntos de medidas contra las principales amenazas. Las dimensiones de seguridad incluyen la red, las aplicaciones y la información de usuario de extremo. Además, se aplican a los proveedores de servicio y las empresas que ofrecen servicios de seguridad a sus clientes. Estas son las dimensiones de seguridad:

1) control de acceso;
2) autenticación;
3) no repudio;
4) confidencialidad de datos;
5) seguridad de la comunicación;
6) integridad de los datos;
7) disponibilidad;
8) privacidad.

Las dimensiones de seguridad definidas e implementadas correctamente soportan la política de seguridad definida para una determinada red y facilitan la aplicación de las normas de gestión de la seguridad.

6.1 Dimensión de seguridad control de acceso

La dimensión de seguridad control de acceso protege contra la utilización de recursos de red sin autorización. El control de acceso garantiza que sólo las personas y los dispositivos autorizados pueden acceder a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Además, el control de acceso basado en las funciones (RBAC, *role-based access control*) establece varios niveles para restringir el acceso a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones, a las personas y los dispositivos autorizados.

6.2 Dimensión de seguridad autenticación

La dimensión de seguridad autenticación se utiliza para confirmar la identidad de las entidades comunicantes. La autenticación garantiza la validez de la identidad que se atribuyen las entidades de una comunicación (por ejemplo, personas, dispositivos, servicios o aplicaciones) y que una entidad no interviene usurpando una identidad o reproduciendo una comunicación anterior sin autorización.

6.3 Dimensión de seguridad no repudio

La dimensión de seguridad no repudio evita que una persona o una entidad niegue que ha realizado una acción de tratamiento de datos, proporcionando la prueba de distintas acciones de red (por ejemplo, de obligación, de intención o de compromiso; prueba de origen de los datos; prueba de

propiedad; prueba de utilización del recurso). Garantiza la disponibilidad de pruebas que se pueden presentar a terceros y utilizar para demostrar que un determinado evento o acción sí ha tenido lugar.

6.4 Dimensión de seguridad confidencialidad de los datos

La dimensión de seguridad confidencialidad de los datos impide que los datos sean divulgados sin autorización. La confidencialidad garantiza que las entidades no autorizadas no pueden entender el contenido de datos. Los métodos utilizados habitualmente son la criptación, las listas de control de acceso o las autorizaciones de archivos.

6.5 Dimensión de seguridad seguridad de la comunicación

La dimensión de seguridad de la comunicación garantiza que la información sólo circula entre los puntos extremo autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremo).

6.6 Dimensión de seguridad integridad de los datos

La dimensión de seguridad integridad de los datos garantiza la exactitud y la veracidad de los datos. Protege los datos contra acciones no autorizadas de modificación, supresión, creación o reactuación, y señala estas acciones no autorizadas.

6.7 Dimensión de seguridad disponibilidad

La dimensión de seguridad disponibilidad garantiza que las circunstancias de la red no impiden el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones. Esta categoría incluye soluciones para recuperación en caso de anomalía.

6.8 Dimensión de seguridad privacidad

La dimensión de seguridad privacidad protege la información que sería posible conocer observando las actividades de la red. Por ejemplo: los sitios web visitados por un usuario, la posición geográfica del usuario y las direcciones IP y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio.

7 Capas de seguridad

Para realizar una solución de seguridad extremo a extremo es necesario aplicar las dimensiones de seguridad descritas en la claúsula 6 a una jerarquía de equipos de red y dispositivos: las capas de seguridad. En esta Recomendación se definen tres capas de seguridad:

– capa de seguridad de infraestructura;
– capa de seguridad de servicios; y
– capa de seguridad de aplicaciones;

que se complementan mutuamente para realizar soluciones de red.

Las capas de seguridad son sistemas de potenciación que permiten realizar soluciones de red seguras: la capa infraestructura potencia la capa servicios, y ésta potencia la capa aplicaciones. La arquitectura de seguridad tiene en cuenta que las vulnerabilidades de seguridad de cada capa son diferentes, y ofrece la flexibilidad necesaria para reaccionar a las posibles amenazas de la forma más apropiada para una determinada capa de seguridad.

Obsérvese que estas capas de seguridad constituyen una categoría aparte, y las tres capas de seguridad se pueden aplicar a cada capa del modelo de referencia OSI.

El sistema de capas proporciona una perspectiva secuencial de la seguridad de red, que determina dónde hay que intervenir para la seguridad en los productos y las soluciones. Por ejemplo, inicialmente se tratan las vulnerabilidades de seguridad en la capa de infraestructura, luego en la capa de servicios y finalmente en la capa de aplicaciones. En la figura 1 se ha representado la aplicación de las dimensiones de seguridad a las capas de seguridad para limitar las vulnerabilidades de cada una y así controlar los ataques contra la seguridad.

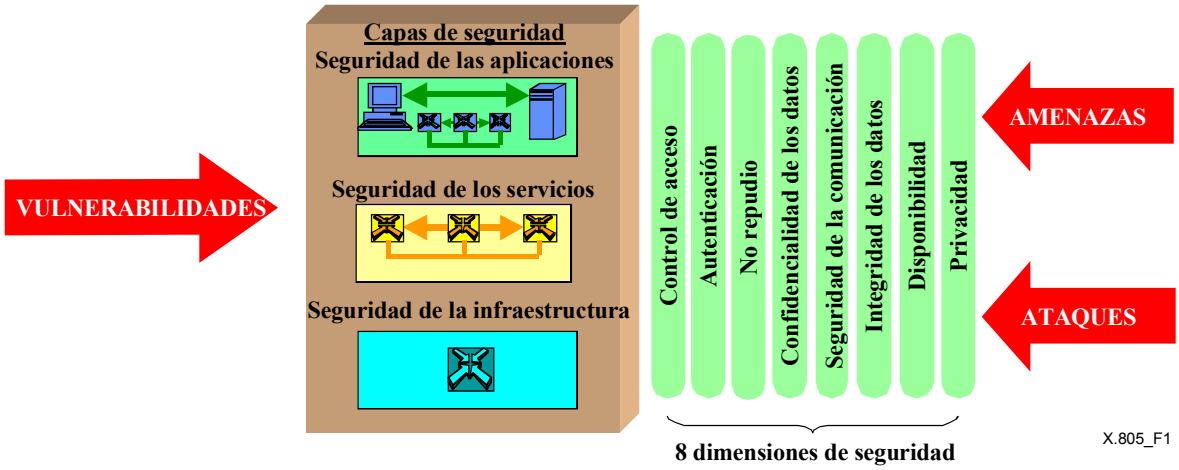


Figura 1/X.805 – Aplicación de las dimensiones de seguridad a las capas de seguridad

