Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1205

(04/2008)

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

Seguridad en el ciberespacio – Ciberseguridad

Aspectos generales de la ciberseguridad

Recomendación UIT-T X.1205

Unión Internacional de Telecomunicaciones

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
Seguridad de las redes	X.1030–X.1049
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

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

Recomendación UIT-T X.1205

Aspectos generales de la ciberseguridad

Resumen

La Recomendación UIT-T X.1205 ofrece una definición de ciberseguridad. En ella se expone la clasificación de las amenazas de seguridad desde el punto de vista de una organización. Se presentan las amenazas a la ciberseguridad, así como sus puntos débiles, incluidas las herramientas más utilizadas por los piratas informáticos. Se tratan las amenazas en las distintas capas de red.

Se exponen también diversas tecnologías de ciberseguridad disponibles para contrarrestar las amenazas, como pueden ser los encaminadores, los cortafuegos, la protección antivirus, los sistemas de detección de intrusión, los sistemas de protección contra intrusión, la computación segura y la auditoría y supervisión. Se exponen los principios de protección de la red, como la defensa en profundidad y la gestión de acceso aplicadas a la ciberseguridad. También se tratan las estrategias y técnicas de gestión de riesgos, incluido la importancia de la formación y la educación a la hora de proteger la red. Se presentan asimismo ejemplos de cómo se protegen diversas redes con las tecnologías presentadas.

Orígenes

La Recomendación UIT-T X.1205 fue aprobada el 18 de abril de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación UIT-T X.1205

Aspectos generales de la ciberseguridad

1 Alcance

En la cláusula 7 de la presente Recomendación figura una definición de ciberseguridad. Se proporciona una clasificación de las amenazas de seguridad desde el punto de vista de una organización.

NOTA – En la presente Recomendación, el término "identidad" no se usa en su sentido absoluto. En particular, no supone ninguna validación positiva.

En la cláusula 7 se debate acerca de la naturaleza del entorno de ciberseguridad de empresa, los riesgos de ciberseguridad y la seguridad de las comunicaciones de extremo a extremo. En la cláusula 8 se tratan las posibles estrategias de protección de la red, como la gestión de política de bucle cerrado y la gestión de acceso uniforme. En esta misma cláusula se tratan también las técnicas de comunicación segura, la seguridad de profundidad variable, la seguridad del plano de gestión, la seguridad por capas y la supervivencia de la red aun en caso de ataque.

En el apéndice I se expone la clasificación de las amenazas de seguridad, las herramientas de piratería informática y las amenazas de seguridad.

En el apéndice II se exponen las disciplinas de tecnologías de ciberseguridad, en particular la criptografía, las tecnologías de control de acceso, las técnicas de protección del perímetro, los sistemas antivirus y la integridad del sistema, la auditoría y la supervisión, así como la gestión.

En el apéndice III se presentan ejemplos de seguridad de red, entre los que se incluyen el acceso a distancia seguro, la seguridad de la telefonía IP, la seguridad de los clientes VoIP, la seguridad de la central distante y la seguridad de las WLAN.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una 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 de extremo a extremo*.

[UIT-T X.811] Recomendación UIT-T X.811 (1995), | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Marcos de seguridad para sistemas abiertos: Marco de autentificación*.

[UIT-T X.812] Recomendación UIT-T X.812 (1995), | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*.

[IETF RFC 1918] IETF RFC 1918 (1996), *Address Allocation for Private Internets* <http://www.ietf.org/rfc/rfc1918.txt?number=1918>.

[IETF RFC 2396] IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax* <http://www.ietf.org/rfc/rfc2396.txt?number=2396>.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 Esta Recomendación utiliza los siguientes términos definidos en [UIT-T X.800]:

a) Autorización

b) Arquitectura de seguridad.

c) Política de seguridad.

d) Usuario.

3.1.2 Esta Recomendación utiliza los siguientes términos definidos en [UIT-T X.805]:

a) Dimensión de seguridad.

b) Servicio de seguridad.

3.1.3 Esta Recomendación utiliza los siguientes términos definidos en [UIT-T X.811]:

a) Autentificación.

b) Principio.

3.1.4 Esta Recomendación utiliza los siguientes términos definidos en [UIT-T X.812]:

a) Información de control de acceso.

b) Acceso.

c) Control de acceso.

d) Usuario.

3.1.5 Esta Recomendación utiliza los siguientes términos definidos en [IETF RFC 2396]:

a) Identificador uniforme de recursos (URI, *uniform resource identifier*).

b) Referencia URI.

3.2 Términos definidos en la presente Recomendación

Esta Recomendación define los siguientes términos:

3.2.1 punto de acceso: Central inalámbrica IEEE 802.11, tipo especial de estación (STA, *station*) que funciona como un punto de acceso.

3.2.2 conjunto básico de servicios (BSS, *basic service set*): Zona de cobertura a la que da servicio un punto de acceso (AP, *access point*).

3.2.3 algoritmo criptográfico: Un algoritmo criptográfico es un medio mediante el cual se alteran los datos y se disimulan en la criptación.

3.2.4 ciberentorno: Esto incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

3.2.5 ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad.

3.2.6 sistema distribuido: Medio no normalizado de conectar un BSS con un ESS.

3.2.7 protocolo de autentificación extensible: Esta extensión PPP que soporta los métodos de autentificación adicionales forma parte de la especificación [b-IEEE 802.1X].

3.2.8 conjunto ampliado de servicios: Una única LAN inalámbrica con BSS en una única subred IP.

3.2.9 cortafuegos: Sistema o combinación de sistemas que establecen una frontera entre dos o más redes. Una pasarela que limita el acceso entre redes de acuerdo con la política de seguridad local.

3.2.10 agente extranjero: El encaminador de la red visitada/anfitriona que da servicio al nodo móvil mientras visita la red anfitriona. Este agente extranjero se encarga de la tunelización y entrega entre el nodo móvil y otros nodos, y entre la red propia móvil y la red anfitriona.

3.2.11 señuelo: Software que emula una red para atraer (y posiblemente confundir) a los intrusos y rastrear sus movimientos. Estos sistemas pueden utilizarse para inferir las intenciones de los intrusos y obtener pruebas.

3.2.12 agente propio: Encaminador que da servicio al nodo móvil mientras visita otras redes, manteniendo la información de ubicación actual del nodo móvil.

3.2.13 zonas de acceso (*hot spots*): Lugares públicos desde los que los usuarios móviles IEEE 802.11 pueden conectarse a Internet.

3.2.14 movilidad IP: Mecanismo que permite una conectividad más transparente para los modos móviles que "visitan" diversas subredes IP mientras transitan. Éste es un mecanismo para la gestión móvil de los nodos móviles de las redes alámbricas e inalámbricas.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siglas y los acrónimos siguientes:

3DES Norma de criptación de datos triple (*triple data encryption standard*)

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

ACL Lista de control de acceso (*access control list*)

AES Norma de criptación avanzada (*advanced encryption standard*)

AP Punto de acceso (*access point*)

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

BSS Conjunto básico de servicios (*basic service set*)

CA Autoridad de certificación (*certification authority*)

CMP Protocolo de gestión de certificados (*certificate management protocol*)

COPS Servicio de política común abierta (*common open policy service*)

CRL Lista de revocación de certificados (*certificate revocation list*)

DISA Acceso directo al sistema interno (*direct inward system access*)

DNS Sistema de nombre de dominio (*domain name system*)

EAP Protocolo de autentificación extensible (*extensible authentication protocol*)

EMS Sistema de gestión de elementos (*element management system*)

ESS Conjunto ampliado de servicios (*extended service set*)

ESSID Identificador del conjunto ampliado de servicios (*extended service set identifier*)

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

HMAC Función de aleatorización basada en MAC (*hash function based MACs*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

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

IKE Intercambio de claves Internet (*Internet key exchange*)

IP Protocolo Internet (*Internet protocol*)

IPSec Seguridad del protocolo Internet (*Internet protocol security*)

ISP Proveedor de servicios Internet (*Internet Service Provider*)

L2TP Protocolo de tunelización de capa 2 (*layer 2 tunneling protocol*)

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

MAC Código de autentificación de mensaje (*message authentication code*)

MD5 Algoritmo 5 de resumen de mensaje (*message digest algorithm 5*)

MIC Verificación de integridad del mensaje (*message integrity check*)

MIME Ampliaciones multifunción del correo Internet (*multipurpose Internet mail extensions*)

MPLS Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)

MU Unidad móvil (*mobile unit*)

NAT Traducción de dirección de red (*network address translation*)

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

NIC Tarjeta de interfaz de red (*network interface card*)

NOC Centro de operaciones de red (*network operations center*)

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

OCSP Protocolo de estado de certificado en línea (*online certificate status protocol*)

OS Sistema operativo (*operating system*)

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

PDP Punto de decisión de política (*policy decision point*)

PEAP	Protocolo EAP protegido (*protected EAP protocol*)
PEP	Punto de imposición de la política (*policy enforcement point*)
PGP	Privacidad bastante buena (*pretty good privacy*)
PKI	Infraestructura de clave pública (*public key infrastructure*)
PKIX	Infraestructura de clave pública X.509 (*public key infrastructure X.509*)
PoP	Prueba de posesión (*proof of possession*)
PPP	Protocolo punto a punto (*point-to-point protocol*)
RADIUS	Servicio de usuario de marcación de autentificación a distancia (*remote authentication dial-in user service*)
RSA	Algoritmo de clave pública Rivest Shamir Adleman (*Rivest Shamir Adleman public key algorithm*)
RTPC	Red telefónica pública conmutada
SHA-1	Algoritmo de aleatorización segura 1 (*secure hash algorithm 1*)
SIP	Protocolo de inicio de sesión (*session initiation protocol*)
SMTP	Protocolo de transferencia de correo simple (*simple mail transfer protocol*)
SNMP	Protocolo simple de gestión de red (*simple network management protocol*)
SP	Proveedor de servicios (*service provider*)
SSH	Intérprete de comandos seguro (*secure shell*)
SSID	Identificación de conjunto de servicios (*service set identification*)
SSO	Firma única (*single sign on*)
TKIP	Protocolo de integridad de clave temporal (*temporal key integrity protocol*)
TLS	Protocolo de seguridad de capa de transporte (*transport layer security protocol*)
UE	Equipo del usuario (*user equipment*)
URI	Identificador uniforme de recursos (*uniform resource identifier*)
UTC	Tiempo universal coordinado (*coordinated universal time*)
VAR	Revendedor con valor añadido (*value-added reseller*)
VLAN	LAN virtual (*virtual LAN*)
VoIP	Protocolo de transmisión de voz por Internet (*voice-over-IP*)
VPLS	Servicio del LAN privada virtual (*virtual private LAN service*)
VPN	Red privada virtual (*virtual private network*)
VPWS	Servicio alámbrico privado virtual (*virtual private wire service*)
WAN	Red de área extensa (*wide area network*)
WEP	Privacidad equivalente a los servicios alámbricos (*wired equivalent privacy*)
WLAN	LAN inalámbrica (*wireless LAN*)
WPA	Acceso protegido a Wi-Fi (*Wi-fi protected access*)
XML	Lenguaje de marcación extensible (*eXtensible markup language*)

5 Convenciones

En la presente Recomendación, el término equipo del usuario (UE) se entiende en un sentido amplio, esto es, todos los dispositivos, entidades (físicas y lógicas), sistemas móviles y/o fijos, computadoras personales (PC), terminales (con capacidad de multimedios), teléfonos, etc., que se encuentran en los locales del usuario y que, a menudo, escapan al control del operador o del proveedor de servicios.

6 Introducción

La utilización de redes para conectar sistemas de tecnología de la información (TI) heterogéneos puede generar un aumento de la productividad para las organizaciones y nuevas capacidades creadas por los sistemas conectados. Hoy en día resulta relativamente fácil obtener información, establecer comunicaciones, supervisar y controlar los sistemas de TI a gran distancia. Por tanto, las redes desempeñan en la actualidad un papel clave para las infraestructuras fundamentales de muchos países, como pueden ser el comercio electrónico, las comunicaciones de voz y datos, las instalaciones, las finanzas, la salud, los transportes y la defensa.

La interconexión de las redes y el acceso ubicuo son elementos clave de los sistemas de TI actuales. No obstante, la amplitud del acceso y la fácil conexión de los sistemas de TI pueden ser una fuente primaria de vulnerabilidad generalizada. Las amenazas que planean sobre los sistemas en red, como los ataques de denegación de servicio, el robo de datos financieros y personales, los fallos de red y la interrupción de telecomunicaciones de voz y datos, son cada vez más numerosas.

Los protocolos de red que se utilizan hoy en día se crearon en un entorno de confianza. La mayoría de las nuevas inversiones e investigaciones se dedican a la creación de nuevas funcionalidades, pero no a su seguridad.

Las amenazas a la ciberseguridad crecen rápidamente. Los virus, gusanos, caballos de Troya, ataques de falsificación, robos de identidad[1], el correo basura y ciberataques están al alza. Es necesario entender lo que es la ciberseguridad para poder sentar los cimientos necesarios a fin de poder proteger las redes del futuro.

Se alienta a que las empresas y organismos gubernamentales consideren la seguridad como un proceso o una perspectiva de protección de los sistemas, redes, aplicaciones y recursos. El principio subyacente es que las redes conectadas conllevan riesgos inherentes. Sin embargo, la seguridad no debe ser un obstáculo para el funcionamiento. El objetivo es saber cómo ofrecer los servicios necesarios de manera segura.

En el entorno comercial y administrativo actual, el concepto de perímetro está desapareciendo. Las fronteras entre redes interiores y exteriores son cada vez más tenues. Las aplicaciones se ejecutan en las redes por capas. Se supone que hay seguridad entre cada una de estas capas. Abordar la seguridad por capas permite a las organizaciones crear múltiples niveles de defensa contra las amenazas.

7 Ciberseguridad

Las organizaciones han de establecer un plan global a fin de satisfacer sus necesidades de seguridad. Conviene que consideren la seguridad como un proceso o una perspectiva de protección de los sistemas, las redes, las aplicaciones y los recursos.

---

[1] El término "robo de identidad" se refiere únicamente a la utilización no autorizada del conjunto de identificadores y otra información que, en conjunto, caracterizan la identidad de un determinado usuario. A diferencia del concepto normal de robo, en el que la víctima se queda sin el objeto robado, por regla general el ladrón de identidad adquiere o copia la información detallada de la identidad de tal modo que el propietario legítimo de la misma puede no darse cuenta del robo.

7.1 ¿Qué es la ciberseguridad?

El término ciberseguridad se define en la cláusula 3.2.5 de la presente Recomendación.

Pueden utilizarse técnicas de ciberseguridad para garantizar la disponibilidad, integridad, autenticidad, confidencialidad y no repudio del sistema. La ciberseguridad puede emplearse para garantizar el respeto de la privacidad de los usuarios. Pueden utilizarse técnicas de ciberseguridad para asentar la confianza de los usuarios.

Tecnologías tales como las redes inalámbricas y el protocolo de transmisión de voz por Internet (VoIP) amplían el alcance y escala de Internet. Desde este punto de vista, el ciberentorno incluye a los usuarios, Internet, los dispositivos informáticos conectados al mismo y todas las aplicaciones, servicios y sistemas que pueden estar directa o indirectamente conectados a Internet y al entorno de las redes de la próxima generación (NGN), sean éstas públicas o privadas. Por tanto, con la tecnología VoIP, un teléfono fijo forma parte del ciberentorno. No obstante, también los dispositivos aislados pueden formar parte del mismo si pueden compartir información con dispositivos informáticos conectados a través de medios extraíbles.

El ciberentorno incluye el software que se ejecuta en los dispositivos informáticos, la información almacenada (y transmitida) en estos dispositivos o la información que éstos generan. Las instalaciones y edificios donde residen los dispositivos también forman parte del ciberentorno. La ciberseguridad ha de tener en cuenta todos estos elementos.

El objetivo de la ciberseguridad es proteger el ciberentorno, un sistema que puede incluir múltiples entidades públicas y privadas, utilizando diversos componentes y distintos métodos de seguridad. Por tanto, conviene considerar la ciberseguridad en los siguientes términos:

– El conjunto de políticas y acciones que se utilizan para proteger las redes conectadas (incluidos los ordenadores, los dispositivos, el hardware, la información almacenada y la información en tránsito) del acceso y la modificación no autorizados, el robo, la interrupción u otras amenazas.
– Una evaluación y supervisión constantes de dichas políticas y acciones a fin de garantizar la continua calidad de la seguridad frente a la naturaleza voluble de las amenazas.

En [b-UIT-T Y.2201] se indican los requisitos de las NGN que pueden emplearse para mejorar la ciberseguridad de estas redes. Se promueve la autentificación, con la posibilidad de autentificar por separado dispositivos y usuarios. En las NGN, la autentificación bilateral basada en varios factores que permiten autorizar por separado cada servicio reduce el riesgo de ataques dirigidos al usuario.

7.2 Naturaleza del entorno de ciberseguridad de la empresa

Las organizaciones han de establecer un plan global para satisfacer sus necesidades de seguridad. La seguridad no es la misma para todo el mundo (véase [UIT-T X.805]). No puede alcanzarse la seguridad con un conjunto de módulos ensamblados. Conviene que las organizaciones consideren la seguridad como un proceso o perspectiva de protección de sistemas, redes, aplicaciones y servicios de red.

La seguridad ha de abarcar todas las capas de la red. Es necesario adoptar un método por capas para la seguridad que, combinado con una sólida gestión y aplicación de la política, brinde a los profesionales de la seguridad una serie de soluciones modulares, flexibles y adaptables.

La seguridad es difícil de probar, predecir y aplicar. La misma seguridad no es válida para todos. Las necesidades de seguridad y las estrategias recomendadas de cada organización son únicas y diferentes. Por ejemplo, cada empresa, proveedor de telecomunicaciones, operador de red o proveedor de servicios tiene una serie propia de necesidades comerciales y puede modificar su entorno de red para adaptarse a las mismas.