7.1 Capa de seguridad infraestructura

La capa de seguridad infraestructura comprende los dispositivos de transmisión de la red y los elementos de red que están protegidos por las dimensiones de seguridad. La capa infraestructura constituye la base fundamental de las redes, sus servicios y aplicaciones. Los componentes de esta capa son, por ejemplo, los encaminadores, los centros de conmutación y los servidores, así como los enlaces de comunicación entre estos encaminadores, centros de conmutación y servidores.

7.2 Capa de seguridad servicios

La capa de seguridad servicios tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes: desde servicios básicos de transporte y conectividad, hasta plataformas potenciadoras para el acceso a Internet (servicios AAA, servicios de dinámicos de configuración de anfitrión, servicios de nombre de dominio, etc.), o servicios de valor añadido como la telefonía gratuita, QoS, RPV, servicios de geodeterminación, mensajería instantánea, etc. La capa de seguridad servicios se utiliza para proteger a los proveedores de servicio y a sus clientes, que están expuestos unos y otros a amenazas contra la seguridad. Por ejemplo, alguien puede tratar de impedir que el proveedor preste los servicios, o tratar de interrumpir el servicio que se presta a un determinado cliente del proveedor (una empresa por ejemplo).

7.3 Capa de seguridad aplicaciones

La capa de seguridad aplicaciones tiene que ver con la seguridad de las aplicaciones de red a las que acceden los clientes de proveedores de servicios. Son aplicaciones potenciadas por servicios de red: aplicaciones básicas de transporte de ficheros (por ejemplo FTP) y de navegación web, aplicaciones fundamentales como la asistencia de directorio, mensajería vocal en red y correo electrónico, y también las aplicaciones más elaboradas, como la gestión de relaciones con los clientes, comercio electrónico o móvil, formación en red, colaboración en vídeo, etc. Las aplicaciones de red pueden ser productos de terceros: proveedores de servicio de aplicaciones (ASP), proveedores de servicios

que intervienen como ASP o empresas que los albergan en centros de datos propios o alquilados. Hay cuatro objetivos de ataques contra la seguridad en esta capa: el usuario de la aplicación, el proveedor de la aplicación, los programas intermedios de terceros que intervienen como integradores (por ejemplo, servicios de albergue en la web) y el proveedor del servicio.

8 Planos de seguridad

Un plano de seguridad es una determinada actividad de red protegida por dimensiones de seguridad. En esta Recomendación se definen tres planos de seguridad que representan los tres tipos de actividades protegidas realizadas en la red:

1) el plano de gestión,

2) el plano de control; y

3) el plano usuario de extremo.

Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como las actividades de usuario de extremo correspondientes.

Es importante que el sistema de red separe totalmente los eventos de dos planos de seguridad. Por ejemplo, una gran cantidad de consultas de DNS en el plano usuario de extremo, iniciadas por peticiones de usuarios, no debería bloquear la interfaz OAM&P en el plano de gestión, para que el gestor pueda resolver el problema.

En la figura 2 se representa la arquitectura de seguridad con sus planos de seguridad. Cada actividad de red tiene necesidades de seguridad particulares. El concepto de planos de seguridad permite distinguir los riesgos de seguridad de cada actividad y tratarlos separadamente. Considérese el caso de un servicio de VoIP, incluido en la capa de seguridad servicios. La gestión del servicio VoIP (por ejemplo la configuración de usuarios) tiene que ser independiente del control del servicio (por ejemplo, protocolos como SIP) y también de la seguridad de los datos del usuario de extremo transportados por el servicio (por ejemplo, voz de usuario).

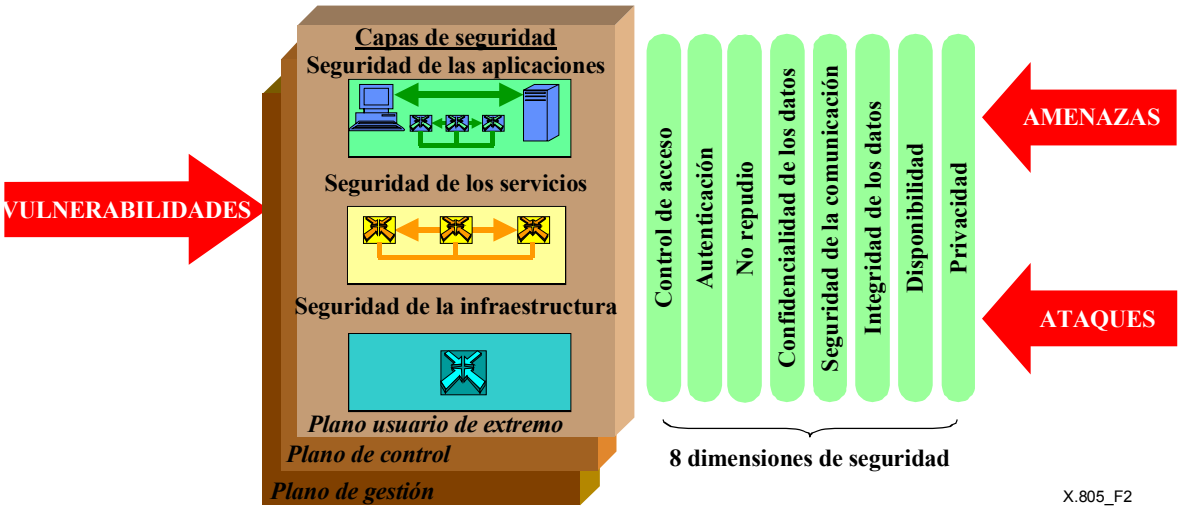


Figura 2/X.805 – Los planos de seguridad reflejan las distintas actividades de red

8.1 Plano de seguridad gestión

El plano de seguridad gestión tiene que ver con la protección de las funciones OAM&P de elementos de red, dispositivos de transmisión, sistemas administrativos (soporte de operaciones, soporte comercial, atención de clientes, etc.) y centros de datos. El plano de gestión soporta las funciones FCAPS (anomalía, capacidad, administración, configuración y seguridad). Obsérvese que

el tráfico para estas actividades puede transportarse en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio.

8.2 Plano de seguridad control

El plano de seguridad control tiene que ver con la protección de las actividades que permiten una distribución eficiente de información, servicios y aplicaciones en la red. Generalmente consiste en la comunicación máquina a máquina de información (por ejemplo centros de conmutación o encaminadores) que permite determinar la mejor forma de encaminar o conmutar el tráfico en la red de transporte subyacente. Se habla de información de control o información de señalización. Estos mensajes se pueden transportar en la red dentro o fuera de la banda, con respecto al tráfico de usuario del proveedor de servicio. Por ejemplo, las redes IP transportan la información de control dentro de la banda, pero las redes RTPC lo hacen fuera de banda, en una red de señalización separada (la red SS7). Los protocolos de encaminamiento, DNS, SIP, SS7, Megaco/H.248, etc., son ejemplos de este tráfico.

8.3 Plano de seguridad usuario de extremo

El plano de seguridad usuario de extremo tiene que ver con la seguridad cuando los clientes acceden y utilizan la red del proveedor de servicio. En este plano también se incluyen flujos de datos efectivos del usuario de extremo. El usuario de extremo puede utilizar una red que sólo proporciona conectividad, puede utilizar redes para servicios de valor añadido como las RPV, o redes para acceder a aplicaciones de red.

9 Amenazas contra la seguridad

La arquitectura de seguridad establece un plan y un conjunto de principios que constituyen una estructura de seguridad para la solución de seguridad extremo a extremo. La arquitectura identifica elementos de seguridad a considerar para evitar amenazas intencionales y accidentales. Las siguientes amenazas están definidas en la Rec. UIT-T X.800 (1991), *Arquitectura de seguridad para la interconexión de sistemas abiertos para aplicaciones del CCITT*:

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

La intersección de cada capa de seguridad y cada plano de seguridad determina una perspectiva en la que se aplican dimensiones de seguridad para contrarrestar amenazas. En el cuadro 1 se indican las dimensiones de seguridad para las distintas amenazas, siendo esta relación válida para todas las perspectivas de seguridad.

Si la letra 'Y' aparece en la casilla de intersección entre una columna y una fila del cuadro, esa dimensión de seguridad es apropiada para contrarrestar esa amenaza contra la seguridad.

Cuadro 1/X.805 – Las dimensiones de seguridad que corresponden a las amenazas

Dimensiones de seguridad	Amenazas contra la seguridad				
	Destrucción de información y otros recursos	Corrupción o modificación de información	Robo, supresión o pérdida de información y de otros recursos	Revelación de información	Interrupción de servicios
Control de acceso	Y	Y	Y	Y	
Autenticación			Y	Y	
No repudio	Y	Y	Y	Y	Y
Confidencialidad de datos			Y	Y	
Seguridad de la comunicación			Y	Y	
Integridad de los datos	Y	Y			
Disponibilidad	Y				Y
Privacidad				Y	

En la figura 3 se representa la arquitectura de seguridad con los distintos elementos y las amenazas contra la seguridad descritas anteriormente. Se ha representado el concepto de protección de una red mediante dimensiones de seguridad en cada plano de seguridad de cada capa de seguridad, para realizar una solución global. Obsérvese que en algunos casos será necesario implementar todos los elementos de la arquitectura (el conjunto completo de dimensiones de seguridad, capas de seguridad y planos de seguridad), según las condiciones de seguridad particulares de la red.

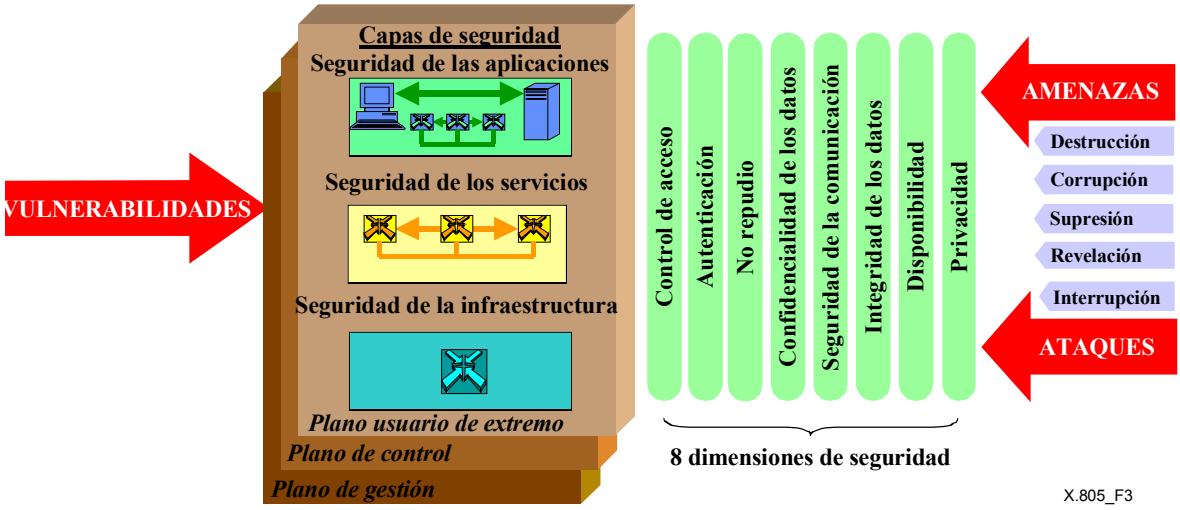


Figura 3/X.805 – Arquitectura para la seguridad de red extremo a extremo

10 Objetivos que se consiguen aplicando dimensiones de seguridad a las capas de seguridad

La arquitectura de seguridad se puede aplicar a todos los aspectos y las etapas de un programa de seguridad (véase la figura 4). Como puede verse, un programa de seguridad comprende políticas, procedimientos y tecnología, y se desarrolla en tres etapas:

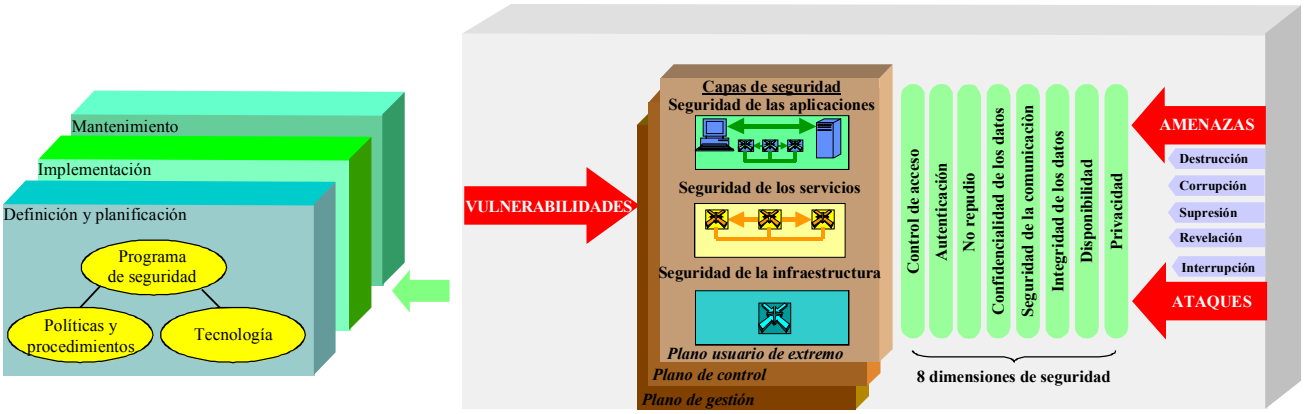
1) etapa de definición y planificación;

2) etapa de implementación; y

3) etapa de mantenimiento.

La arquitectura de seguridad puede aplicarse a las políticas y los procedimientos de seguridad, y también a la tecnología, en las tres etapas de un programa de seguridad

La arquitectura de seguridad puede servir de orientación para definir políticas de seguridad globales, planes de reacción a incidentes y recuperación, o arquitecturas de tecnología, integrando todas las dimensiones de seguridad en todas las capas y planos de seguridad durante la definición y la planificación. La arquitectura de seguridad también puede ser la base de una evaluación de seguridad, para analizar el efecto del programa de seguridad en las dimensiones, las capas y los planos de seguridad, cuando se realizan las políticas y los procedimientos, y se implanta la tecnología. La constante evolución del entorno de seguridad exige un mantenimiento para actualizar los programas de seguridad implantados. La arquitectura de seguridad puede facilitar la gestión de políticas y procedimientos de seguridad, planes de reacción a incidentes y recuperación, o arquitecturas de tecnología, porque permite comprobar si las modificaciones del programa de seguridad son apropiadas para cada dimensión de seguridad en las distintas capas y planos de seguridad.



X.805_F4

Figura 4/X.805 – Aplicación de la arquitectura de seguridad a los programas de seguridad

De otra parte, la arquitectura de seguridad se puede aplicar a cualquier tipo de red en todos los niveles de la jerarquía de protocolos. Por ejemplo, en la red IP que reside en la capa 3 de la jerarquía de protocolos, la capa infraestructura comprende los encaminadores, los enlaces de comunicación punto a punto entre encaminadores (SONET, ATM PVCs, etc.) y las plataformas de servidor que proporcionan los servicios de soporte necesarios en una red IP. La capa servicios comprende el servicio IP básico propiamente dicho (por ejemplo, conectividad Internet), los servicios de soporte IP (AAA, DNS, DHCP, etc.) y los servicios avanzados de valor añadido que ofrece el proveedor de servicio (VoIP, QoS, RPV, etc.). La capa aplicaciones tiene que ver con la seguridad de aplicaciones de usuario a las que se accede a través de la red IP (por ejemplo, correo electrónico).

En el caso de una red ATM, que reside en la capa 2 de la jerarquía de protocolos, la capa infraestructura comprende los centros de conmutación y los enlaces de comunicación punto a punto entre estos centros de conmutación (dispositivos portadores, por ejemplo DS-3). La capa servicios comprende los distintos tipos de transporte del sistema ATM (velocidad binaria constante, velocidad binaria variable – en tiempo real o no – velocidad binaria disponible y velocidad binaria no especificada). La capa aplicaciones tiene que ver con las aplicaciones a las que el usuario de extremo accede a través de la ATM, por ejemplo videoconferencias.

La figura 5 es una representación de la arquitectura de seguridad en forma de cuadro, que constituye un análisis metódico de la seguridad de una red. Como puede verse, la intersección de cada capa de seguridad y cada plano de seguridad determina una perspectiva única para considerar las ocho dimensiones de seguridad. Cada uno de los nueve módulos combina las ocho dimensiones de seguridad, que se aplican a una determinada capa en un determinado plano de seguridad. Téngase presente que las dimensiones de seguridad de cada módulo tienen objetivos diferentes, y por tanto suponen medidas de seguridad diferentes. La representación en un cuadro es práctica para describir los objetivos de las dimensiones de seguridad para cada módulo.