Por ejemplo, una empresa cerrada utiliza líneas privadas lógicas (por ejemplo, retransmisión de tramas) o físicas, dando acceso a distancia de manera selectiva a los empleados que necesitan acceder a Internet. Se llega a la web a través de un centro de datos Internet de un proveedor de servicios (responsable del establecimiento de un entorno seguro). La organización también proporciona acceso por marcación convencional a los empleados a distancia (por ejemplo, que trabajan desde un hotel). La empresa utiliza el correo privado entre los empleados sin acceso externo. También se utilizan las LAN inalámbricas.

Por otra parte, una empresa extendida, proveedor de telecomunicaciones, operador de red o proveedor de servicios, caracterizados por diversos modelos comerciales, pueden ofrecer soporte para el teletrabajo y el acceso distancia a la oficina a través de VPN IP por Internet o conexiones de menor costo y más veloces, incluido el acceso para fines generales a Internet como, por ejemplo, el interfuncionamiento entre el sistema de correo interno y el resto del mundo.

En cambio, en una empresa abierta el modelo comercial consiste en utilizar Internet para permitir a sus socios, proveedores y clientes acceder al centro de datos Internet gestionado por la empresa, e incluso les da acceso selectivo a las bases de datos y aplicaciones internas (por ejemplo, como parte de un sistema de gestión de la cadena de producción). Los usuarios internos y externos pueden acceder a la red de la empresa desde sus hogares, oficinas distantes u otras redes utilizando dispositivos alámbricos o móviles. En este sentido, los requisitos de seguridad para este tipo de empresas son diferentes del resto.

En la figura 7-1 se ilustran los tipos de empresa.

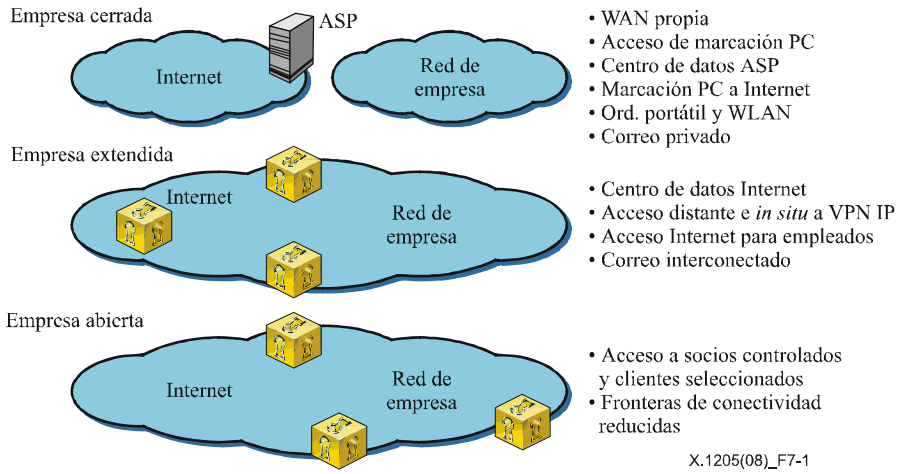

Figura 7-1 – Tipos genéricos de empresa

La ciberseguridad necesita de una gestión de riesgos. Este proceso conlleva la identificación del conjunto de componentes que han de protegerse. A fin de facilitar el análisis de riesgos, conviene considerar que los ataques se organizan en las siguientes categorías:

1) Ataques de interrupción de servicio: Este tipo de ataques inhabilita el acceso de los usuarios a los servicios deseados de manera temporal o permanente. Como ejemplos pueden citarse la falta de acceso a un sitio web o la incapacidad de llevar a cabo una transacción financiera o de iniciar una llamada de voz. Diversos tipos de ataques pueden conducir a una interrupción del servicio. Por ejemplo, la denegación de servicio (DoS, *denial of service*), los ataques de denegación de servicio distribuidos (DDoS, *distributed denial of service attacks*), o los daños a edificios que albergan infraestructura crítica y pueden impedir a los usuarios acceder a un servicio.

2) Activos en peligro: Este tipo de ataques conlleva el robo o utilización fraudulenta de la infraestructura. Los ataques de este tipo pueden repercutir en la ciberseguridad si se llevan a cabo a gran escala.

3) Piratería de componentes: Este tipo de ataques supone tomar el control de algunos dispositivos y utilizarlos para lanzar nuevos ataques contra otros componentes del ciberentorno.

Cualquier elemento del ciberentorno puede considerarse un riesgo de seguridad, que en general se trata de una evaluación ponderada de las amenazas. El análisis de amenazas incluye la descripción del tipo de posibles ataques, los agresores potenciales y sus métodos y las consecuencias del éxito de un ataque. Por otra parte, en esta Recomendación, vulnerabilidad hace referencia a un punto débil que puede ser explotado por un agresor. La evaluación de riesgos sumada al análisis de amenazas permite a la organización evaluar los posibles riesgos a que se enfrenta su red.

Los ataques pueden originarse en el ciberentorno, a través de gusanos u otro tipo de programas malignos; pueden ser ataques directos a la infraestructura básica, como los cables de telecomunicaciones, o pueden derivarse de las acciones de un usuario interno fiable. También es posible combinar distintos tipos de ataque. Por norma general, los riesgos se clasifican en altos, medios y bajos. El nivel de riesgo varía de un componente a otro del ciberentorno.

La seguridad depende fundamentalmente de la gestión de riesgos. Para gestionar los riesgos pueden utilizarse muchas técnicas distintas. Por ejemplo, puede desarrollarse una estrategia de defensa en la que se especifiquen las medidas que se adoptarán ante posibles ataques; puede recurrirse a la detección, que incluye la identificación de un ataque en curso o después de que se haya llevado a cabo; se puede formular una respuesta a un ataque en la que se especifiquen las medidas que es necesario adoptar para frenar el ataque o reducir sus consecuencias; o se puede formular una estrategia de recuperación que permita a la red reanudar su funcionamiento a partir de un estado conocido.

7.3 Amenazas a la ciberseguridad y metodología para contrarrestarlas

Desde el punto de vista de la X.800, las amenazas a los sistemas de comunicaciones de datos incluyen las siguientes:

a) destrucción de información y/u otros recursos;

b) corrupción o modificación de información;

c) robo, eliminación o pérdida de información y/u otros recursos;

d) divulgación de información confidencial; e

e) interrupción de servicios.

De acuerdo con la [UIT-T X.800] las amenazas pueden clasificarse en accidentales o intencionales y pueden ser activas o pasivas. Las amenazas accidentales son las que existen sin que sean premeditadas. Ejemplos de ello pueden ser el disfuncionamiento del sistema, los errores operativos o del software. Las amenazas intencionales pueden ir del simple examen mediante herramientas de supervisión fáciles de conseguir a los ataques más perfeccionados que requieren conocimientos especiales del sistema. De llevarse a cabo, una amenaza intencional puede considerarse un "ataque". Las amenazas pasivas son las que, de ponerse en práctica, no causarían ninguna modificación de la información contenida en el(los) sistema(s) y no se modificaría el funcionamiento ni el estado del sistema. La utilización de escuchas pasivas para observar la información que se transmite a través de una línea de comunicaciones es un tipo de realización de amenaza pasiva. Las amenazas activas a un sistema conllevan la alteración de la información del sistema o la modificación de su estado o funcionamiento. La modificación malintencionada de los cuadros de encaminamiento de un sistema por parte de un usuario no autorizado puede considerarse un ejemplo de amenaza activa. En el apéndice I se presenta un breve resumen de algunos tipos específicos de ataques.

Las amenazas a la seguridad descritas en la X.800 se aplican igualmente al ciberentorno. Según [UIT-T X.800] las características de seguridad suelen incrementar el coste de un sistema y pueden dificultar su utilización. Por consiguiente, antes de diseñar un sistema seguro, se aconseja identificar las amenazas específicas que hacen necesaria la protección. Esto se conoce como evaluación de amenazas. Un sistema tiene muchas vulnerabilidades, pero sólo algunas de ellas son explotables, porque el agresor carece de oportunidades o porque el resultado no justifica los esfuerzos necesarios ni el riesgo de ser detectado. Aunque los detalles de la evaluación de amenazas quedan fuera del alcance de la presente Recomendación, en líneas generales se trata, en primer lugar, de hacer un inventario de los activos que requieren protección, por cuanto éstos son el objeto de las amenazas.

El siguiente paso consiste en analizar las amenazas, las vulnerabilidad (incluida la evaluación del impacto), las medidas para contrarrestarlas y los mecanismos de seguridad, con el fin de:

a) identificar las vulnerabilidades del sistema;

b) analizar la probabilidad de amenazas cuyo objetivo sea explotar estas vulnerabilidades;

c) evaluar las consecuencias de cada amenaza, en caso de que se llevase a cabo con éxito;

d) estimar el coste de cada ataque;

e) determinar el coste de las posibles medidas de respuesta; y

f) seleccionar los mecanismos de seguridad que se justifican (posiblemente recurriendo al análisis de rentabilidad).

En algunos casos, las medidas no técnicas, como la cobertura de seguros, pueden ser alternativas rentables a las medidas de seguridad técnicas. En general, no es posible lograr una seguridad técnica perfecta. Por tanto, el objetivo debe ser elevar el coste de los ataques de manera que se reduzcan los riesgos a niveles aceptables.

7.4 Seguridad de las comunicaciones de extremo a extremo

En [UIT-T X.805] se define un marco de seguridad de red para atender la seguridad de la red de extremo a extremo. La [UIT-T X.805] es aplicable a distintos tipos de redes donde la seguridad de extremo a extremo se considera un problema. La arquitectura es independiente de la tecnología de red subyacente.

La arquitectura de seguridad comprende todos los retos de seguridad de los proveedores de servicios, empresas y consumidores y es aplicable a las redes de voz, datos y convergentes inalámbricas, ópticas y alámbricas. La arquitectura observa los problemas de seguridad de la gestión, control y utilización de la infraestructura de red, los servicios y las aplicaciones. La [UIT-T X.805] permite la detección dinámica y la mitigación de las vulnerabilidades de seguridad para las amenazas conocidas. La arquitectura de seguridad divide lógicamente un conjunto complejo de características de seguridad de la red de extremo a extremo en diversos componentes arquitecturales. Esta separación permite la adopción de un método sistemático para la seguridad de extremo a extremo que puede utilizarse para planificar nuevas soluciones de seguridad y para evaluar la seguridad de las redes existentes.

Según [UIT-T X.805], una dimensión de seguridad es un conjunto de medidas de seguridad diseñadas para solventar un determinado aspecto de la seguridad de la red. En [UIT-T X.805] se definen ocho dimensiones que proporcionan protección contra las principales amenazas de seguridad. Estas dimensiones no se limitan a la red, sino que también se extienden a las aplicaciones y a la información de usuario extremo. Las dimensiones de seguridad se aplican a los proveedores de servicios o empresas que ofrecen servicios de seguridad a sus clientes. Las dimensiones de seguridad son:

1) control de acceso;

2) autentificación;

3) no repudio;

4) confidencialidad de datos;

5) seguridad de las comunicaciones;

6) integridad de los datos;

7) disponibilidad; y

8) privacidad.

A fin de proporcionar una solución de seguridad de extremo a extremo, las dimensiones de seguridad deben aplicarse a una jerarquía de equipos de red y agrupamientos funcionales que se denominan capas de seguridad. Se trata de las tres siguientes capas de seguridad:

1) la capa de seguridad de infraestructura;

2) la capa de seguridad de servicios; y

3) la capa de seguridad de aplicaciones.

Las capas de seguridad identifican los puntos en que es necesario utilizar productos y soluciones de seguridad presentando una perspectiva secuencial de la seguridad de la red. Por ejemplo, en primer lugar se tratan las vulnerabilidades de seguridad de la capa de infraestructura, luego las de la capa de servicios y las de la capa de aplicaciones. En la figura 7-4.1 se muestra cómo se aplican las dimensiones de seguridad a las capas de seguridad a fin de reducir las vulnerabilidades de cada capa.

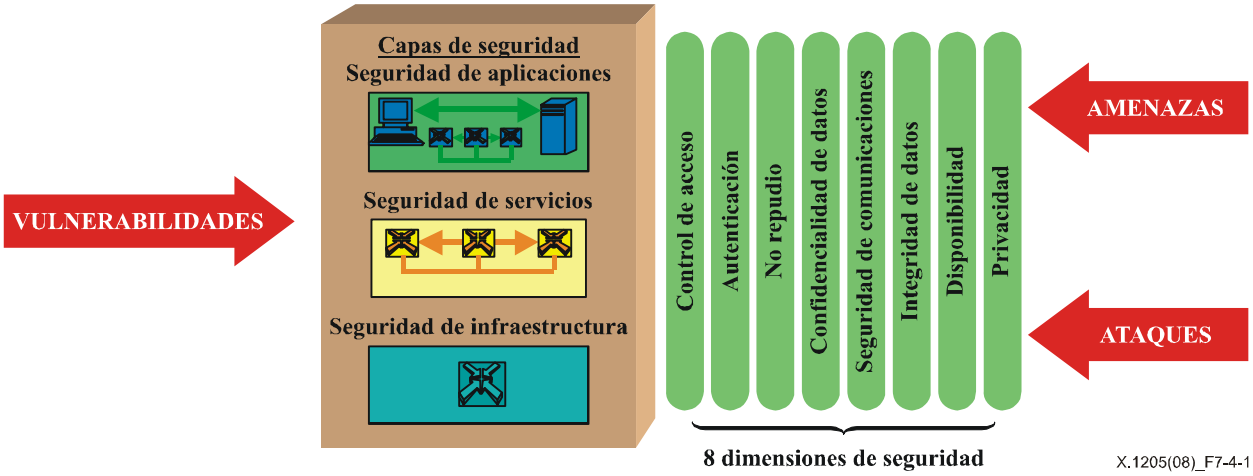

Figura 7-4.1 – Aplicación de las dimensiones de seguridad a las capas de seguridad

En [UIT-T X.805] un plano de seguridad es un determinado tipo de actividad de red protegida por las dimensiones de seguridad. En [UIT-T X.805] se definen tres planos de seguridad que representan tres tipos de actividades protegidas que se llevan a cabo en la red. Los planos de seguridad son:

1) el plano de gestión;

2) el plano de control; y

3) el plano de usuario extremo.

Estos planos de seguridad observan las necesidades de seguridad específicas asociadas con las actividades de gestión de red, las actividades de control o señalización de red y las actividades de los usuarios extremos, respectivamente. En [UIT-T X.805] se sugiere que se diseñen las redes de manera que cualquier cosa que ocurra en uno de los planos de seguridad se mantenga aislado de los otros planos de seguridad. Por ejemplo, una inundación de búsquedas de DNS en el plano de

usuario extremo, iniciada por las peticiones de los usuarios extremos, no debe bloquear la interfaz OAM&P en el plano de gestión, permitiendo así al administrador corregir el problema.

En la figura 7-4.2 se muestra la arquitectura de seguridad con los planos de seguridad incluidos. El concepto de planos de seguridad permite diferenciar los problemas de seguridad específicos asociados con dichas actividades y da la capacidad de solucionarlos independientemente. Por ejemplo, en un servicio VoIP, que corresponde a la capa de seguridad de servicios, la tarea de asegurar la gestión del servicio debe ser independiente de la tarea de proteger el control del servicio. Estas tareas son independientes de la tarea de proteger los datos de usuario extremo que transporta el servicio (por ejemplo, la voz del usuario).

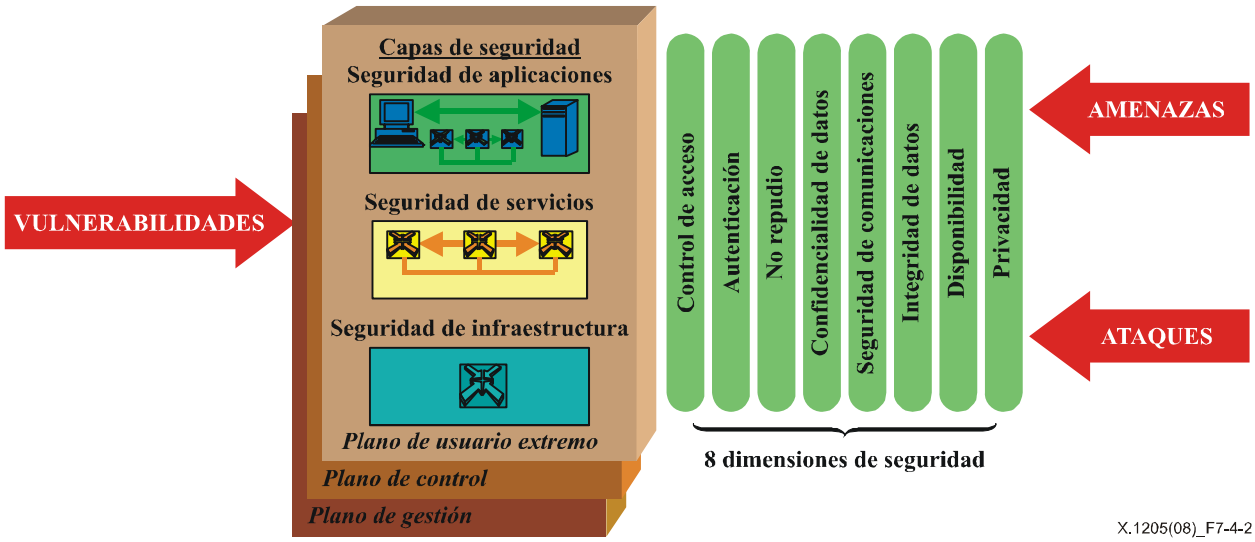

Figura 7-4.2 – Los planos de seguridad reflejan los distintos tipos de actividades de la red

8 Posibles estrategias de protección de la red

La seguridad incluye todas las capas de la arquitectura de red. Este método es un buen punto de partida para el diseño de redes seguras. Esta descomposición permite a la capa superior definir sus propios requisitos de seguridad en esa capa específica y también le permite utilizar los servicios de seguridad de las capas inferiores. El método de seguridad por capas facilita el desarrollo de soluciones de seguridad flexibles y adaptables en el nivel de red, el nivel de aplicación y el nivel de gestión de todas las organizaciones.

8.1 Gestión de política de bucle cerrado

Una política de seguridad adecuadamente diseñada y aplicada es un requisito básico para todos los tipos de empresas y organizaciones. La política de seguridad debe ser dinámica, en teoría y en práctica, y aplicarse, observarse y actualizarse de manera que refleje todos los cambios que experimenten la infraestructura de la empresa u organización y los requisitos de servicio.

La política de seguridad debe identificar claramente los recursos de la organización (y de la empresa) que corren riesgos y los correspondientes métodos para contrarrestar las amenazas. La política de seguridad debe prever la evaluación de vulnerabilidad y riesgos y definir las reglas de control de acceso adecuadas. La evaluación de vulnerabilidad y riesgos ha de llevarse a cabo en todos los niveles de la red. Con esta política deberá poderse identificar y descubrir las violaciones de seguridad y en ella estarán definidas las medidas de respuesta necesarias.

Se recomienda a los administradores de TI que utilicen herramientas de piratas para realizar la evaluación de vulnerabilidad de sus redes. Rige el principio de acceso con menos privilegios. Una

de las tareas de los administradores de TI y de red es asegurarse de que se revisan los rastros de auditoría, cerrando así el bucle de la gestión de política. De encontrarse problemas en las auditorías, los administradores de TI velarán por que la política se actualice para reflejar las revisiones realizadas.

Una política de seguridad que no se observa es inútil. La observancia de la política de seguridad depende de las personas. Debe quedar claramente determinada la responsabilidad y dependencia de la observancia de la política.

8.2 Gestión de acceso uniforme

El término gestión de acceso se utiliza para definir sistemas que pueden utilizar tanto los servicios de autentificación como de autorización para controlar la utilización de un recurso. La autentificación es el proceso según el cual un usuario solicita a una red el establecimiento de una identidad. La autorización determina el nivel de privilegios de esa identidad de acuerdo con el control de acceso. El control del nivel de acceso depende de la definición y observancia de la política de control. En la figura 8-2 se muestra el modelo de referencia que ha de utilizarse como modelo de referencia para la autentificación y autorización seguras.

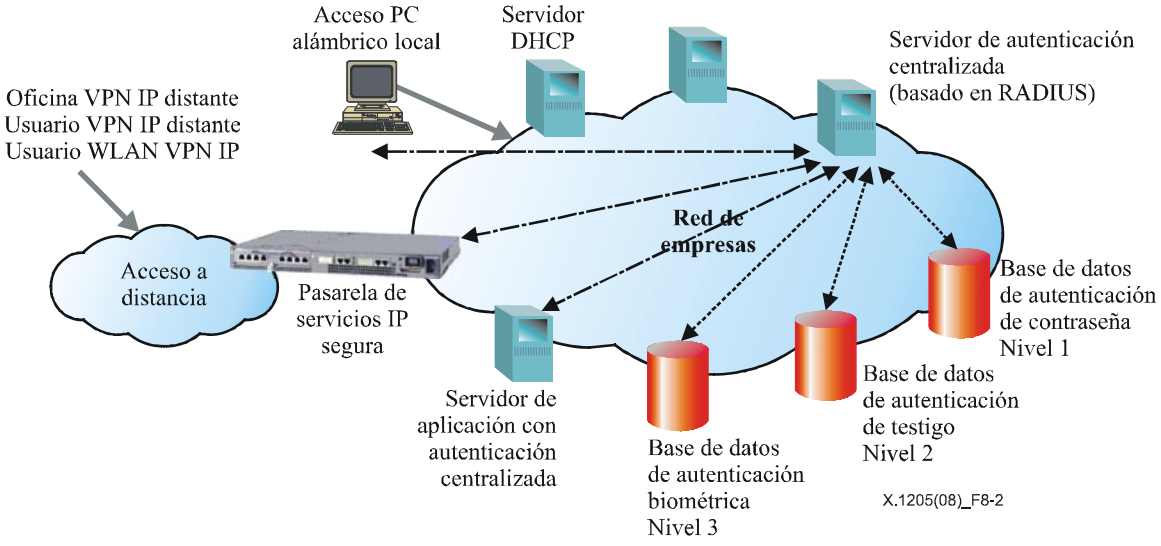

Figura 8-2 – Modelo de referencia de autentificación y autorización seguras

De la figura 8-2 se desprenden las siguientes recomendaciones:

1) Utilización de un mecanismo de autentificación centralizada para facilitar la administración y eliminar la necesidad de almacenar localmente las contraseñas. (Las contraseñas almacenadas a nivel local suelen ser estáticas y débiles.)

2) Utilización de un sistema de autorización centralizada, estrechamente vinculado al sistema de autentificación, con la granularidad adecuada para cada empresa.

3) Utilización de reglas de contraseñas fuertes (complejas) para todas las contraseñas.

4) Almacenamiento seguro de todas las contraseñas en formato de criptación en un solo sentido (aleatorizadas).

5) Aplicación del principio de sencillez, que implica la facilidad de utilización y de administración. Un sistema sencillo es un sistema seguro, ya que es más fácil seguir las consignas de seguridad.

6) Registro cronológico seguro de todos los eventos de seguridad relacionados con la autentificación y la autorización.

Los métodos para la gestión de acceso incluyen el filtrado de origen IP, los intermediarios y las técnicas basadas en credenciales. Cada método tiene sus ventajas y limitaciones. Dependiendo del tipo de empresa, e incluso para un mismo tipo, pueden utilizarse uno o más métodos, o una combinación de ellos. Por ejemplo, una empresa puede optar por gestionar el acceso a las estaciones de trabajo utilizando el filtrado de origen IP y puede elegir utilizar un plan de credenciales para los demás usuarios.

Pueden utilizarse varios métodos para autentificar un usuario, entre los que se cuentan, las contraseñas, los pases de validez limitada, las técnicas biométricas, las tarjetas inteligentes y los certificados. La autentificación por contraseñas debe utilizar contraseñas fuertes (por ejemplo de, al menos, ocho caracteres con, como mínimo, uno alfabético, uno numérico y un carácter especial). La autentificación por contraseñas por sí sola puede no ser suficiente. De acuerdo con la evaluación de vulnerabilidad, puede ser necesario combinar la autentificación por contraseñas con otros procesos de autentificación y autorización como los certificados, el protocolo ligero de acceso al directorio (LDAP), el servicio de usuario de marcación de autentificación a distancia (RADIUS), Kerberos y la infraestructura de clave pública (PKI).

Todos los mecanismos de autentificación tienen ventajas e inconvenientes. Las combinaciones de ID de usuario/contraseña son sencillas, baratas y fáciles de gestionar, aunque los usuarios suelen tener dificultades para recordar muchas contraseñas complejas. Los sistemas de autentificación de doble y de triple factor añaden solidez a la autentificación, pero son onerosos, más complejos y son difíciles de mantener.

Un sistema de "contraseña única" con contraseñas fuertes puede ser una buena solución para la autentificación y autorización de empresa. Un sistema de este tipo proporciona una alta seguridad de autentificación, autorización granular y es fácil de administrar. Con este sistema, se sincroniza la contraseña fuerte única de usuario con muchas aplicaciones y sistemas de toda la empresa con fines de autorización y autentificación. Todos los sistemas y aplicaciones de la empresa remiten las funciones de autentificación y autorización al sistema de contraseña única. Al haber sólo una contraseña fuerte que recordar, el sistema es más sencillo de utilizar y no es probable que los usuarios lo eviten. Éstas son las ventajas del sistema de contraseña única:

- Un único método coherente para la creación de contraseñas.
- Un único método coherente para la autentificación y la autorización.
- Un único método para el registro y terminación de cuentas de usuario.
- Observancia de las directrices firmes de la empresa sobre contraseñas.
- Coherencia: los usuarios saben qué deben hacer.
- Normalización: facilidad de soporte y adopción.
- Rapidez: interfaces y API normalizadas.
- Coste reducido y menos peticiones de ayuda.

La empresa abierta y extendida encuentra más problemas para diseñar su política de gestión de acceso. Resulta conveniente considerar la gestión de acceso como parte integrante de la política de seguridad. Estas organizaciones deben diseñar un sistema de gestión de acceso uniforme con reglas de granularidad más fina que han de aplicarse adecuadamente a:

- Directorios y bases de datos de identidades.
- Múltiples sistemas de autentificación como contraseñas, Kerberos, TACACS y RADIUS.
- Anfitriones, aplicaciones y servidores de aplicación.

El sistema de gestión de acceso uniforme debe gestionar las sesiones por usuario después de que éste haya sido autentificado. Se recomienda la utilización de una configuración flexible y una aplicación de política con reglas de granularidad fina capaces de tratar objetos específicos. También conviene realizar la adecuada supervisión, contabilidad y auditorías de seguridad. Es recomendable utilizar cuentas exclusivas para cada administrador donde se puedan rastrear las acciones realizadas por cada usuario, responsabilizándolos de las mismas.

8.3 Comunicaciones seguras

Las redes unificadas pueden transportar paquetes de voz, datos y vídeo. La finalidad de proteger el tráfico de red es garantizar la confidencialidad, la integridad y la exactitud de las comunicaciones de red. También ha de preverse la seguridad de las llamadas y el tráfico de señalización en las redes telefónicas. Ha de utilizarse una tecnología de criptación para las redes de datos y voz y las redes móviles.

La criptación puede obtenerse a través de:

- Técnicas VPN con IPSec, con encabezamiento de autentificación (AH, *authentication header*) y encapsulación de cabida útil de seguridad (ESP, *encapsulating security payload*) o tunelización gracias al protocolo de tunelización de capa 2 (L2TP, *layer 2 tunneling protocol*).
- La gestión de claves puede basarse en el intercambio de claves Internet (IKE, *Internet key exchange*).
- La gestión de certificados se basa en la infraestructura de clave pública [b-UIT-T X.509] (PKIX, *public key infrastructure X.509*).
- El protocolo de gestión de certificados (CMP, *certificate management protocol*) (véase [b-IETF RFC 2510]) y el protocolo de estado de certificado en línea (OCSP, *online certificate status protocol*) (véase b-IETF RFC 4557]).
- En la capa de aplicación, mediante la utilización de TLS (véase [b-IETF RFC 4366]) con claves fuertes.

Es importante utilizar algoritmos de criptación normalizados y funciones de aleatorización como DES, 3DES, AES, RSA y DSA (véase [b-IETF RFC 2828]). MD5 (véase [b-IETF RFC 1321]) y SHA-1 (véase [b-IETF RFC 3174]) podrían utilizarse para la integridad del mensaje, y Diffie-Hellman (véase [b-IETF RFC 2631]) y RSA (véase [b-IETF RFC 2828]) para el intercambio de claves.

NOTA – El NIST (National Institute of Standards and Technology) alienta la utilización del SHA-256 (algoritmo de troceado seguro (*secure hash algorithm*) con claves codificadas de 256 bits) en lugar del SHA-1.

La privacidad equivalente a la de las redes alámbricas (WEP, *wired equivalent privacy*), como se define en las normas [b-IEEE 802.11]), define una técnica para proteger la transmisión aérea entre los puntos de acceso de LAN inalámbrica (WLAN, *wireless LAN*) y las tarjetas de interfaz de red (NIC, *network interface cards*). Se ha visto que este protocolo no es seguro. Para dar seguridad a las WLAN con WEP se han de añadir medidas de protección como IPSec. Alternativamente, para lograr una mayor protección se puede utilizar el acceso protegido a Wi-Fi (WPA, *Wi-Fi protected access*).

8.4 Seguridad de profundidad variable

Una VLAN (LAN virtual) es un grupo de dispositivos de red, tales servidores y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red. En una VLAN, los recursos y servidores de otros usuarios en la red serán invisibles para los miembros de las demás VLAN. Las VLAN ayudan a cumplir los requisitos de calidad de funcionamiento por cuanto dividen la red de manera más eficaz. Además, restringen la distribución de información en

modo difusión y el tráfico entre nodos, de modo que se reduce el volumen de tráfico ajeno que pasa por la red. Todos los paquetes circulan entre varias VLAN pueden atravesar también un encaminador, por lo que pueden aplicarse medidas de seguridad en este dispositivo para limitar el acceso al segmento.

La seguridad por capas permite ofrecer grados de seguridad variables. Cada nivel de seguridad adicional se basa en las capacidades de la capa inferior y ofrece mayor seguridad con una granularidad más fina.

Por ejemplo, pueden recurrirse a las VLAN para efectuar una segmentación y una compartimentación básicas de la red, lo que permite contener y segmentar las diversas funciones de la empresa en sus propias redes de área local privadas controlando estrictamente o prohibiendo el intercambio de tráfico con otros segmentos de la VLAN. De la implantación de VLAN para zonas pequeñas o medianas dentro de la empresa se desprenden varios beneficios. Así pues, la utilización de "etiquetas" VLAN permite segregar el tráfico en grupos específicos, como finanzas, recursos humanos y diseño. La separación de los datos sin que haya "fugas" entre las VLAN es un elemento importante para la seguridad.

Puede lograrse una segunda capa de seguridad utilizando un perímetro y cortafuegos-filtros distribuidos en puntos estratégicos de la red. La capa de cortafuegos permite segmentar aún más la red en zonas pequeñas y ofrece conexiones seguras con la red pública. Los cortafuegos limitan el acceso al tráfico interno y externo a los protocolos explícitamente configurados en ese cortafuegos. Además, puede introducirse la autentificación de usuarios entrantes o salientes. Los cortafuegos que soportan la traducción de dirección de red (NAT) permiten optimizar el direccionamiento IP dentro de la red, como se especifica en [IETF RFC 1918] (atribución de direcciones para Internet privada).

Los cortafuegos aportan otra capa de protección útil para el control de acceso. La aplicación de un acceso conforme a la política permite la personalización del acceso de acuerdo con las necesidades de la empresa. La utilización de un método de cortafuegos distribuidos tiene además la ventaja de que puede adaptarse a la evolución de las necesidades de la empresa. Pueden instalarse cortafuegos personales en los sistemas extremos para garantizar la integridad de las aplicaciones.

Como tercera capa de seguridad pueden añadirse VPN de capa 3. Las VPN afinan la granularidad del control de acceso y la personalización. Las VPN aportan seguridad de granularidad muy fina hasta el nivel de usuario y permiten el acceso a distancia seguro para los emplazamientos distantes y los socios comerciales. Con las VPN no se necesita utilizar líneas dedicadas. El encaminamiento dinámico por túneles seguros en Internet es una solución muy segura, fiable y adaptable. La utilización de VPN sumadas a las VLAN y los cortafuegos facilitan al administrador de red la limitación del acceso por usuarios o grupos de usuarios de acuerdo con los criterios de la política y las necesidades de la empresa. Las VPN garantizan más solidamente la integridad y la confidencialidad de los datos. En esta capa puede aplicarse una fuerte criptación de datos para lograr la confidencialidad y la integridad de los datos.

Las soluciones de seguridad basadas en el método por capas son flexibles y adaptables a las necesidades de seguridad de la empresa.

8.5 Gestión de la seguridad

Ya se considere como una "práctica idónea" o como parte integrante de la arquitectura de seguridad de una organización o empresa, el canal o plano de gestión seguro es la base de todos los demás elementos de la gestión de la red, su calidad de funcionamiento y supervivencia. En la figura 8-5 se propone un posible modelo de referencia para asegurar la gestión de red en el centro de operaciones de red (NOC, *network operations center*).

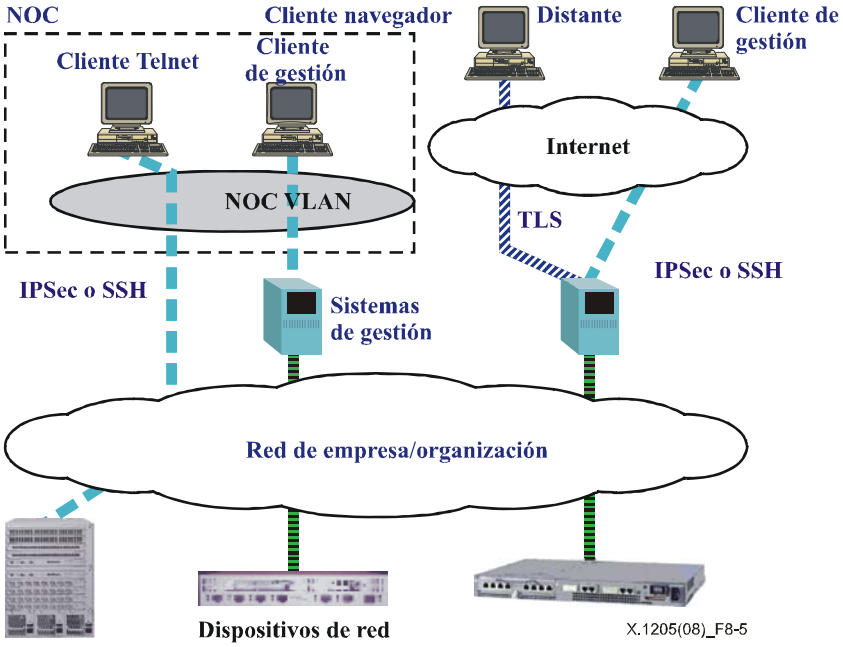

Figura 8-5 – Modelo de referencia para proteger la gestión

La gestión segura es más un método global que un conjunto de características de seguridad de un elemento de red determinado. Por este motivo, el método recomendado en esta Recomendación abarca zonas fundamentales de la infraestructura de red y presenta medidas específicas para contrarrestar las posibles amenazas que se ciernen sobre la red. Cada una de las zonas que se exponen a continuación representa un componente crítico que necesita atención para lograr formar un tejido protector alrededor de la red.