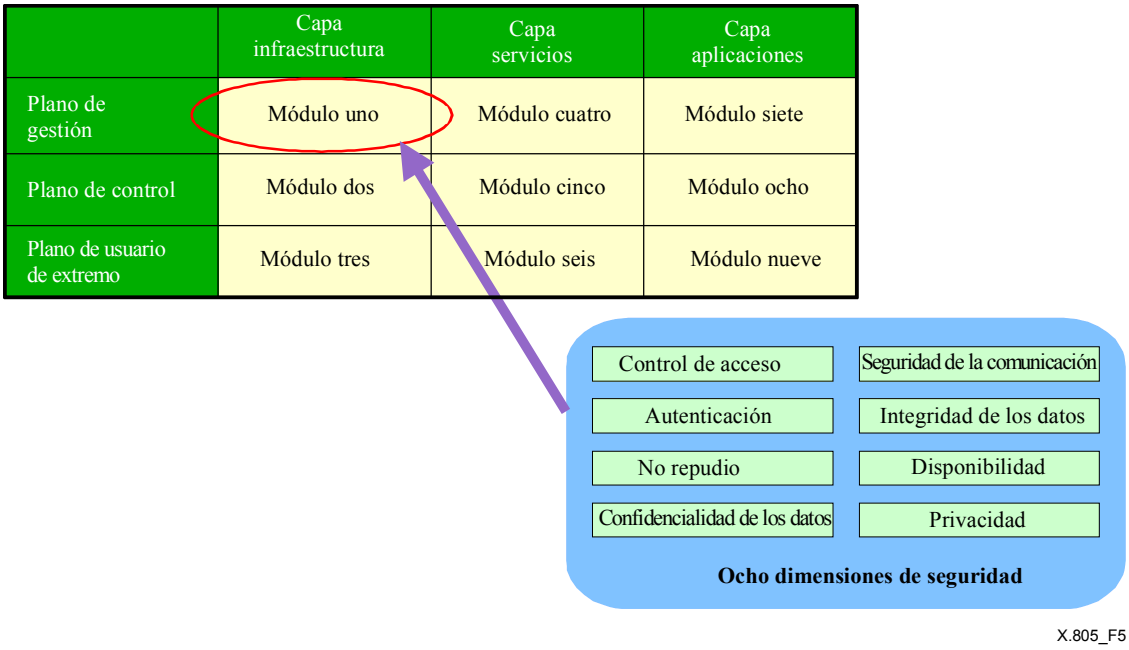


Figura 5/X.805 – La arquitectura de seguridad representada en un cuadro

10.1 Garantizar la seguridad de la capa infraestructura

10.1.1 En la capa infraestructura, las medidas de seguridad del plano gestión consisten en garantizar la seguridad de operaciones, administración, mantenimiento y configuración (OAM&P) de los distintos elementos de red, los enlaces de comunicaciones y las plataformas de servidor que constituyen la red. Se considera que la configuración de los dispositivos de red y los enlaces de comunicaciones también es una actividad de gestión. La intervención de personal de explotación para configurar un encaminador o un centro de conmutación es un ejemplo de gestión de infraestructura que es necesario proteger. En el cuadro 2 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa infraestructura en el plano de gestión.

Cuadro 2/X.805 – Aplicación de las dimensiones de seguridad a la capa infraestructura en el plano de gestión

Módulo 1: capa infraestructura, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados (por ejemplo dispositivos gestionados por protocolo SNMP) son los únicos que pueden realizar actividades de gestión o administración en el dispositivo de red o el enlace de comunicaciones. Se aplica por igual a la gestión directa desde un puerto de configuración y la gestión del dispositivo a distancia.
Autenticación	Verificar la identidad de la persona o el dispositivo que realizan la actividad de gestión o administrativa en el dispositivo de red o el enlace de comunicaciones. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa en el dispositivo de red o el enlace de comunicaciones, y la acción realizada. Este registro puede utilizarse para probar quién ha originado la actividad de gestión o administrativa .
Confidencialidad de los datos	Proteger la información de configuración del dispositivo de red o el enlace de comunicaciones contra el acceso o la consulta no autorizados. Se aplica a la información de configuración que reside en el dispositivo de red o el enlace de comunicaciones, la información de configuración que se transmite al dispositivo de red o el enlace de comunicaciones, y la información de configuración duplicada para seguridad y almacenada en sistemas no conectados. Proteger la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador) contra el acceso o la consulta no autorizados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de datos.
Seguridad de la comunicación	En el caso de la gestión a distancia de un dispositivo de red o un enlace de comunicaciones, garantizar que la información de gestión sólo circula entre las estaciones de gestión distantes y los dispositivos o enlaces de comunicaciones gestionados. La información de gestión no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Integridad de los datos	Proteger la información de configuración de dispositivos de red o enlaces de comunicaciones contra la modificación, la supresión, la creación y la reactuación sin autorización. Se aplica a la información de configuración que reside en el dispositivo de red o el enlace de comunicaciones, y también la información de configuración que está en tránsito o almacenada en sistemas no conectados. Se incluye en esta protección la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan gestionar el dispositivo de red o el enlace de comunicaciones. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información administrativa de autenticación (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar el dispositivo de red o el enlace de comunicaciones no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar un dispositivo de red permite, por ejemplo, dirigir un ataque.

10.1.2 Proteger el plano control de la capa infraestructura consiste en garantizar la seguridad de la información de control o señalización que reside en los elementos de red y las plataformas de servidor que constituyen la red, y la seguridad de recepción y transmisión de información de control o señalización por los elementos de red y las plataformas de servidor. Por ejemplo, es necesario proteger los cuadros de conmutación residentes en centros de conmutación de la red, contra la alteración o la divulgación no autorizadas. También hay que garantizar que los encaminadores no

reciben ni propagan actualizaciones de encaminamiento falsas, y que no responden a falsas solicitudes de encaminamiento de un encaminador falsificado. En el cuadro 3 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa infraestructura en el plano de control.