Hay nueve dominios de gestión de red clave cuya seguridad ha de tenerse en cuenta antes de que el plano de gestión de red pueda considerarse seguro. Éstos son:

- Registros cronológicos de actividad seguros.
- Autentificación del operador de red.
- Control de acceso para los operadores de red.
- Criptación del tráfico de gestión de red.
- Acceso a distancia seguro para los operadores.
- Cortafuegos.
- Detección de intrusión.
- Endurecimiento del OS.
- Software sin virus.

8.5.1 Gestión de política

Los registros cronológicos seguros pueden utilizarse para mantener una auditoría de las actividades de los usuarios o el administrador y de los eventos generados por el dispositivo mismo, y son un elemento fundamental para cerrar el bucle de la gestión de política. Los datos brutos recopilados se denominan "registro cronológico de auditoría", y el trayecto verificable de eventos gracias a los registros cronológicos de auditoría se denomina "rastro de auditoría". Para ser eficaces, los registros cronológicos de auditoría de seguridad tienen que contener suficiente información para permitir una investigación o análisis a posteriori de los incidentes de seguridad. Estos registros cronológicos de auditoría sirven para lograr varios objetivos de seguridad, incluidos la responsabilidad individual, la

reconstrucción de eventos pasados, la detección de intrusión y el análisis de los problemas. Los registros cronológicos también pueden utilizarse para el análisis de tendencias a largo plazo. La información de los registros cronológicos de auditoría ayuda a identificar la causa primera de un problema de seguridad y a evitar futuros incidentes. Esta información debe almacenarse de manera segura. Por ejemplo, los registros cronológicos de auditoría pueden emplearse para reconstruir la secuencia de eventos que ha conducido a un problema, como que un intruso logre acceso no autorizado a los recursos del sistema, o el disfuncionamiento del sistema causado por una configuración incorrecta o una aplicación fallida.

8.5.2 Gestión de acceso seguro

La autentificación del operador de red debe basarse en una fuerte autentificación centralizada de los operadores y administradores de red. La administración centralizada de contraseñas contribuye a la solidez de las contraseñas y elimina la necesidad de almacenar localmente las contraseñas en los elementos de red y los sistemas EMS. RADIUS es el mecanismo básico para automatizar la autentificación centralizada.

Para controlar el acceso de los operadores de red han de seguirse las prácticas adecuadas. Por ejemplo, a fin de determinar el nivel de autorización, puede emplearse una técnica basada en servidores RADIUS para lograr un nivel básico de control de acceso, y añadirse un servidor LDAP para que la granularidad del control de acceso sea más fina, de ser necesario.

8.5.3 Criptación del tráfico de gestión de red

Se recomienda la criptación de todo el tráfico de datos utilizado para la gestión de red a fin de garantizar la confidencialidad e integridad de los datos. Con cada vez más frecuencia, las empresas emplean una gestión de red en banda, por lo que es necesario separar el tráfico de gestión mediante criptación. La criptación del tráfico de gestión da una fuerte protección contra los usuarios internos, a excepción de un pequeño grupo que tiene acceso legítimo a las claves de criptación. Es necesaria la criptación entre los clientes del centro de operaciones de red (NOC) y los servidores y/o elementos de red del sistema de gestión de elementos (EMS), lo que incluye el tráfico SNMP, pues se sabe que SNMP v1 y v2 tienen vulnerabilidades resueltas en SNMP v3. Dependiendo del tipo de tráfico, los protocolos de seguridad que hay que utilizar en estos enlaces son TLS, IPSec y el intérprete de comandos seguro (SSH) (véase [b-IETF RFC 4252]). SSH es un protocolo de seguridad de nivel de aplicación que sustituye directamente a Telnet (véase [b-IETF RFC 854]) y FTP (véase [b-IETF RFC 959]), pero que normalmente no puede utilizarse para proteger otro tipo de tráfico. Por otra parte, el protocolo IPSec sólo se ejecuta entre la capa de red (capa 3) y la capa de transporte (capa 4) y puede emplearse para proteger cualquier tipo de tráfico de datos, independientemente de las aplicaciones y protocolos utilizados. IPSec es el método más recomendable, aunque SSH puede utilizarse si el tráfico sólo está formado por Telnet y FTP. La tecnología TLS puede proteger el tráfico HTTP cuando se utiliza en una capacidad de la gestión de red entre los clientes NOC y el EMS y/o los elementos de red. Para proteger el tráfico de gestión puede recurrirse a un dispositivo VPN IPSec externo en diversas partes de la red.

8.5.4 Acceso a distancia seguro para los operadores

Debe darse seguridad a los operadores y administradores que gestionan la red desde emplazamientos distantes a través de una red pública. La mejor solución es crear una red privada virtual segura con IPSec, ya que así se garantizará la fuerte criptación y autentificación de todos los operadores distantes. Debe situarse una VPN en la interfaz del sistema de gestión y todos los operadores deberán estar equipados con clientes de acceso extranet en sus ordenadores portátiles o de escritorio.

8.5.5 Cortafuegos

Para aplicar los principios de seguridad de profundidad variable conviene dividir el entorno de gestión de red con VLAN y cortafuegos. El cortafuegos controla el tipo (protocolo, número de puerto, dirección de origen y destino) del tráfico utilizado para cruzar la frontera entre distintos dominios de seguridad. Dependiendo del tipo de cortafuegos (aplicación por oposición a filtrado de paquetes), también puede ampliarse hasta comprender el filtrado del contenido de aplicación del flujo de datos. La ubicación del cortafuegos, su tipo y las reglas de filtrado dependen específicamente de la implementación de cada red.

8.5.6 Detección de intrusión

Los sistemas de detección de intrusión basados en el anfitrión pueden incorporarse a los servidores de gestión para defenderse de las intrusiones en la red. Los sistemas de detección de intrusión pueden emplearse para advertir a los administradores de red de la posibilidad de que ocurra un incidente de seguridad, como la puesta en peligro de un servidor o un ataque de denegación de servicio.

8.5.7 Capa de seguridad de aplicación

Se recomienda el endurecimiento de todos los sistemas operativos utilizados en la gestión de red. Es necesario endurecer todos los sistemas operativos utilizados para la gestión de red, ya sean sistemas operativos generales o sistemas operativos en tiempo real incorporados. En el caso de los sistemas operativos que no disponen de directrices de endurecimiento específicas, es necesario remitirse al fabricante del sistema para obtener los parches y procedimientos más recientes.

8.5.8 Software sin virus

Todo el software, ya se haya creado dentro de la empresa o se haya comprado a terceros, ha de examinarse para garantizar, en la medida de lo posible, que no tiene virus. Ha de diseñarse un proceso para la detección de virus, que comprenda el análisis de todo el software con una herramienta de detección de virus específica antes de poder instalarlo.

8.6 Seguridad por capas en la aplicación, la red y la gestión de red

Cada organización o empresa tiene un umbral de seguridad y una infraestructura tecnológica distinta. Las aplicaciones Internet representan mayores riesgos y amenazas para las empresas. Estas aplicaciones deben tener algún tipo de seguridad incorporada en el nivel de aplicación, aunque con las funcionalidades de seguridad de capas de red inferiores se puede mejorar la seguridad de las aplicaciones.

Las empresas con presencia en Internet están advertidas de que deben tener mucho cuidado al diseñar sus sitios. En [b-IETF RFC 2196] (Manual de Seguridad de Sitios) puede encontrarse una buena referencia sobre la seguridad de los sitios. Al nivel de aplicación, se recomienda utilizar una política de seguridad con granularidad fina. En la medida de lo posible, se deben direccionar los objetos en el nivel de identificadores uniformes de recursos (URI, *uniform resource identifiers*). Han de inhabilitarse las funcionalidades innecesarias y, siempre que se pueda, conviene utilizar TLS. Se recomienda la utilización de pasarelas a nivel de aplicación, así como un sólido mecanismo de autentificación y autorización. Si la infraestructura de seguridad lo permite, los servicios de correo electrónico deben protegerse con S/MIME (véase [b-IETF RFC 2311]) y técnicas como PGP (véase [b-IETF RFC 1991]).

En la capa de red se habrán de utilizar las técnicas expuestas en la cláusula 8.7 para garantizar una seguridad aceptable en la empresa. Esta seguridad se logra empleando la arquitectura de capas, que puede adaptarse a las necesidades de seguridad de cada empresa.

La protección del tráfico de gestión de red es uno de los requisitos fundamentales de la protección de la red. Para ello, en primer lugar es necesario verificar que el sistema operativo está endurecido contra las amenazas conocidas. Será necesario obtener del fabricante del sistema operativo los últimos parches y procedimientos de endurecimiento del OS. Habrán de tomarse las medidas necesarias para garantizar que todo el software instalado está libre de virus conocidos. Es preferible criptar siempre todo el tráfico de gestión con IPSec o TLS para proteger el tráfico HTTP. La criptación es una práctica adecuada y recomendable si el tráfico transita fuera de la LAN local. Se recomienda utilizar SNMPv3 y RADIUS para controlar el acceso a distancia de los operadores de red, además de múltiples mecanismos de control en varios niveles, que incluyan la utilización de contraseñas y la capacidad de administrar de manera centralizada el sistema de control de acceso. Es fundamental la protección de los registros cronológicos del tráfico de gestión de red.

8.7 Supervivencia de la red incluso en caso de ataque

En el entorno actual, las redes de empresa soportan operaciones fundamentales y son vitales para su funcionamiento. La red debe ser segura, fiable y estar disponible para todos los socios comerciales en cualquier momento.

Hay muchas técnicas que pueden emplearse para garantizar la fiabilidad de la red, de la que depende el adecuado funcionamiento de una red en caso de fallo de los componentes de software y/o hardware. No obstante, en presencia de amenazas de seguridad, ha de emplearse el concepto de redes supervivientes. Una red superviviente es una red que sigue llevando a cabo una serie de funcionalidades básicas mínimas convenientemente en caso de sufrir un ataque. La funcionalidad básica consiste en la prestación básica y oportuna de servicios, incluso si parte de la red es inalcanzable o está en estado de fallo a causa de un ataque.

Para diseñar redes supervivientes es necesario empezar organizando los servicios de red en dos categorías: servicios básicos y servicios no básicos. Por supervivencia se entiende que la red pueda resistir un ataque. Es indispensable contar con una estrategia clara sobre cómo tratar y recuperarse de los ataques. Dependiendo del tipo de ataque, el administrador de red puede considerar diversas estrategias de resistencia, identificación y recuperación. Una de las características de las redes supervivientes es su adaptabilidad. Por ejemplo, la red puede reencaminar el tráfico de un servidor a otro, si se detecta en el primer servidor una intrusión o un ataque.

Es necesario determinar en la fase de diseño de la política de seguridad cuáles son los servicios básicos que la red debe poder prestar incluso en caso de ataque. En esta fase se debe identificar cómo la red resistirá al ataque, cómo la red superará tales ataques y cuál será el mejor método para recuperarse de ellos. En este análisis se tendrán en cuenta los sistemas de gestión, los anfitriones, las aplicaciones, los encaminadores y los conmutadores.

Puede aumentarse la resistencia de las redes supervivientes a los ataques utilizando mecanismos de control de acceso con autentificación y criptación fuertes. El filtrado de mensajes y paquetes y la segmentación de red y servidor también mejoran la resistencia de la red en caso de ataque. Con las adecuadas técnicas de detección de intrusión se puede identificar un ataque. Pueden emplearse las técnicas de copia de seguridad adecuadas para la recuperación del sistema y la red.

Apéndice I

Técnicas de ataque

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

En este apéndice se exponen brevemente algunos de los ataques más peligrosos en el entorno del procesamiento y las comunicaciones de datos.

I.1 Clasificación de las amenazas de seguridad

Se aconseja a los profesionales de TI que consideren su red como un recurso al que accederán usuarios que, en general, no son fiables. Los agresores disponen de numerosas herramientas, técnicas y metodologías para poner la red en peligro. Los piratas pueden emplear estas herramientas para lanzar ataques multinivel a fin de acceder a la red. En ocasiones, los agresores explotarán un punto débil de la seguridad y lanzarán ataques secundarios para dañar otras partes de la red.

En esta cláusula se describen las técnicas, herramientas y metodologías utilizadas por agresores, piratas e intrusos para poner en peligro una red.

I.1.1 Amenazas de autorización

El acceso no autorizado a los recursos de una red suele ser el resultado de una configuración inadecuada del sistema y de fallos en la utilización. Los agresores pueden acceder ilegalmente aprovechando la insuficiencia de autentificación y autorización de usuarios y tareas en los sistemas de empresa, o descuidos de los empleados (por ejemplo, recordatorios escritos de las contraseñas, cuando el usuario ha de memorizar múltiples contraseñas).

La atribución impropia de espacio oculto y la compartición de privilegios entre aplicaciones representan serias vulnerabilidades. Es posible emplear ataques de trampilla para obtener acceso no autorizado. Por ejemplo, los agresores pueden acceder de manera no autorizada adivinando los nombres de usuario y las contraseñas gracias a un diccionario de cadenas comunes. Los agresores pueden deducir las contraseñas con algoritmos. También es posible interceptar las contraseñas si se transmiten en abierto.

Una vez adivinados el nombre de usuario y la contraseña correspondiente, el agresor podrá acceder a los recursos de la organización. El nivel de acceso depende de los privilegios de la cuenta agredida. El nivel de daños que se pueden infligir a la organización depende de la voluntad del agresor. En muchos casos, los piratas atacan una cuenta para instalar una puerta trasera en la empresa.

Los protocolos de acceso distante al correo electrónico, como IMAP, POP3 y POP2 utilizan técnicas de autentificación de nombre de usuario y contraseña simples. Estos protocolos pueden emplearse para facilitar los ataques de fuerza bruta. Existen métodos para que los agresores puedan explotar a distancia los servicios de estos protocolos.

Hay maneras más refinadas de obtener acceso no autorizado. Pueden utilizarse gusanos para lanzar un ataque de falsificación de sistema, en el que un componente de sistema asume la identidad de otro. Por ejemplo, los gusanos pueden aprovechar fallos de la opción de depuración de correo enviado y de .rhosts (por ejemplo, en UNIX) gracias a una autentificación débil. La opción de depuración de correo enviado puede desactivarse. Dejar esta opción activada es un ejemplo de utilización incorrecta.

I.1.2 Falsificación IP

La falsificación IP es un ataque complejo que se aprovecha de las relaciones de confianza. Utilizando técnicas de impostura, el agresor se apropia de los identificadores de un anfitrión a fin de sabotear la seguridad del anfitrión objeto del ataque. El anfitrión objetivo cree que está en comunicación con un anfitrión fiable.

Para este tipo de ataques, el agresor en primer lugar identifica el anfitrión fiable de cuyo identificador se va a apropiar, lo que puede lograrse determinando los patrones de confianza del anfitrión. Esto conlleva normalmente la determinación de la gama de direcciones IP en que confía el anfitrión. El siguiente paso consiste en inhabilitar al anfitrión, ya que el agresor va a apropiarse de sus identificadores. Esto último puede conseguirse empleando técnicas tales como los ataques de inundación SYN TCP.

Los ataques de falsificación IP pueden tener éxito porque resulta sencillo falsificar direcciones IP, y a causa de las limitaciones de las técnicas de autentificación de direcciones basadas en la red. El ataque de falsificación IP se hace a ciegas, pues es posible que el agresor no tenga acceso a las respuestas del anfitrión objetivo. No obstante, el agresor puede realizar comunicaciones bidireccionales, si se manipulan los cuadros de encaminamiento para que se emplee la dirección IP de origen falsificada. Los ataques de falsificación IP suelen utilizarse como un primer paso para otros ataques, como la denegación de servicio (DoS) y las inundaciones.

Cabe decir que la mayoría (aunque no todos) de los ISP y muchas redes de empresa más responsables aplican ahora un filtrado de las direcciones salientes, lo que impide los ataques de falsificación IP directos. Como consecuencia, los agresores se han ocupado acumulando "bot nets" a fin de mantener su anonimato.

I.1.3 Rastreadores de red

En un principio, los rastreadores de red se diseñaron como una ayuda para que los gestores de red pudiesen diagnosticar problemas, realizar análisis o mejorar la calidad de funcionamiento de sus redes. Los rastreadores de red trabajan en un segmento de la red que no está conmutado, como los segmentos conectados a una central. De esta manera, el rastreador puede ver todo el tráfico de ese segmento.

Los antiguos rastreadores leen los encabezamientos de los paquetes del tráfico de red y se centran en la identificación de las características de paquete de bajo nivel, como las direcciones de origen y destino. Sin embargo, los rastreadores actuales pueden decodificar datos de los paquetes en todas las capas del modelo OSI.

Los agresores emplean rastreadores para ver la información de usuario y las contraseñas en los paquetes en redes públicas o privadas. Con estos rastreadores, los agresores pueden obtener información valiosa sobre los nombres de usuario y las contraseñas, principalmente de las aplicaciones como FTP, Telnet, etc., que envían las contraseñas sin criptar. Los protocolos de acceso distante al correo electrónico, como IMAP, POP3 y POP2 utilizan técnicas de autentificación de nombre de usuario y contraseña simples, susceptibles de sufrir ataques de rastreo.

Dado que los usuarios tienden a reutilizar las contraseñas en múltiples aplicaciones y plataformas, los agresores pueden utilizar la información adquirida para acceder a diversos recursos de red, donde su confidencialidad puede verse en peligro. Además, estos recursos también pueden utilizarse como rampas de lanzamiento de otros ataques.

En general, los agresores pueden utilizar rastreadores de red poniendo en peligro la seguridad física de la empresa, lo que equivale a que alguien entre en una empresa y conecte su ordenador portátil a la red. Los mismos riesgos se aplican a las redes inalámbricas, donde cualquier persona desde el aparcamiento puede acceder a la red local de la empresa. Acceder a la red de paquetes principal permite al agresor determinar configuraciones y modos de funcionamiento que pueda aprovechar en un futuro.

I.1.4 Denegación de servicio

Los ataques de denegación de servicio (DoS) tienen por objetivo impedir a los usuarios legítimos de un servicio que utilicen dicho servicio. Los ataques DoS son fáciles de llevar a cabo y causan graves daños. Pueden interrumpir el funcionamiento de una empresa y desconectarla efectivamente del resto del mundo. Los ataques de denegación de servicio distribuidos utilizan recursos de más de una máquina para lanzar un ataque DoS sincronizado a un recurso.

Los ataques DoS pueden adoptar diversas formas y dirigirse a distintos servicios. El objetivo es agotar los recursos de red, servidores, anfitrión y aplicación. Algunos ataques DoS se centran en interrumpir la conectividad de la red. Por ejemplo, el ataque de inundación SYN emplea peticiones de conexión TCP semiabiertas ficticias que agotan la capacidad de memoria del recurso atacado. Este tipo de ataques puede impedir a los usuarios legítimos el acceso a los anfitriones, aplicaciones web y otros recursos de red. Los ataques DoS pueden:

- denegar la conectividad de la red a Internet;
- denegar la disponibilidad de un elemento de red a los usuarios legítimos;
- denegar la disponibilidad de aplicación a los usuarios legítimos.

Los ataques DoS explotan los puntos débiles de la arquitectura del sistema atacado. En algunos casos, se explotan los puntos débiles de muchos protocolos Internet comunes, como el protocolo de mensajes de control Internet (ICMP, *Internet control message protocol*). Por ejemplo, un ataque DoS envía un gran número de paquetes eco (ping) ICMP a una dirección de difusión IP. Los paquetes utilizan una dirección IP falsificada como objetivo potencial. Las respuestas que se devuelven al objetivo pueden paralizarlo. Este tipo de ataques se denominan ataques "smurf". Otros ataques utilizan paquetes UDP, pero se basan en el mismo concepto.

I.1.5 Ataque en cadena

Los ataques en cadena también se conocen como ataques por intromisión. En este caso, el agresor intercepta mensajes durante el intercambio de clave pública entre un servidor y un cliente. El agresor retransmite los mensajes, sustituyendo su clave pública por la solicitada. Los participantes originales creen que mantienen una comunicación entre ellos. El agresor puede simplemente acceder a los mensajes o modificarlos. Pueden utilizarse rastreadores de red para lanzar este tipo de ataques.

I.1.6 Trampillas traseras

Las puertas traseras son un método rápido de acceder a los recursos de red, que:

- Pueden haberse introducido deliberadamente en el sistema por sus diseñadores para disponer de un acceso rápido durante la fase de creación y que no se han cerrado una vez terminado.
- Pueden haberse introducido por los empleados para facilitar la realización de sus tareas.
- Pueden ser parte de la instalación normal del sistema operativo, que no se han eliminado mediante endurecimiento de las combinaciones ID de usuario/contraseña por defecto para la inscripción.
- Pueden haber sido introducidas por empleados hostiles para poder acceder después del cierre.
- Pueden haberse creado por la ejecución de un código malicioso, como un virus.

I.1.7 Impostura

Consiste en fingir ser personal de mantenimiento o programación válido a fin de acceder a la red. Es sólo la punta del iceberg de todas las amenazas que se basan en lagunas de seguridad físicas y fallos humanos. Por ejemplo, el intruso puede modificar datos relacionados con la gestión de la configuración y las capas de señalización de la red, así como la facturación y los datos de uso.

I.1.8 Ataques por respuesta

Este tipo de ataque se da cuando se repite un mensaje, o parte del mismo, para obtener un efecto no autorizado. Por ejemplo, una entidad responde un mensaje válido con información de autentificación para autentificarse.

I.1.9 Modificación de mensajes

La modificación de un mensaje ocurre cuando el contenido de una transmisión de datos se altera sin que se detecte y causa un efecto no autorizado.

I.1.10 Ataques desde el interior

Los ataques desde el interior ocurren cuando usuarios legítimos de un sistema se comportan de manera imprevista o no autorizada. Muchos de los delitos informáticos conocidos cuentan con la participación de usuarios internos que ponen en peligro la seguridad del sistema. Se pueden reducir los riesgos de ataques desde el interior escogiendo cuidadosamente al personal y llevando a cabo una vigilancia constante del hardware, el software y la política de seguridad. También es conveniente llevar un minucioso registro de auditoría para aumentar las posibilidades de detectar este tipo de ataques.

I.2 Amenazas de seguridad

Todas las organizaciones, como las empresas, se enfrentan a diversos tipos de amenazas. Las necesidades de seguridad y la estrategia de seguridad recomendada de cada empresa es diferente y exclusiva. El entorno más necesitado de seguridad es el de la empresa abierta. En este caso, debe protegerse toda la empresa a fin de controlar el acceso de los empleados, los socios e incluso los clientes a las bases de datos y aplicaciones de la empresa.

I.2.1 Ataques en la capa de aplicación

Los ataques en la capa de aplicación pueden adoptar diversas formas y emplear distintos métodos. Dado que los anfitriones web son accesibles por el público en general por direcciones de puerto conocidas, especificadas por protocolos como HTTP (puerto 80), los piratas pueden aprovechar estas direcciones para lanzar ataques capaces de atravesar los cortafuegos.

Los ataques en la capa de aplicación explotan las vulnerabilidades del sistema operativo y las aplicaciones a fin de acceder a los recursos. Una mala configuración y autorización pueden causar brechas de seguridad. Por ejemplo, un anfitrión puede ser un servidor web y debe proporcionar a todo el mundo las páginas web requeridas. En la política de seguridad se podría especificar que los anfitriones restrinjan el acceso al intérprete de instrucciones a los administradores.

La cosecha de cuentas tiene por objetivo el proceso de autentificación cuando una aplicación pide a un usuario su ID y contraseña. Las aplicaciones que generan distintos mensajes de error cuando se utilizan ID de usuario y contraseñas erróneas son vulnerable a este tipo de ataques. De acuerdo con el tipo de mensaje de error, el intruso puede adaptar el ataque para determinar en primer lugar un ID de usuario válido y a continuación utilizar otro tipo de técnicas para obtener la contraseña.

Los ataques en la capa de aplicación pueden basarse en virus, gusanos, desbordamiento de la memoria intermedia, cosecha de contraseñas, etc. Los servicios web y la tecnología de firma única no han hecho más que agravar el problema, pues tienden a habilitar en la red aplicaciones

heredadas. Estas aplicaciones no se diseñaron teniendo en cuenta la conectividad a la web y la seguridad.

Algunos ataques en la capa de aplicación sólo pretenden desmantelar un sitio web. Otros ataques envenenan las cookies de un sitio web para obtener ilegalmente información sobre un servidor concreto. Por norma general, las aplicaciones no verifican la validez de las cookies y pueden ser víctimas de códigos maliciosos ocultos en ellas. Son conocidas las vulnerabilidades de algunos navegadores actuales que permiten los ataques por cookies.

Un agresor puede también emplear el lenguaje de guiones para insertar un código malicioso bajo la apariencia de un guión añadido a una URL. El código se ejecutará cuando un usuario haga clic en esa URL. TLS puede solucionar algunos de los problemas de seguridad en la capa de aplicación. Sin embargo, SSL no protege por completo las aplicaciones web. Aun cuando se utiliza SSL pueden seguir lanzándose ataques como la cosecha de cuentas y la obtención ilícita de contraseñas.

A fin de reducir las amenazas de ataques en la capa de aplicación, se recomienda endurecer todos los sistemas operativos utilizados en la gestión de red, ya sean generales o sistemas operativos en tiempo real incorporados. Han de seguirse las directrices de endurecimiento actualizadas y específicas del fabricante. Es posible que los fabricantes no puedan facilitar parches para algunos sistemas heredados que emplean sistemas operativos más antiguos. También se recomienda utilizar el correo electrónico seguro, cortafuegos en la capa de aplicación, sistemas de prevención y detección de intrusión, técnicas de autentificación sólidas, contraseñas fuertes y un adecuado control de salida en los sitios web a fin de impedir la visualización de modificaciones no autorizadas del contenido web.

I.2.2 Ataques en la capa de red

Los agresores pueden utilizar las herramientas habituales para lanzar ataques en la capa de red, cuya gravedad puede variar. Las empresas extendidas y abiertas son especialmente vulnerables a los ataques en la capa de red. Hay una serie de graves amenazas de seguridad asociadas comúnmente a la infraestructura de red. Estas amenazas incluyen el sabotaje, el vandalismo, la mala configuración del sistema y la denegación de servicio, la curiosidad, el espionaje industrial y el robo de servicio. Los ataques pueden ser fruto de usuarios internos, que los lanzan desde la misma red, o de fuentes externas, como los piratas.

Las tecnologías de piratería más recientes, como los analizadores de puerto en terminales móviles, demuestran que los ataques a la red pueden lanzarse también desde terminales móviles. Se recomienda formular una buena política de seguridad y un proceso de seguridad comprensible a fin de proteger la infraestructura de red. Los conmutadores, encaminadores, puntos de acceso, servidores de acceso a distancia, puntos de acceso inalámbricos, anfitriones y otros tipos de recursos son elementos que, por regla general, cabe proteger.

A continuación se exponen las amenazas y vulnerabilidades de la infraestructura de red, típicas de las redes de paquetes IP:

1) Proliferación de protocolos inseguros: Algunas redes siguen utilizando protocolos conocidos por tener vulnerabilidades de seguridad, como: ICMP, TELNET, SNMPv1&2, DHCP, TFTP, RIPv1, NTP, DNS y HTTP.

2) Utilización de contraseñas, débiles, estáticas, gestionadas a nivel local: Algunas redes siguen permitiendo la utilización de contraseñas débiles basadas en palabras comunes, cortas, fáciles de adivinar. Algunos administradores pueden utilizar una contraseña para todos los elementos de red, que pueden ser compartidos, y, por tanto, conocidos de todos los administradores.

3) Información de seguridad desprotegida: En algunas redes, la información crítica, como los ficheros de contraseñas, no está criptada. Otro tipo de información, como las contraseñas, se transmite en abierto por la red. Los parámetros de los cortafuegos están mal configurados y se emplean claves criptográficas débiles.

4) Ficheros de configuración y descargas de software no autorizados: Las redes pueden verse amenazada por la descarga de un software incorrecto o malicioso, o los ficheros de configuración pueden causar la pérdida del servicio y resultar en una baja calidad de funcionamiento. Esto abre grietas de seguridad por las que usuarios internos y externos pueden instalar caballos de Troya u otro tipo de código malicioso. También se configuran erróneamente los dispositivos.

5) Elementos de red y sistemas operativos no endurecidos: Las amenazas a la red pueden resultar de descargas de sistemas operativos por defecto que no están endurecidos contra los ataques comunes. Esto incluye la ejecución de servicios innecesarios, que dejan habilitadas las cuentas y contraseñas.

6) Puertos e interfaces gestionados innecesariamente expuestos a la red pública: Las amenazas pueden proceder de las interfaces de gestión en banda a las que se puede acceder desde el Internet público. Otras amenazas pueden proceder de abusos de los mecanismos de soporte, como el acceso a la red principal en modo soporte por marcación, RDSI u otro tipo de conexión.

I.2.3 Acceso no autorizado

Acceso no autorizado es un término que puede referirse a toda una serie de ataques. La meta final del agresor es acceder ilegalmente a un recurso. Este problema de seguridad afecta a todos los tipos de empresa. Toda empresa que habilite el acceso a Internet o a la LAN a distancia es susceptible de sufrir ataques de acceso no autorizado.

Los servicios de acceso a distancia que permiten a los empleados en desplazamiento acceder por marcación al correo electrónico, conectarse a la oficina a distancia por líneas de marcación, intranets y extranets que conectan terceros a la red de empresa, pueden vulnerabilizar la red de cara a los piratas, los virus y otro tipo de agresiones. Los piratas pueden emplear las herramientas habituales para acceder a la red de empresa, poniendo en peligro información sensible o utilizando la red para lanzar ataques contra otras redes.

La protección de la red a diversos niveles puede contribuir a evitar el acceso no autorizado. En la capa de red, los cortafuegos, servidores intermediarios y el filtrado usuario a sesión pueden aportar protección adicional, pero los piratas siguen logrando superarlos. También pueden minimizarse los riesgos de acceso no autorizado aplicando un control de acceso de usuarios en las capas de red y aplicación con el grado de autentificación y autorización necesario.

I.2.4 Escucha

La escucha es una amenaza difícil de detectar. El objetivo del agresor es escuchar y, más exactamente, registrar datos brutos en la LAN de empresa. Este ataque utiliza el "modo promiscuo" de los adaptadores Ethernet que se encuentran en el mercado. Este modo permite a un agresor capturar todos los paquetes de la red. Hay muchos rastreadores de red gratuitos en la web que los agresores pueden emplear para realizar una escucha.

Cualquier empresa que permite el acceso a distancia es vulnerable a este tipo de ataque. Las empresas abiertas y extendidas son las que más riesgos corren. La conmutación Ethernet es completamente ineficaz contra las amenazas de escucha, pues la falsificación de ARP puede pervertir completamente el mecanismo de conmutación. La conmutación Ethernet sólo es efectiva contra las "escuchas pasivas". Se pueden minimizar las amenazas de ataques de este tipo utilizando técnicas de gestión de acceso robustas y criptación.

Apéndice II

Disciplinas de las tecnologías de ciberseguridad

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

La complejidad y eficacia de las tecnologías de ataque crecen constantemente. Hoy en día, los intrusos pueden desarrollar rápidamente ataques dirigidos a explotar las vulnerabilidades descubiertas en los productos. Los agresores pueden automatizar estos ataques y ponerlos a disposición del público en general. En el cuadro II.1 se muestran los distintos campos de las tecnologías disponibles para luchar contra las ciberamenazas.

Cuadro II.1 – Tecnologías de ciberseguridad

Técnicas	Categoría	Tecnología	Objetivo
Criptografía	Certificado y arquitectura de clave pública	Firma digital	Se utiliza para permitir la expedición y mantenimiento de certificados que se utilizarán en las comunicaciones digitales
		Criptación	Criptación de los datos durante la transmisión o el almacenamiento
		Intercambio de claves	Determina si se va a utilizar una clave de sesión o una clave de transacción para asegurar una conexión
	Seguro	Criptación	Garantiza la autenticidad de los datos
Control de acceso	Protección del perímetro	Cortafuegos	Controla el acceso desde y hacia una red
		Gestión de contenido	Supervisa el tráfico de información no conforme
	Autentificación	Factor único	Un sistema que utiliza combinaciones de ID de usuario/contraseña para verificar el identificador
		Doble factor	Un sistema que requiere dos componentes para otorgar a un usuario acceso al sistema, como la posesión de un testigo físico además del conocimiento de un secreto
		Triple factor	Añade otro factor de identificación como características biométricas o la medición de una característica corporal
		Testigos inteligentes	Establece identificadores fiables de los usuarios mediante un circuito específico de un dispositivo, como una tarjeta inteligente
	Autorización	Por función	Mecanismos de autorización que controlan el acceso de los usuarios a los recursos del sistema adecuados, de acuerdo con su función asignada
		Por regla	Mecanismos de autorización que controlan el acceso de los usuarios a los recursos del sistema adecuados, de acuerdo con reglas específicas asociadas a cada usuario, independientemente de su función dentro de la organización

Cuadro II.1 – Tecnologías de ciberseguridad

Técnicas	Categoría	Tecnología	Objetivo
Integridad del sistema	Antivirus	Métodos de firma	Protege contra los códigos informáticos maliciosos, como los virus, gusanos y caballos de Troya utilizando sus firmas de código
		Métodos de comportamiento	Verifica que los programas que se ejecutan no tengan un comportamiento no autorizado
	Integridad	Detección de intrusión	Puede utilizarse para advertir a los administradores de red de la posibilidad de que ocurra un incidente de seguridad, como la puesta en peligro de archivos en un servidor
Auditoría y supervisión	Detección	Detección de intrusión	Compara el tráfico de red y los registros cronológicos de entrada del anfitrión para encontrar firmas de datos indicativas de piratas
	Prevención	Prevención de intrusión	Detecta ataques en una red y toma las medidas especificadas por la organización para contrarrestar los ataques. Las actividades sospechosas disparan las alarmas del administrador, así como otras respuestas configurables
	Registro cronológico	Herramientas de registro cronológico	Supervisa y compara el trafico de red y los registros cronológicos de entrada del anfitrión para encontrar firmas de datos y perfiles de dirección de anfitrión indicativos de piratas
Gestión	Gestión de red	Gestión de configuración	Permite el control y la configuración de las redes y la gestión de fallos
		Gestión de parches	Instala las últimas actualizaciones y arreglos de dispositivos de red
	Política	Observancia	Permite a los administradores supervisar e imponer las políticas de seguridad

II.1 Criptografía

La criptografía consiste en transformar datos simples para cifrarlos con un código secreto. Descifrando los datos secretos se puede recuperar el texto original. Las actuales técnicas de criptografía pueden utilizarse para cifrar/descifrar datos, así como para autentificar el origen de un mensaje y para el no repudio.

La criptografía desempeña un importante papel en la protección de la información almacenada en un dispositivo u otro medio de almacenamiento, y durante su transmisión a través de un enlace de comunicaciones.