Cuadro 3/X.805 – Aplicación de las dimensiones de seguridad a la capa infraestructura en el plano de control

Módulo 2 – Capa infraestructura, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a la información de control que reside en el dispositivo de red (por ejemplo, un cuadro de encaminamiento) o está almacenada en un dispositivo no conectado. Garantizar que el dispositivo de red sólo aceptará mensajes de información de control de dispositivos de red autorizados (por ejemplo, actualizaciones de encaminamiento).
Autenticación	Verificar la identidad de la persona o el dispositivo que observan o modifican información de control residente en el dispositivo de red. Verificar la identidad del dispositivo que envía información de control a un dispositivo de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que han observado o modificado información de control en el dispositivo de red, y la acción realizada. Este registro puede utilizarse como prueba de acceso a la información de control o modificación de esa información. Crear un registro de los dispositivos emisores de mensajes de control enviados al dispositivo de red, y la acción realizada. Este registro puede utilizarse para probar que el dispositivo es el emisor del mensaje de control.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control residente en un dispositivo de red o un sistema de almacenamiento no conectado. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red. Proteger la información de control destinada a un dispositivo de red contra el acceso o la consulta no autorizados durante el transporte por la red.
Seguridad de la comunicación	Garantizar que la información de control transportada por la red (por ejemplo, actualización de encaminamiento) sólo circula entre la fuente de esa información y el destino especificado. La información de control no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger la información de control que reside en los dispositivos de red, que está en tránsito por la red o almacenada fuera de línea, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que los dispositivos de red están siempre disponibles para recibir información de control de las fuentes autorizadas, lo que incluye una protección contra ataques deliberados como la denegación de servicio (DoS) y contra situaciones accidentales como el cambio rápido de rutas.
Privacidad	Garantizar que la información que permite identificar el dispositivo de red o el enlace de comunicaciones no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar dispositivos de red o enlaces de comunicaciones permite, por ejemplo, dirigir un ataque.

10.1.3 Proteger el plano usuario de extremo de la capa infraestructura consiste en garantizar la seguridad de los datos y la voz de usuario que residen en elementos de red, que están en tránsito entre ellos y durante el transporte entre enlaces de comunicación. Es necesario proteger los datos de usuario que residen en plataformas de servidor, y protegerlos también contra la interceptación ilícita durante el transporte entre elementos de red o por enlaces de comunicación. En el cuadro 4 se

indican los objetivos de la aplicación de dimensiones de seguridad a la capa infraestructura en el plano usuario de extremo.

Cuadro 4/X.805 – Aplicación de las dimensiones de seguridad a la capa infraestructura en el plano usuario de extremo

Módulo 3: capa infraestructura, plano de usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado.
Autenticación	Verificar la identidad de la persona o el dispositivo que intentan acceder a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que han accedido a los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, y la acción realizada. Este registro puede utilizarse como prueba de acceso a los datos de usuario de extremo.
Confidencialidad de los datos	Proteger los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, contra el acceso o la consulta no autorizados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación no son desviados ni interceptados entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal).
Integridad de los datos	Proteger los datos de usuario de extremo que transitan por un elemento de red o un enlace de comunicación, o que residen en un dispositivo no conectado, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que nada impedirá que las personas (incluyendo usuarios de extremo) y los dispositivos autorizados puedan acceder a los datos de usuario de extremo que residen en un dispositivo no conectado. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS) y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación (por ejemplo, identificación y contraseñas de usuario o de administrador).
Privacidad	Garantizar que los elementos de red no proporcionan información sobre las actividades del usuario de extremo en la red (por ejemplo, la posición geográfica del usuario o los sitios web visitados) a personas o dispositivos no autorizados.

10.2 Garantizar la seguridad de la capa servicios

Una dificultad adicional para garantizar la seguridad de esta capa es que los servicios se pueden formar unos a partir de otros, para satisfacer las necesidades del cliente. Por ejemplo, para ofrecer el servicio de VoIP, el proveedor debe proporcionar antes el servicio IP básico y los servicios de potenciación indispensables, como AAA, DHCP, DNS, etc. En algunos casos el proveedor del servicio tendrá que implantar un servicio de RPV para satisfacer las condiciones de QoS y seguridad de sus clientes para el servicio VoIP. Por eso es necesario considerar separadamente los servicios constitutivos para garantizar la seguridad global.

10.2.1 Las medidas de seguridad del plano gestión de la capa servicios consisten en garantizar la seguridad de operaciones, administración, mantenimiento y configuración (OAM&P) de los servicios de red. Se considera que la configuración de los servicios de red también es una actividad de gestión. La intervención de personal de explotación para dar de alta los usuarios autorizados de

un servicio IP es un ejemplo de gestión de servicios que es necesario proteger. En el cuadro 5 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa servicios en el plano de gestión.

Cuadro 5/X.805 – Aplicación de las dimensiones de seguridad a la capa servicios, plano de gestión

Módulo 4: capa servicios, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden realizar las actividades de gestión o administración del servicio de red (por ejemplo dar de alta los usuarios del servicio).
Autenticación	Verificar la identidad de las personas o los dispositivos que intentan realizar actividades de gestión o administración del servicio de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa del servicio de red, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha realizado la actividad de gestión o administrativa.
Confidencialidad de los datos	Proteger la información de configuración y gestión del servicio de red (por ejemplo, los valores del protocolo de seguridad IPSec de un cliente para un servicio RPV, que se pueden descargar) contra el acceso o la consulta no autorizados. Se aplica a la información de configuración y gestión que reside en dispositivos de red, que se transmite por la red o que está almacenada en sistemas no conectados. Proteger la información de gestión o administrativa del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador) contra el acceso o la consulta no autorizados.
Seguridad de la comunicación	En el caso de la gestión a distancia de un servicio de red, garantizar que la información de gestión o administrativa sólo circula entre la estación de gestión distante y los dispositivos gestionados en el contexto del servicio de red. La información de gestión y administrativa no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información de autenticación del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Integridad de los datos	Proteger la información de gestión y administrativa de los servicios de red contra la modificación, la supresión, la creación y la reactuación sin autorización. Se aplica a la información de gestión y administrativa que reside en dispositivos de red, que se transmite por la red o está almacenada en sistemas no conectados. Se incluye en esta protección la información de autenticación del servicio de red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan gestionar el servicio de red. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación administrativa del servicio de red (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar los sistemas de gestión o administrativos del servicio de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un sistema. La posibilidad de identificar los sistemas administrativos de un servicio de red permite, por ejemplo, dirigir un ataque.