En criptografía, el cifrado de los datos con código secreto utilizando algoritmos matemáticos se denomina criptación. Por otro lado, la función inversa, la decriptación de los datos, se aplica a los datos criptados para volver a obtener los datos originales. La criptografía utiliza claves secretas para los procesos de criptación y decriptación.

Las técnicas criptográficas pueden ser de dos tipos básicos: de clave simétrica y de clave asimétrica.

1) La criptografía de clave simétrica utiliza algoritmos en que la clave de criptación y la clave de decriptación son idénticas. La seguridad del modelo depende de la dificultad de adivinar la clave. Las partes en comunicación deben llegar a un acuerdo sobre la clave y mantenerla en secreto. Entre los algoritmos de clave simétrica se encuentran la norma de criptación de

datos triple (3DES, *triple data encryption standard*) y la norma de criptación avanzada (AES, *advanced encryption standard*).

2) La criptografía de clave asimétrica utiliza algoritmos que emplean una clave para criptar los datos y otra distinta para decriptar el texto cifrado. En este tipo de criptografía, el usuario tendrá una clave privada sólo conocida por él mismo y una clave pública que pueden conocer los demás. La clave pública la utilizan los demás usuarios para criptar el texto original y sólo el detentor de la correspondiente clave privada podrá decriptar los datos.

Por norma general, las técnicas de criptografía de clave simétrica son más rápidas de aplicar que las asimétricas. No obstante, la principal complicación de la criptografía de clave simétrica es la distribución de las claves. Por tanto, normalmente no sirven para utilizarlas a gran escala. Por otro lado, la criptografía de clave asimétrica (también conocida como criptografía de clave pública) solventa algunas de las limitaciones de gestión de claves de la criptografía de clave simétrica. La criptografía de clave pública se asienta en la utilización de certificados digitales para la gestión y revocación de claves públicas. A fin de mejorar la velocidad de cálculo, pueden utilizarse las técnicas de criptografía de clave pública como medio para intercambiar de manera segura una clave simétrica para utilizarla en una sesión o transacción.

Las firmas digitales son ejemplos de aplicación práctica de la tecnología criptográfica de clave pública. Un certificado digital garantiza la asociación entre una clave pública y el detentor del certificado. Las firmas digitales sirven para la autentificación, la integridad de los datos y el no repudio de las transacciones. Las firmas digitales pueden utilizarse para corroborar la supuesta identidad del emisor de un mensaje. A menudo se utilizan junto con certificados digitales. Éstos se utilizan como vehículo que transporta la información necesaria para la criptografía de clave pública y las firmas digitales. Las autoridades aprobadas o fiables pueden expedir certificados digitales a los usuarios.

El código de autentificación de mensaje (MAC, *message authentication code*) es una verificación de suma de autentificación que se deriva aplicando un esquema de autentificación, además de una clave secreta, al mensaje. Por oposición a las firmas digitales, un MAC se calcula y verifica utilizando la misma clave. Así, el MAC sólo puede ser verificado por el destinatario deseado. En las funciones de aleatorización basadas en MAC (HMAC, *hash función based MAC*) (véase [b-IETF RFC 2104]) se utiliza una clave (o claves) con una función de aleatorización para obtener una verificación de suma que se anexa al mensaje.

II.2 Tecnologías de control de acceso

El control de acceso se focaliza en garantizar que sólo los usuarios autorizados pueden acceder a un dispositivo de red o un sistema anexo. De hecho, el control de acceso permite a los profesionales de TI analizar y entender mejor el tipo y naturaleza de los ataques que sufre la red. Hay muchas técnicas que pueden utilizarse para controlar el acceso. Estos métodos se exponen en las siguientes subcláusulas.

II.2.1 Protección del perímetro

La tecnología de protección del perímetro impide el acceso a la red de cualquier usuario externo no autorizado o no fiable. Esta tecnología instala una frontera lógica o física entre las zonas protegidas y las que están abiertas al público y los usuarios externos no fiables (pero no los usuarios internos no fiables). La protección del perímetro puede aplicarse para proteger una red o un único dispositivo. Las tecnologías de protección del perímetro comprenden:

1) Software de filtrado del contenido o de gestión del contenido que restringe el tipo de datos a los que se puede acceder o que se pueden distribuir en una red (véase [b-ISO/CEI 10828-3]). Restringe la capacidad de los usuarios de acceder al contenido más allá de su frontera. Así se minimizan las posibilidades de descargar virus y otro tipo de códigos maliciosos procedentes de ubicaciones no fiables. El filtrado del contenido puede hacerse

con filtros URI (véase [IETF RFC 2396]), que pueden negar el acceso de los usuarios a páginas web con contenido dudoso. El filtrado del contenido puede utilizarse para examinar mensajes de aplicación, como los correos electrónicos, en busca de virus o contenido no permitido.

2) Cortafuegos: Esta tecnología (véase [b-ISO/CEI 10828-3]) puede dividirse en cuatro grandes categorías: filtros de paquetes, pasarelas a nivel de circuito, pasarelas a nivel de aplicación y cortafuegos de inspección multicapa por estados.

- Los cortafuegos de filtrado de paquetes funcionan en la capa IP. Generalmente forman parte de un cortafuegos encaminador. Comparan cada paquete IP con una regla definida establecida antes de remitirlo al siguiente camino o a su destino final. Dependiendo del resultado de la comparación, el cortafuegos puede descartar el paquete, remitirlo o enviar un mensaje a su origen. Las reglas pueden incluir las direcciones IP de origen y destino, el número de puerto de origen y destino y el protocolo utilizado. Los encaminadores de traducción de dirección de red (NAT, *network address translation*) ofrecen las ventajas de los cortafuegos de filtrado de paquetes y también pueden ocultar las direcciones IP de los dispositivos que se encuentran detrás del cortafuegos. Los cortafuegos de filtrado de paquetes tienen poca repercusión en la calidad de funcionamiento de la red y dan cierto grado de seguridad en la capa de red.
- Las pasarelas a nivel de circuito trabajan en la capa TCP del TCP/IP para supervisar la toma de contacto TCP entre paquetes a fin de descubrir si la sesión requerida es legítima o no. Además, las peticiones enviadas a un ordenador distante a través de la pasarela a nivel de circuito aparecerán ante el receptor como si tuvieran su origen en la pasarela. Esta técnica contribuye a ocultar información de la red protegida. Las pasarelas a nivel de circuito no filtran paquetes individuales.
- Los intermediarios o las pasarelas a nivel de aplicación pueden filtrar paquetes en la capa de aplicación del modelo OSI. Las peticiones entrantes o salientes no pueden acceder a los servicios que no tienen intermediario. Los intermediarios examinan los paquetes en la capa de aplicación para filtrar instrucciones específicas de la aplicación como HTTP POST (véase [b-IETF RFC 2616]). Un intermediario no permitirá que el tráfico no configurado alcance la aplicación. También pueden utilizarse los intermediarios para registrar cronológicamente las actividades e inscripciones de los usuarios. Los intermediarios pueden proporcionar un alto nivel de seguridad y repercutir significativamente en la calidad de funcionamiento de la red.
- Los cortafuegos de inspección multicapa basada en estados combinan las características de los cortafuegos antedichos. Los cortafuegos multicapa filtran paquetes en la capa de red, determinan si los paquetes de sesión son válidos y filtran el contenido de los paquetes en la capa de aplicación. Los cortafuegos multicapa son transparentes a las conexiones entre emisor y receptor.

3) Traducción de dirección de red (NAT): Esta tecnología da la capacidad de ocultar el esquema de direccionamiento de la red detrás de un cortafuegos. En NAT, se establece la correspondencia entre la dirección IP de un sistema de la red interna y una dirección IP encaminable externa correspondiente. Con NAT es posible que muchos sistemas detrás de un cortafuegos compartan la misma dirección IP externa. Los recursos detrás del cortafuegos seguirán siendo accesibles para los usuarios externos mediante el reenvío por conexiones internas a través de determinados números de puerto. La NAT puede aplicarse en la mayoría de dispositivos de red, como los conmutadores, los encaminadores y los cortafuegos.

4) Pasarelas a nivel de aplicación: Estos sistemas (véase [b-ISO/CEI 10828-3]) están formados por un dispositivo o un conjunto de dispositivos con hardware y software. Están diseñados para restringir el acceso entre dos redes separadas. Estos sistemas utilizan la inspección de

paquetes basada en estados y las técnicas de intermediario de aplicación para restringir el acceso entre redes. También pueden utilizarse combinaciones y variaciones (por ejemplo, cortafuegos a nivel de circuito) de estas técnicas. Además, es asimismo posible que las pasarelas a nivel de aplicación apliquen la NAT.

5) Intermediario de aplicación: Estos sistemas (véase [b-ISO/CEI 10828-3]) supervisan los intentos de conexión a nivel de aplicación mediante el examen de los paquetes en la capa más alta de la pila de protocolo. Los intermediarios de aplicación tienen plena visibilidad de los intercambios de datos en la capa de aplicación. Esta capacidad les permite ver fácilmente e inmediatamente los detalles granulares de cada intento de conexión y aplicar las políticas de seguridad que se impongan. Los intermediarios de aplicación tienen la capacidad de poner fin a las conexiones cliente e iniciar una nueva conexión con una red protegida interna. Esto da más seguridad, ya que separa los sistemas internos y externos.

II.2.2 Red virtual privada (VPN, *virtual private network*)

En [b-ISO/CEI 18028-5] se pueden encontrar los detalles de la utilización de las VPN para asegurar las comunicaciones en las redes.

En la actualidad, las VPN se utilizan para interconectar redes y como método de conectar los usuarios distantes a las redes. Las VPN, en su forma más simple, ofrecen un mecanismo de establecimiento de canal o canales de datos seguros en una red existente o en conexiones punto a punto. Las VPN pueden crearse o eliminarse dinámicamente. La red anfitriona puede ser pública o privada.

El acceso a distancia a través de una VPN se lleva a cabo por encima de una conexión punto a punto normal ya establecida entre el usuario local y la ubicación distante (véase [b-ISO/CEI 18028-5]). Las VPN pueden utilizarse como un servicio gestionado según el cual se proporcionan a una infraestructura compartida conectividad, gestión y direccionamiento seguro y fiable, equivalentes a los de una red privada.

Hay diversas formas de representar tipos de VPN (véase [b-ISO/CEI 18028-5]). En principio, una VPN puede ser:

– una única conexión punto a punto (por ejemplo, un dispositivo de cliente que accede a distancia a una red de empresa a través de una pasarela); o

– una conexión punto a nube (utilizando las técnicas).

Hay tres tipos principales de VPN (véase [b-ISO/CEI 18028-5]):

– Las VPN de capa 2 emulan una LAN al utilizar las conexiones VPN activas con una red anfitriona para enlazar los sitios de una empresa o para establecer una conexión distante con una organización. Las ofertas de proveedores típicas incluyen el servicio alámbrico privado virtual (VPWS, *virtual private wire service*), que proporciona una conexión sólo alámbrica simulada, o el servicio del LAN privada virtual (VPLS, *virtual private LAN service*), que proporciona un servicio LAN emulado más completo.

– Las VPN de capa 3 emulan una WAN al utilizar las conexiones VPN activas con una infraestructura de red. Ofrecen la capacidad de utilizar esquemas de direccionamiento IP privados en una infraestructura pública, práctica que no estaría permitida de utilizarse conexiones IP públicas. No obstante, la utilización de direcciones privadas en redes públicas gracias a la NAT puede complicar el establecimiento y utilización de IPSec (véase [b-IETF RFC 2411]).

– Las VPN de capa 4 se utilizan para asegurar las transacciones que se llevan a cabo en redes públicas. Este tipo de conexiones VPN suelen establecerse mediante TCP, que es el protocolo de capa 4. Este tipo de VPN establece un canal seguro entre las aplicaciones en comunicación para garantizar la confidencialidad y la integridad de los datos durante la transacción.

Las VPN pueden implementarse dentro de una red privada bajo el control de la empresa propietaria, o en redes del dominio público. También es posible combinar estos dos esquemas. Por otra parte, los canales pueden establecerse empleando canales seguros utilizando los túneles activos en las redes del proveedor de servicio Internet. En este caso, el Internet público es efectivamente el sistema de transporte subyacente, por lo que hay más riesgos para la confidencialidad de los datos transportados por la VPN.

Un túnel es un trayecto de datos entre dispositivos conectados en red, que se establece dentro de una infraestructura de red existente. El túnel es transparente para las operaciones de red. Una VPN creada con túneles es en general más flexible que una red basada en enlaces físicos. Los túneles pueden crearse utilizando circuitos virtuales, la conmutación por etiquetas o la encapsulación de protocolo.

En el cuadro II.2.2 se presentan los aspectos de seguridad de los distintos tipos de VPN (véase [b-ISO/CEI 18028-5]).

Cuadro II.2.2 – Aspectos de seguridad de la VPN

VPN	Tecnología	Autentificación de usuario	Criptación de datos	Gestión de claves	Verificación de la integridad
VPN de capa 2	Retransmisión de tramas, ATM, MPLS, PPP, L2F	N/A	N/A	N/A	N/A
	L2TP (véase [b-IETF RFC 2661])	Tipo CHAP	N/A	N/A	N/A
VPN de capa 3	IPSec	Clave secreta precompartida (de paquete) basada en certificado	Varios algoritmos negociables (paquete)	IKE	Negociable
	IPSec con L2TP	Clave secreta precompartida (de paquete) basada en certificado	Varios algoritmos negociables (paquete)	IKE	Negociable
	MPLS	N/A	N/A	N/A	N/A
VPN de capa 4	TLS	Basada en certificado	Negociable	Negociable	Negociable
	Intérprete de comandos seguro	Par de claves generado por el sistema (no certificado)	Negociable	Intercambio de claves públicas con el emisor de datos	Negociable

NOTA 1 – En vez de TLS, puede utilizarse SSL.

NOTA 2 – [b-IETF RFC 3031] presenta los aspectos generales de la arquitectura de conmutación por etiquetas multiprotocolo (MPLS, *multiprotocol label switching architecture*). En [b-IETF RFC 1661] se describe el protocolo punto a punto (PPP, *point-to-point protocol*). En [b-IETF RFC 2427] se trata de la interconexión multiprotocolo con la retransmisión de tramas.

II.2.3 Autentificación

Pueden utilizarse diversos métodos para autentificar a un usuario, entre ellos, las contraseñas, los pases con validez limitada, las técnicas biométricas, las tarjetas inteligentes [b-ISO/CEI 7816-x] y los certificados. La autentificación basada en contraseñas debe utilizar contraseñas fuertes (por ejemplo, de, al menos, ocho caracteres con, como mínimo, un carácter alfabético, uno numérico y un carácter especial). Es posible que la autentificación por contraseña no sea suficiente, De acuerdo con la evaluación de vulnerabilidad, es posible que sea necesario combinar la autentificación por contraseña con otros procesos de autentificación y autorización como los certificados, el protocolo ligero de acceso al directorio (LDAP, *lightweight directory access protocol*), (véase [b-IETF RFC 3377]), el servicio de usuario de marcación de autentificación a distancia (RADIUS, *remote authentication dial-in user service*) (véanse [b-IETF RFC 2869], [b-IETF RFC 3579] y [b-IETF RFC 3580]), Kerberos (véase [b-IETF RFC 1510]), y la infraestructura de clave pública (PKI, *public key infrastructure*) (véase [b-IETF RFC 2459]).

Los sistemas de autentificación pueden clasificarse de acuerdo con el número de factores de identificación necesarios. La autentificación de factor único se refiere a un sistema que utiliza un solo factor (combinaciones de ID de usuario/contraseña). La autentificación de doble factor describe un proceso que requiere dos componentes para acceder al sistema, como la posesión de un testigo físico y el conocimiento de un secreto (por ejemplo, una contraseña). La autentificación de triple factor añade otro factor de identificación, que puede ser biométrico o la medición de una característica corporal. El empleo de más factores de autentificación da como resultado una autentificación más segura, aunque el mayor número de factores añade complejidad, aumenta el coste y complica la gestión. El principal reto de cualquier sistema de autentificación reside en llegar al equilibrio óptimo entre sencillez y seguridad.

Hoy en día la autentificación de factor único ID de usuario/contraseña es el sistema más utilizado. Los sistemas de autentificación por contraseña son sencillos, fáciles de administrar y muy conocidos por los usuarios. Si se utilizan contraseñas fuertes, los sistemas de autentificación de factor único proporcionan un alto grado de seguridad. Sin embargo, los sistemas por contraseña tradicionales han planteado ciertos problemas, ya que los usuarios tienen dificultades para recordar múltiples contraseñas fuertes. Como se tratará más adelante, estas desventajas pueden minimizarse a fin de encontrar una solución óptima con un sistema de "contraseña fuerte única".

En muchos sistemas de autentificación se añaden, como segundo factor, testigos tales como las tarjetas inteligentes. Los testigos aportan seguridad a la autentificación, ya que el usuario ha de demostrar que posee físicamente el testigo antes de ser autentificado. Cualquier agresor debería, del mismo modo, disponer del testigo del usuario para acceder al sistema. Cuanto más alto sea el nivel de la autentificación, más costoso será el sistema, debido a la necesidad de testigos y lectores de testigos. Además, resulta fácil perder los testigos, lo que representará una carga adicional para la administración que deba reexpedirlos.

Puede conseguirse una autentificación criptográficamente fuerte utilizando certificados digitales expedidos a los usuarios y almacenados en testigos o en la memoria del ordenador del usuario. Se emplean algoritmos criptográficos para garantizar que un determinado certificado ha sido legítimamente expedido al usuario. La infraestructura de clave pública se utiliza para la expedición y mantenimiento de los certificados digitales. Los sistemas criptográficamente fuertes aseguran una autentificación muy fuerte, pero son muy onerosos y suponen una carga administrativa adicional, por lo que en la actualidad sólo se utilizan en entornos muy seguros.

II.2.4 Autorización

Una vez realizada la autentificación, los mecanismos de autorización controlan el acceso de los usuarios a los recursos del sistema adecuados. La autorización puede clasificarse de acuerdo con la granularidad del control, es decir, en función del nivel de detalle con que se dividen los recursos del

sistema. La autorización de grano fino se refiere, en general, a un sistema que controla el acceso a puntos muy específicos, como aplicaciones o servicios individuales.

La autorización es con frecuencia "dependiente de la función", por lo que el acceso a los recursos del sistema se basa en la función que se ha asignado a la persona dentro de la organización. La función de administrador del sistema puede tener un acceso muy privilegiado a todos los recursos del sistema, mientras que la de usuario general sólo tendrá acceso a un subconjunto de estos recursos. De aplicarse la autorización de grano fino, la función de administrador de recursos humanos puede tener acceso exclusivo a las bases de datos de recursos humanos altamente confidenciales, y la función de contable acceso exclusivo a las bases de datos del sistema de contabilidad.

La autorización también puede ser "dependiente de la regla" si el acceso a los recursos del sistema se basa en reglas específicas asociadas con cada usuario, independientemente de su función dentro de la organización. Por ejemplo, pueden crearse reglas que permitan acceso de sólo lectura o acceso de lectura/escritura a determinados ficheros del sistema.

II.2.5 Protocolos de autentificación y autorización

Para los servicios de autentificación se han adoptado diversos protocolos comunes. El protocolo RADIUS (servicio de usuario de marcación de autentificación a distancia) (véase [b-IETF RFC 2865]) es muy utilizado para centralizar los servicios de autentificación por contraseña. Diseñado en su origen para autentificar a los usuarios de marcación a distancia, el protocolo RADIUS se ha adoptado para los servicios de autentificación de usuarios en general. El LDAP (protocolo ligero de acceso al directorio) se utiliza mucho en los sistemas de autentificación y autorización. El LDAP es un método cómodo de almacenar las credenciales de autentificación y autorización de usuarios.

Con frecuencia, los servidores de autentificación RADIUS van unidos al almacenamiento de credenciales en directorios LDAP a fin de centralizar el sistema de autentificación y autorización. Cuando un usuario intenta acceder a una aplicación concreta del sistema, ésta pedirá las credenciales de autentificación del usuario y las reenviará al sistema centralizado. El servidor RADIUS verificará entonces las credenciales presentadas comparándolas con las almacenadas en la base de datos LDAP y pedirá a ésta que autorice la información de regla de autorización. Los resultados de la autentificación (positivo o negativo) se devuelven a la aplicación junto con la información de regla de autorización para ese usuario. Las reglas de autorización se aplicarán en la aplicación a fin de permitir al usuario acceder a datos o servicios concretos. Desde el punto de vista del usuario extremo, se prevé que estos sistemas de autentificación y autorización sean automáticos y fáciles de utilizar.

II.3 Antivirus e integridad del sistema

Los gusanos, códigos maliciosos, virus y caballos de Troya pueden modificar un sistema y sus datos, por lo que es fundamental utilizar tecnologías de búsqueda de virus que garanticen la preservación de la integridad del sistema.

Un gusano es un programa que se reproduce replicándose de un sistema a otro sin necesidad de intervención humana. Los virus pueden anexarse a ficheros de usuario y despertarse replicándose en otros ficheros cuando un usuario cualquiera realice una acción, como abrir un fichero infectado. Por otra parte, el caballo de Troya suele presentarse al usuario como un programa útil que oculta un código dañino.

La tecnología antivirus contribuye a proteger los sistemas contra ataques por gusanos, códigos maliciosos y caballos de Troya. El software puede instalarse en los dispositivos del usuario o prestarse como servicio de la red o el proveedor de servicio Internet. Las técnicas de integridad del sistema utilizan software que verifica que sólo se realizan en los ficheros de sistema fundamentales las actualizaciones autorizadas.

Los software antivirus pueden utilizar técnicas de firmas en cadena para identificar los virus y códigos maliciosos. Esta técnica requiere un conocimiento previo de los códigos maliciosos para que el software antivirus pueda detectarlos, por lo que la base de datos de firmas debe mantenerse al día para que la protección sea efectiva.

Los exploradores de actividad verifican las actividades no autorizadas realizadas por un código de ejecución. El software notifica al usuario las actividades sospechosas. Los exploradores activos suelen tener un éxito limitado contra los virus, pero pueden ser más eficaces contra los gusanos y caballos de Troya. Los exploradores estáticos heurísticos analizan el código para intentar identificar actividades que pueden asociarse con el comportamiento de un virus.

Las técnicas de integridad del sistema utilizan software que supervise las modificaciones realizadas en los ficheros de sistema fundamentales. Estas técnicas pueden utilizarlas los administradores de TI para verificar el sistema y determinar si los piratas han logrado introducirse con éxito en el sistema (los piratas suelen dejar puertas traseras).

II.4 Auditoría y supervisión

Las técnicas de auditoría y supervisión permiten a los administradores de TI evaluar la seguridad global de sistema, incluyen el software de detección de instrucciones y prevención. Los administradores de TI pueden recurrir a esta tecnología para analizar el sistema a fin de determinar su debilidad después de un ataque. En algunos casos, el análisis del sistema puede realizarse durante un ataque activo al sistema.

El sistema de detección de intrusión (IDS, *intrusion detection system*) (véase [b-ISO/CEI 18043]) puede emplearse para supervisar la red con el objetivo de garantizar que ningún usuario no autorizado acceda a la red. La mayoría de las aplicaciones IDS comparan el tráfico de red y las entradas del registro cronológico del anfitrión para encontrar firmas y perfiles de dirección de anfitrión indicativos de piratas. El software de detección de intrusión identifica patrones de tráfico que indican la presencia de usuarios no autorizados. Las actividades sospechosas disparan las alarmas de administrador y otras respuestas configurables. El sistema de detección de intrusión (IDS) puede clasificarse a grandes rasgos de acuerdo con los siguientes criterios:

- plano de detección de incidentes: tiempo real o fuera de línea, dependiendo de si los registros cronológicos del sistema y el tráfico de red se analizan a medida que ocurren o globalmente en las horas fuera de servicio;
- tipo de instalación: en red o en anfitrión. Un IDS en red suele contar con múltiples supervisores (generalmente dispositivos preconfigurados) instalados en estrechamientos de la red (donde todo el tráfico entre dos puntos puede supervisarse). Un IDS en anfitrión necesita que se instale el software directamente en los servidores que se han de proteger y que supervise las conexiones de red y actividades de usuario de dichos servidores; y
- tipo de reacción ante incidentes: el IDS interviene activamente para contrarrestar un ataque (modificando las reglas del cortafuegos o los filtros del encaminador) o simplemente notifica el problema al personal o a otros sistemas de la red.

La mayoría de los productos IDS del mercado ofrecen una combinación de capacidades de supervisión en red y en anfitrión con un anfitrión de gestión central que recibe los informes de los distintos supervisores y alertan al personal de apoyo de la red. Se recomienda la utilización de un IDS en red para la mayoría de instalaciones en red, dependiendo de las necesidades particulares del cliente.

II.5 Gestión

Las técnicas de gestión de la configuración permiten a los administradores de TI configurar y verificar los parámetros de seguridad en los dispositivos de sus redes. La gestión de política habilita a los administradores de TI a definir la seguridad de acuerdo con su actividad, así como las políticas

de calidad de servicio y a aplicarlas en toda la organización sin necesidad de entender todas las reglas y parámetros específicos de los dispositivos necesarios para aplicar estas políticas. Técnicamente, las políticas son conjuntos de reglas para administrar, gestionar y controlar el acceso a los recursos de TI; y han de derivarse de las políticas empresariales definidas por la organización. En el espacio de seguridad, la gestión de política controla la complejidad y las difíciles curvas de aprendizaje asociadas con estas tecnologías (por ejemplo, cortafuegos, IDS, listas y filtros de acceso, técnicas de autentificación), y palia la falta de una visión de sistema entre todas las partes de la red (centro de datos, oficina distante, terreno).

Aunque hay numerosas soluciones parciales del problema, el sistema de gestión de política general proporciona una configuración centralizada de la red, garantizando que los parámetros de seguridad están configurados de manera coherente en los distintos nodos, reduciendo el riesgo de vulnerabilidad de la red. Esto no significa que hay sólo un sistema de política: en una red más grande, con múltiples dominios administrativos, puede ser necesario que haya múltiples sistemas de política responsables del control de un subconjunto de dispositivos y de la coherencia entre dominios.

La principal ventaja de aplicar plenamente un sistema de gestión de política es su facilidad de utilización y la mayor seguridad del entorno. Lo ideal para los gestores de red sería que pudieran definir políticas para las operaciones de red utilizando un vocabulario no técnico y que el sistema de política lo traduzca automáticamente a los mecanismos de seguridad adecuados que se aplicarán en la red.

II.5.1 Modelo de referencia de gestión de política

En la figura II.5.1 se muestra el marco arquitectural del IETF para la gestión de política ([b-IETF RFC 2753]). Este modelo se utiliza de referencia para la gestión de política y de seguridad y calidad de servicio. Por tanto, la gestión de política basada en este modelo se aplicará en toda la red y en todas las capas de la arquitectura y estará disponible para todos los tipos de usuarios y aplicaciones, incluidos los empleados, los técnicos de red, los socios e incluso los clientes.

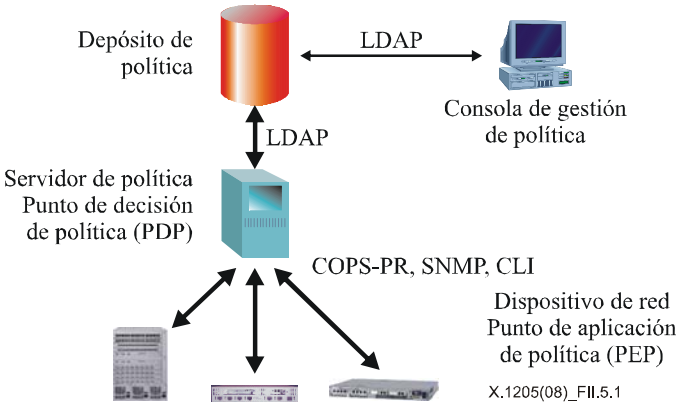

Figura II.5.1 – Modelo de referencia de gestión de política

Los componentes del modelo son:

- *Punto de imposición de la política (PEP, policy enforcement point)*: Una red o un dispositivo de seguridad que acepta una política (reglas de configuración) del punto de decisión de política y que aplica dicha política al tráfico de red que atraviesa el dispositivo. En esta aplicación se utilizan, según conviene, los mecanismos de seguridad de la red y los asistidos por la red.
- *Punto de decisión de política (PDP, policy decisión point)*: Los PDP o los servidores de política abstraen las políticas de red en mensajes de control de dispositivo específicos, que

se transmiten a su vez a los puntos de aplicación de política. Estos servidores de política suelen ser sistemas independientes que controlan todos los conmutadores y encaminadores de un dominio administrativo concreto, y se comunican con estos dispositivos utilizando un protocolo de control (por ejemplo, COPS, instrucciones Configurar de SNMP, Telnet o la interfaz de línea de instrucción (CLI, *command line interface*) específica del dispositivo.

- *Servicio de política común abierta (COPS, common open policy service)*: COPS es un protocolo basado en TCP de pregunta y respuesta simple basado en estados que puede utilizarse para intercambiar información de política entre un punto de decisión de política (PDP) y sus puntos de imposición de la política (PEP) clientes. Se especifica en [b-IETF RFC 2748]. El COPS depende de que el PEP pueda establecer conexiones con un PDP primario (un PDP secundario, si el primario no es alcanzable) en todo momento. Alternativamente, puede utilizarse un dispositivo intermediario COPS que traduzca los mensajes COPS procedentes de un servidor de política en instrucciones SNMP o CLI que puedan entender los dispositivos de seguridad y red.

  El protocolo COPS soporta dos modelos de extensión distintos para el control de política, un modelo dinámico en régimen externo COPS-RSVP, especificado en [b-IETF RFC 2749], y un modelo de configuración o determinación COPS-PR, especificado en [b-IETF RFC 3084]. Las extensiones de configuración del protocolo COPS permitirán la instalación "inmediata" de las políticas del PDP en el PEP, permitiendo a este último que tome las decisiones de política aplicables a los paquetes de datos de acuerdo con esta información preconfigurada. Además, es necesario que el PDP y el PEP comuniquen para mantener sincronizadas las políticas configuradas en el depósito de datos (es decir, el directorio) con las enviadas al PEP.

- *Depósito de política*: El directorio de red es el depósito de toda la información de política; describe los usuarios de red, las aplicaciones, los ordenadores y los servicios (es decir, los objetos y atributos) y las relaciones entre estas entidades. Hay una estrecha identificación de la dirección IP y el usuario extremo (gracias a un protocolo dinámico de control de anfitrión, DHCP, y un sistema de nombre de dominio, DNS). El directorio suele encontrarse en una máquina de base de datos dedicada. El protocolo ligero de acceso al directorio es el mecanismo que utilizan los servidores de política para acceder al directorio.

  El depósito de política se emplea para almacenar información relativamente estática sobre la red (por ejemplo, configuraciones de dispositivos), mientras que los servidores de política almacenan información más dinámica sobre el estado de la red (por ejemplo, atribución de anchura de banda o información sobre las conexiones establecidas). El servidor de política extrae información de política del directorio y la aplica a los elementos de red correspondientes.

  No hay una norma definida para describir la estructura de la base de datos del directorio, es decir, cómo se definen y representan los objetos de red y sus atributos. Se necesita un esquema de directorio común si múltiples aplicaciones de vendedor han de compartir la misma información de directorio; por ejemplo, cuando todos los vendedores necesitan interpretar y almacenar la información de configuración de los encaminadores de igual manera. La futura norma de interconexión de redes por directorio (DEN, *directory-enabled networking*), que está desarrollando el DMTF (*Desktop Management Task Force*), cubrirá estas necesidades. La DEN incluye un modelo de información que comprende la abstracción de perfiles y política, dispositivos, protocolos y servicios, lo que constituye un modelo unificado para la integración de usuarios, aplicaciones y servicios de interconexión de redes, además de un marco extensible orientado al servicio.

- *Protocolo ligero de acceso al directorio* (LDAP versión 3) está especificado en [b-IETF RFC 3377]: LDAP es un protocolo cliente-servidor de acceso al servicio de directorio. El modelo de información LDAP se basa en la entrada, que contiene información sobre algún objeto (por ejemplo, una persona) y se compone de atributos, que

tienen un tipo y uno o dos valores. Cada atributo tiene una sintaxis que determina qué tipo de valores se permiten en el atributo y cómo han de comportarse durante las operaciones de directorio.

- *Consola de gestión de política*: Las personas interactúan con el sistema de gestión de política a través de la consola de gestión, que generalmente se ejecuta en un ordenador personal o estación de trabajo. Si no, un buscador web puede utilizarse para dar acceso al gestor prácticamente desde cualquier sitio, utilizándose una seguridad a nivel de objeto de política para limitar el número de políticas que puede modificar una persona concreta. Es a través de la consola de gestión que las políticas se instancian en el directorio. La consola dispone de una interfaz de usuario gráfica y de las herramientas necesarias para que los gestores definan las políticas de red como reglas empresariales. También puede dar acceso al operador a configuraciones de bajo nivel de seguridad en conmutadores o encaminadores específicos.

Los elementos del modelo de referencia de gestión de política interactúan para llevar a cabo una gestión de política de bucle cerrado, que incluye la configuración de dispositivos de borde, la aplicación de las políticas en la red y la verificación de la funcionalidad de red desde el punto de vista de la aplicación de usuario extremo. La aplicación de políticas en la red incluye los controles de admisión de las aplicaciones o usuarios que desean acceder a los recursos de la red. La gestión de política puede contribuir a simplificar el entorno de gestión de la configuración en las empresas, reduciendo al mínimo la posibilidad de que haya un error humano.

II.5.2 Endurecimiento del sistema operativo del servidor

El endurecimiento de los sistemas operativos (OS, *operating system*) es uno de los elementos clave a la hora de proteger los sistemas de información en la capa de seguridad de aplicación. Una empresa típica puede disponer de múltiples sistemas operativos distintos para las diversas aplicaciones de datos (incluida la gestión de red), pero también para los servidores de aplicación que soportan la telefonía IP y las aplicaciones de comunicación intensiva. Es frecuente encontrar varias versiones del mismo OS en una infraestructura de TI, lo que dificulta aún más garantizar su seguridad.

El sistema operativo de datos más común también se utiliza masivamente para los servidores que soportan telefonía IP y aplicaciones de comunicación intensiva. Los fabricantes ofrecen una versión robusta de estos sistemas con software de seguridad comerciales para ejecutar funciones como la protección antivirus, la detección de intrusión y las auditorías de inscripción. El endurecimiento de un OS comienza con la necesidad de evitar el clonaje de servidor y de confiar en los medios desde los que se descargue el sistema operativo, y parte de esos puntos. Para los sistemas operativos que no disponen de directrices de endurecimiento específicas, es necesario consultar con el vendedor del IS a fin de obtener los parches y procedimientos de endurecimiento del OS más modernos.

Apéndice III

Ejemplo de seguridad de red

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

En este apéndice se presentan ejemplos de cómo se protegen diversos aspectos de una organización o empresa grande utilizando las técnicas expuestas en esta Recomendación.