10.2.2 Las medidas de seguridad del plano de control de la capa servicios consisten en proteger la información de control o señalización que se utiliza en el servicio de red. Por ejemplo, proteger el protocolo SIP que se utiliza para iniciar y mantener las sesiones de VoIP. En cuadro 6 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa servicios en el plano de control.

Cuadro 6/X.805 – Aplicación de las dimensiones de seguridad a la capa servicios, plano de control

Módulo 5: capa servicios, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que la información de control que recibe un dispositivo de red para un servicio de red proviene de una fuente autorizada (por ejemplo, mensaje de inicio de sesión VoIP emitido por un usuario o dispositivo autorizados) antes de aceptarla. En el caso de VoIP, proteger contra la falsificación del mensaje de inicio de sesión en un dispositivo no autorizado.
Autenticación	Verificar la identidad de la fuente de información de control del servicio de red enviada a dispositivos de red que participan en ese servicio. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que emiten los mensajes de control del servicio de red recibidos por un dispositivo de red que participa en ese servicio, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha emitido el mensaje de control del servicio de red.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control del servicio de red que reside en un dispositivo de red (por ejemplo, bases de datos de sesiones IPSec), transportada por la red o almacenada en sistemas no conectados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red, para un servicio de red.
Seguridad de la comunicación	Garantizar que la información transportada por la red para el control de un servicio de red (por ejemplo, mensajes de negociación de clave IPSec) sólo circula entre la fuente de esta información de control y el destino especificado. La información de control del servicio de red no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger contra la modificación, la supresión, la creación y la reactuación sin autorización, la información de control de un servicio de red que reside en dispositivos de red, que transita por la red o está almacenada en sistemas no conectados.
Disponibilidad	Garantizar que los dispositivos de red que participan en un servicio de red están siempre disponibles para recibir información de control de fuentes autorizadas. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS).
Privacidad	Garantizar que la información que permite identificar los dispositivos de red y los enlaces de comunicación que participan en un servicio de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar los dispositivos de red y los enlaces de comunicación permite, por ejemplo, dirigir un ataque.

10.2.3 Las medidas de seguridad del plano usuario de extremo en la capa servicios consisten en proteger los datos y la voz cuando el usuario utiliza el servicio de red. Por ejemplo, proteger la confidencialidad de la conversación de un usuario en un servicio VoIP. En el servicio DNS también hay que garantizar la confidencialidad de los usuarios. En el cuadro 7 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa servicios en el plano usuario de extremo.

Cuadro 7/X.805 – Aplicación de las dimensiones de seguridad a la capa servicios, plano usuario de extremo

Módulo 6: capa servicios, plano usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder al servicio de red y utilizarlo.
Autenticación	Verificar la identidad del usuario o el dispositivo que intentan acceder al servicio de red y utilizarlo. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas y los dispositivos que han tenido acceso y han utilizado el servicio de red, y la acción realizada. Este registro puede utilizarse para probar que el usuario de extremo o el dispositivo han accedido al servicio de red y lo han utilizado.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados los datos de usuario de extremo transportados, procesados o almacenados por un servicio de red. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo transportados, procesados o almacenados por un servicio de red no son desviados ni interceptados durante el transporte entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal).
Integridad de los datos	Proteger la información de usuario de extremo transportada, procesada o almacenada por un servicio de red, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que nada puede impedir el acceso al servicio de red a los usuarios de extremo y dispositivos autorizados. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación del usuario de extremo (por ejemplo, identificación y contraseñas de usuario).
Privacidad	Garantizar que el servicio de red no proporciona información sobre la utilización que hace el usuario de extremo (por ejemplo, partes llamadas en un servicio VoIP) a personas y dispositivos no autorizados.

10.3 Garantizar la seguridad de la capa aplicaciones

Las medidas de seguridad del plano gestión en la capa aplicaciones consisten en garantizar la seguridad de operaciones, administración, mantenimiento y configuración (OAM&P) de la aplicación de red. Se considera que la configuración de las aplicaciones de red también es una actividad de gestión. En el caso de una aplicación de correo electrónico una de las actividades de gestión a proteger sería la configuración y la administración de buzones de usuarios. En el cuadro 8 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa aplicaciones en el plano de gestión.

Cuadro 8/X.805 – Aplicación de las dimensiones de seguridad a la capa aplicaciones, plano de gestión

Módulo 7: capa aplicaciones, plano de gestión	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden realizar las actividades de gestión o administración de la aplicación de red (por ejemplo administrar buzones de usuarios en una aplicación de correo electrónico).
Autenticación	Verificar la identidad de las personas o los dispositivos que intentan realizar actividades de gestión o administración de la aplicación de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que realizan cada actividad de gestión o administrativa de la aplicación de red, y la acción realizada. Este registro puede utilizarse para probar esa persona o dispositivo ha realizado la actividad de gestión o administrativa.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados todos los ficheros que se utilizan para crear y ejecutar la aplicación de red (por ejemplo, ficheros fuente, de objetos, ejecutables o temporales, etc.) y los ficheros de configuración de la aplicación. Se aplica a los ficheros de la aplicación que residen en dispositivos de red, que se transmiten por la red o almacenados en sistemas no conectados. Proteger la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador) contra el acceso o la consulta no autorizados.
Seguridad de la comunicación	En el caso de la gestión o administración a distancia de una aplicación de red, garantizar que la información de gestión o administrativa sólo circula entre la estación de gestión distante y los dispositivos que constituyen la aplicación de red. La información de gestión y administrativa no será desviada ni interceptada entre estos puntos extremo. Se incluye en esta protección la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Integridad de los datos	Proteger todos los ficheros que se utilizan para crear y ejecutar la aplicación de red (por ejemplo, ficheros fuente, de objetos, ejecutables o temporales) y los ficheros de configuración de la aplicación, contra la modificación, la supresión, la creación y la reactuación sin autorización. Hay que proteger los ficheros de la aplicación que residen en dispositivos de red, que se transmiten por la red o que están almacenados en sistemas no conectados. Se incluye en esta protección la información de gestión o administrativa de la aplicación en la red (por ejemplo, identificación y contraseñas de usuario o de administrador).
Disponibilidad	Garantizar que nada impedirá que las personas y los dispositivos autorizados puedan administrar o gestionar la aplicación de red. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de información administrativa de autenticación para la aplicación en la red (por ejemplo, identificación y contraseñas de administrador).
Privacidad	Garantizar que la información que permite identificar los sistemas para administración o gestión de la aplicación de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un sistema. La posibilidad de identificar los sistemas administrativos de una aplicación de red permite, por ejemplo, dirigir un ataque.

10.3.1 Las medidas de seguridad del plano control de la capa aplicaciones consisten en proteger la información de control o señalización que se utiliza en las aplicaciones de red. Normalmente, la aplicación realiza una acción en respuesta a la información recibida. Se trata, por ejemplo, de la protección de protocolos SMTP y POP que se utilizan para controlar le distribución de correo electrónico. En el cuadro 9 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa aplicaciones en el plano de control.

Cuadro 9/X.805 – Aplicación de las dimensiones de seguridad a la capa aplicaciones, plano de control

Módulo 8: capa aplicaciones, plano de control	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que la información de control de la aplicación recibida en un dispositivo de red que participa en la aplicación de red proviene de una fuente autorizada, antes de aceptarla (por ejemplo, un mensaje SMTP que solicita la transferencia de correo electrónico). En algunos casos habrá que impedir que un dispositivo no autorizado falsifique un cliente SMTP.
Autenticación	Verificar la identidad de la fuente de información de control de la aplicación enviada a los dispositivos de red que participan en esa aplicación de red. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de las personas o dispositivos que emiten los mensajes de control de la aplicación recibidos por un dispositivo de red que participa en esa aplicación de red, y la acción realizada. Este registro puede utilizarse para probar que esa persona o dispositivo ha emitido el mensaje de control de la aplicación.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados la información de control de la aplicación que reside en un dispositivo de red (por ejemplo, bases de datos de sesiones SSL), que se transporta por la red o está almacenada en sistemas no conectados. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de la información de control que reside en el dispositivo de red, para una aplicación de red.
Seguridad de la comunicación	Garantizar que la información de control de la aplicación transportada por la red (por ejemplo, mensajes de negociación SSL) sólo circula entre la fuente de esta información de control y el destino especificado. La información de control de la aplicación de red no será desviada ni interceptada entre estos puntos extremo.
Integridad de los datos	Proteger la información de control de una aplicación de red residente en dispositivos de red, que transita por la red o que está almacenada en sistemas no conectados, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que los dispositivos de red que participan en una aplicación de red siempre están disponibles para recibir información de control de fuentes autorizadas. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS).
Privacidad	Garantizar que la información que permite identificar los dispositivos de red y los enlaces de comunicación que participan en una aplicación de red no está disponible para personas y dispositivos no autorizados. Son ejemplos de este tipo de información la dirección IP o el nombre de dominio DNS de un dispositivo de red. La posibilidad de identificar los dispositivos de red y los enlaces de comunicación permite, por ejemplo, dirigir un ataque.

10.3.2 Las medidas de seguridad del plano usuario de extremo en la capa aplicaciones consisten en proteger los datos de usuario proporcionados a una aplicación de red. Por ejemplo, proteger la confidencialidad del número de tarjeta de crédito del usuario en una aplicación de comercio electrónico. En el cuadro 10 se indican los objetivos de la aplicación de dimensiones de seguridad a la capa aplicaciones en el plano usuario de extremo.

Cuadro 10/X.805 – Aplicación de las dimensiones de seguridad a la capa aplicaciones, plano usuario de extremo

Módulo 9: capa aplicaciones, plano usuario de extremo	
Dimensiones de seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a la aplicación de red y utilizarla.
Autenticación	Verificar la identidad del usuario o el dispositivo que intentan acceder a la aplicación de red y utilizarla. Es posible que se incluyan técnicas de autenticación entre las condiciones de control de acceso.
No repudio	Crear un registro de los usuarios y los dispositivos que han tenido acceso y han utilizado la aplicación de red, y la acción realizada. Este registro puede utilizarse para probar que el usuario de extremo o el dispositivo han accedido a la aplicación de red y la han utilizado.
Confidencialidad de los datos	Proteger contra el acceso o la consulta no autorizados los datos de usuario de extremo transportados, procesados o almacenados por una aplicación de red (por ejemplo, el número de la tarjeta de crédito). Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación. Las técnicas que se utilizan para el control de acceso pueden contribuir a la confidencialidad de los datos de usuario de extremo.
Seguridad de la comunicación	Garantizar que los datos de usuario de extremo transportados, procesados o almacenados por una aplicación de red no son desviados ni interceptados durante el transporte entre estos puntos extremo sin una autorización de acceso (por ejemplo, interceptación legal). Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación.
Integridad de los datos	Proteger la información de usuario de extremo transportada, procesada o almacenada por una aplicación de red, contra la modificación, la supresión, la creación y la reactuación sin autorización. Se incluye la protección de los datos de usuario durante el transporte entre el usuario y la aplicación.
Disponibilidad	Garantizar que nada impedirá el acceso a la aplicación de red a los usuarios de extremo y los dispositivos autorizados. Incluye una protección contra ataques activos, por ejemplo de denegación de servicio (DoS), y contra ataques pasivos, por ejemplo la modificación o la supresión de la información de autenticación del usuario de extremo (por ejemplo, identificación y contraseñas de usuario).
Privacidad	Garantizar que la aplicación de red no proporciona información sobre la utilización que hace el usuario de extremo (sitios web visitados, etc.) a personas y dispositivos no autorizados. Por ejemplo, este tipo de información sólo será revelado a las autoridades competentes y con una orden de registro.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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 multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
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 X	**Redes de datos y comunicación entre sistemas abiertos**
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

Ginebra, 2004