En concreto, se tratan los principios de construcción de soluciones de seguridad por capas para proteger las pasarelas a Internet, el centro de datos, las oficinas distantes, el acceso a distancia y la telefonía IP. Se emplean las técnicas tratadas en esta Recomendación para ilustrar que para proteger una empresa no existe un modelo válido para todos los casos. En el cuadro III.1 se expone un ejemplo de los aspectos de seguridad pertinentes que se han de tener en cuenta. El ejemplo de la empresa 1 consiste en una empresa pequeña que utiliza unas cuantas líneas físicas privadas que conectan los emplazamientos, y que ofrece acceso a distancia limitado a sus empleados y su presencia en la web se basa en un centro de datos de Internet que facilita un proveedor de servicios (que es responsable de mantener un entorno seguro). El ejemplo 2 consiste en una empresa abierta con un modelo comercial que potencia Internet gracias a que los socios, proveedores y clientes tienen un acceso limitado a las aplicaciones de gestión de la empresa. En el último ejemplo, los usuarios internos y externos acceden a la red de la empresa desde casa, oficinas distantes u otras redes utilizando dispositivos móviles o alámbricos.

Cuadro III.1 – Resumen de los aspectos de seguridad de la empresa pertinentes

Zona de red	Ejemplo de empresa 1	Ejemplo de empresa 2
Protección del terreno	Sí	Sí, pues representa los requisitos de seguridad más restrictivos
Protección de la oficina distante	Criptación posible por las líneas privadas virtuales o físicas	Sí, incluido el acceso a Internet desde la oficina distante
Protección del acceso a distancia	Sí, pero sólo para el acceso de marcación privado	Sí, incluidos los socios y clientes
Protección del centro de datos	Sí, para los centros de datos internos	Sí, incluidos los centros de datos Internet
Protección de la telefonía IP	Sí	Sí, aprovechando las VPN

III.1 Protección del acceso a distancia

Las tecnologías de acceso a distancia permiten a la empresa u organización utilizar eficientemente al personal y los recursos allí donde residan. No obstante, estas tecnologías también pueden representar problemas de seguridad para la empresa. La mayoría de los usuarios de acceso a distancia son empleados de la empresa que se encuentran de viaje o trabajan desde sus hogares, pero en esta categoría también entran las oficinas pequeñas que se conectan cuando es necesario a la red de empresa. Los mayores problemas se experimentan al nivel de la seguridad de red y la gestión del acceso seguro. La seguridad de la gestión de red se ejecuta en el sitio central. La seguridad de la aplicación es importante en tanto que el dispositivo distante debe estar protegido con un software antivirus y cortafuegos personales.

Una de las principales amenazas a que se enfrentan los usuarios distantes es el robo de los equipos de éstos. No debe dejarse que el robo de los equipos de un usuario distante conduzca a intrusiones

en otras zonas de la red de empresa o al acceso a la información que pueda estar almacenada en el sistema. Ahora bien, los usuarios móviles desean llevar consigo sus dispositivos o terminales de acceso a la red, por lo que resulta indispensable criptar la información sensible almacenada en los sistemas utilizados para el acceso a distancia, de preferencia, un sistema que se integre fácilmente en el funcionamiento normal de las aplicaciones. Los actuales sistemas de criptación disponibles permiten al usuario trabajar normalmente, sin necesidad de criptar/decriptar los ficheros. Por ejemplo, es posible almacenar criptados sistemas de ficheros o "carpetas", integrándose la decriptación en el acceso normal al sistema de ficheros. Puede haber otras amenazas cuando el usuario distante trabaja en una LAN inalámbrica, desde su casa o desde un hotel, por ejemplo. En este caso, es importante contar con un antivirus y un cortafuegos personal actualizados.

Las formas más comunes de acceso a distancia en las comunicaciones de datos son el acceso por marcación, directamente a la empresa o a un ISP, y el acceso directo por Internet empleando una línea de abonado digital (DSL, *digital subscriber line*), módems de cable, Ethernet nativo (por ejemplo, en hoteles) y LAN inalámbricas (por ejemplo, en aeropuertos). Los servicios de datos públicos inalámbricos que soportan el acceso a Internet son cada vez mayores y aumentan la movilidad de los ordenadores portátiles y los dispositivos manuales. La cada vez mayor disponibilidad y las economías que se logran con Internet contribuyen a su rápido crecimiento en las VPN de acceso a distancia, tanto por marcación como por acceso directo. En la figura III.1 se muestra un ejemplo de protección del acceso a distancia.

Figura III.1 – Protección del acceso a distancia

Al utilizar las técnicas que se presentan en esta Recomendación, será necesario seguir los siguientes pasos para proteger el acceso a distancia:

1) *Acceso por marcación al sitio de empresa centralizado*

Un usuario de marcación para acceso a distancia establece una llamada telefónica desde un módem anexo a su sistema informático hacia un módem de grupo (también denominado conmutador de acceso a distancia) ubicado en el sitio central o regional de la empresa. Los sistemas de marcación estarán configurados para emplear un sistema de gestión de acceso seguro con autentificación y autorización de acceso, como ya se ha descrito anteriormente. El acceso por conmutación directo, aunque se utiliza masivamente durante la década de los 80 y a principios de los 90, ha sido rápidamente sustituido por VPN de acceso a distancia por Internet.

2) *VPN de acceso a distancia*

El acceso a distancia por Internet da una gran flexibilidad y anchura de banda. Hay dos posibilidades: VPN con IPSec utilizando clientes VPN de acceso a distancia, o VPN con SSL basadas en la capacidad SSL del navegador del usuario.

3) *VPN con IPSec*

IPSec es un método de la capa de red que puede utilizarse en las aplicaciones (por ejemplo, si se establece una conexión VPN con IPSec, el usuario puede acceder al correo electrónico, las aplicaciones de autoservicio y navegar por la red interna y acceder a las aplicaciones autorizadas). El equipo utilizado por el usuario para el acceso a distancia debe tener cargado un cliente IPSec. También los dispositivos manuales pueden tener un cliente. El equipo del usuario deberá contar también con software de detección antivirus.

Esté basado en acceso de marcación a un POP ISP o en acceso directo alámbrico o inalámbrico, el cliente VPN autentica al usuario, verifica la integridad del sistema informático del usuario y establece un vínculo seguro (o un túnel) con la empresa. El cliente VPN proporciona las capacidades (por ejemplo, cortafuegos) para garantizar que el sistema distante es en sí seguro, sobre todo durante el establecimiento de la conexión con la empresa. En la fase de establecimiento de sesión se utiliza tráfico criptado y autentificado con la empresa.

Se parte del supuesto de que las VPN de acceso a distancia pueden detectar y, de ser posible, evitar los obstáculos de Internet comunes, como NAT y cortafuegos externos (es decir, establecer un vínculo con la red de la empresa desde otra red protegida con cortafuegos), o, al menos, proporcionar al usuario distante información sobre la naturaleza de los obstáculos encontrados.

Desde el lado de la empresa, las conexiones de acceso a distancia por Internet se someten al sistema de pasarelas IPSec. El lado de la empresa debe contar con protección contra los puntos únicos de fallo gracias a pasarelas con múltiples trayectos a Internet. Dependiendo del alcance de la empresa, se recomienda también la separación geográfica de las pasarelas. Las pasarelas deben tener una serie de características para soportar eficazmente el acceso a distancia en toda la empresa. Entre las características recomendadas se cuentan la configuración de cliente simple, la capacidad de mantener las conexiones a través de la red de empresa interna, por oposición a la terminación de sesión, y la posibilidad de funcionar como un cortafuegos basado en estados para evitar la necesidad de disponer de un cortafuegos distinto. Además, se recomienda que la pasarela utilice diversos mecanismos de autentificación, como RADIUS, PKI y LDAP a fin de añadir flexibilidad de elección para la autentificación de usuarios. La pasarela debe dar a la empresa la flexibilidad de integrar otros mecanismos, como RADIUS, ID de usuario/contraseña de directorio, o incluso autentificación por tarjeta inteligente o testigo desde los portátiles de los usuarios que ya se utilicen. Conviene el soporte de L2TP y PPTP.

III.2 Protección de la telefonía IP

Las organizaciones y empresas están empezando a utilizar soluciones de telefonía IP a fin de aprovechar los beneficios de la convergencia en la LAN y la WAN, y las aplicaciones convergentes. Todos los sistemas VoIP están formados por hardware/software con cuatro funciones lógicas:

- Teléfonos IP y clientes de software en PC.
- Servidores de comunicaciones (también denominados servidores de gestión o controladores de pasarela).
- Pasarelas de medios con acceso flexible a la red (por ejemplo por PBX tradicionales y la red telefónica pública conmutada (RTPC) y la red pública inalámbrica, etc.).

- Servidores de aplicación (por ejemplo, aplicaciones de mensajería, conferencias y conjuntas SIP unificadas).

Estas funciones, así como los servidores de aplicación relacionados, y elementos tales como el centro de contacto y la mensajería unificada, están distribuidos por la red IP telefónica o de empresa, que proporciona los niveles necesarios de fiabilidad, calidad vocal y gestión de la congestión. Se logra más alcance y movilidad con las LAN inalámbricas y por Internet a través de VPN IP.

En la figura III.2 se muestra el método típico de las organizaciones para proteger la telefonía IP.

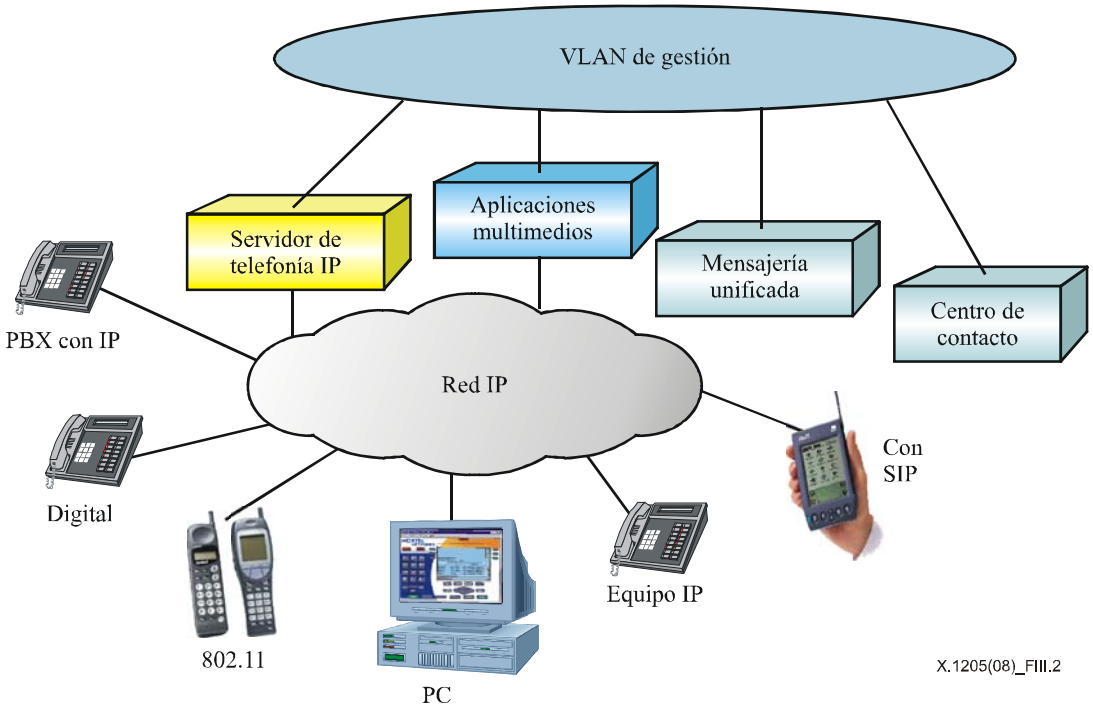

Figura III.2 – Protección de la telefonía IP

La telefonía IP es una aplicación que se ejecuta en la red IP y que aprovecha la funcionalidad de seguridad de la red. A diferencia de la mayoría de aplicaciones, la telefonía IP tiene importancia temporal y es fundamental para el funcionamiento de la empresa. Al igual que otras aplicaciones de datos, los sistemas de telefonía IP pueden ser objeto de diversos ataques, como:

- los ataques al encaminador pueden dejar fuera de servicio los servicios vocales y de datos de una organización;
- la denegación de servicio puede sobrecargar el servidor o el cliente de comunicaciones de telefonía IP;
- el "ping of death" puede dañar las operaciones VoIP enviando múltiples pings a los dispositivos VoIP;
- el análisis de puerto puede encontrar las vulnerabilidades de los clientes y servidores VoIP;
- el rastreo de paquetes puede grabar y/o interceptar conversaciones;
- la falsificación IP puede representar erróneamente el origen o destino del tren de medios o de señalización;
- los virus, gusanos, caballos de Troya y las bombas con temporizador pueden atacar a los servidores y clientes.

La telefonía IP puede estar en peligro. Por ejemplo, hay casos de piratas tomando el control de clientes IP a causa de una mala administración de las contraseñas en un caso, y a causa de vulnerabilidades en la ejecución del XML (véase [b-W3C XML 1.0]) en el otro. Estos ataques pueden ser una gran amenaza cuando VoIP se ejecuta nativamente por Internet, y una amenaza algo más leve cuando la telefonía IP se utiliza estrictamente dentro de la empresa y por conexiones tunelizadas en Internet.

Como ocurre con cualquier aplicación, es necesario evaluar los riesgos de la telefonía IP para determinar su valor intrínseco, las consecuencias de su pérdida en el contexto de la organización y para formular una política de seguridad. La telefonía es una función básica de la empresa y, por tanto, al igual que la red, se habrá de proteger todo el sistema telefónico contra las amenazas de seguridad y los ataques.

Por norma general, los usuarios de telefonía se autentifican cuando acceden desde fuera de la red utilizando un conjunto de características denominado acceso directo al sistema interno (DISA, *direct inward system access*). Por otro lado, suele requerirse a los usuarios de datos que empleen múltiples identidades de usuario y contraseñas para acceder a la red y las aplicaciones. Esta complejidad es contraria a la protección del entorno de empresa. La sencillez es tanto más importante en el caso de la VoIP, dado que lo que se espera es un tono de llamada inmediato. Huelga decir que ningún mecanismo de seguridad VoIP puede menoscabar la necesaria conectividad y calidad vocal.

Directrices para proteger la telefonía IP:

1) las soluciones de telefonía IP de la empresa funcionan dentro de los confines de la empresa e interfuncionan con la red pública a través de conexiones con conmutación de circuito;
2) los sistemas de telefonía IP de la empresa dependen de la protección de la infraestructura de interfuncionamiento IP desde el punto de vista de los datos y de que su creación y diseño se ajusten a los requisitos de latencia y fiabilidad de la telefonía;
3) los servidores de comunicaciones de telefonía IP de la empresa son fundamentales para su funcionamiento y están protegidos físicamente, así como contra los ataques internos y externos;
4) se ofrece la autentificación segura de los clientes VoIP;
5) la criptación de la voz sólo es necesaria cuando se atraviesa una LAN de medios compartidos o Internet;
6) se adopta un método global de seguridad en todo el entorno de telefonía, incluidos los clientes y servidores VoIP, los servidores de aplicación (por ejemplo para la mensajería unificada y los centros de contacto) y las PBX tradicionales.

Para proteger la telefonía IP hay que adoptar un método coordinado en todas las capas de red. La gestión de política y la gestión de acceso seguro garantizan la autentificación de usuarios y controlan las características y capacidades de llamada de la telefonía IP. Es necesario utilizar técnicas de gestión seguras para proteger los dispositivos VoIP como los servidores de comunicaciones y las pasarelas de medios. Pueden aprovecharse los mecanismos de seguridad utilizados para la VoIP, por ejemplo, utilizando IPSec para proteger el acceso a distancia, la conectividad de sucursales y para el acceso a la LAN inalámbrica. Gracias a la gestión de política puede lograrse más seguridad añadiendo una inspección por estados VoIP de los cortafuegos y la funcionalidad de traducción de direcciones de red. La seguridad de las aplicaciones puede lograrse de diversas maneras, incluido el endurecimiento del OS y la protección contra virus en los equipos del usuario.

III.2.1 Protección de los servidores de aplicaciones y de comunicaciones de telefonía IP

El corazón del sistema de telefonía IP es el servidor de comunicaciones, que puede ser un servidor independiente o estar integrado en un gestor de comunicaciones empresariales PBX IP. Igual de

importantes son los servidores de aplicación responsables del centro de contacto, las aplicaciones multimedios, la mensajería unificada y los sistemas de respuesta de voz interactivos autogestionados. La protección de estos servidores empieza con el endurecimiento de los sistemas operativos, como ya se ha expuesto.

III.2.2 Protección de los clientes VoIP

Las soluciones VoIP soportan una amplia gama de clientes y configuraciones de acceso, incluidos los teléfonos IP alámbricos e inalámbricos y el software de PC, vulnerables a los ataques cuando están conectados a una red IP.

Hay diversos protocolos de señalización de telefonía como SIP. El tráfico de señalización suele emplear TCP en el nivel de transporte. En el futuro, existirá la posibilidad de proteger fácilmente el tráfico de señalización en el cliente VoIP. En los sistemas de telefonía IP, la señal de voz se paquetiza utilizando una norma como [b-UIT-T G.729] (a 8 kbit/s) y un algoritmo de detección de actividad vocal, y se emplea el protocolo en tiempo real (RTP) con UDP en el nivel de transporte.

Hay importantes diferencias en la minimización del riesgo para los teléfonos IP y los clientes de telefonía de software de PC. Los teléfonos IP son aparatos creados exclusivamente para la telefonía. No hay ningún tipo de almacenamiento o activo que proteger en el teléfono mismo (aparte de ser un dispositivo fiable presente en la red). Los únicos activos que hay que proteger son la identificación del llamante y la llamada misma. Estos aparatos telefónicos utilizan comúnmente un protocolo lógico privado que depende del servidor de comunicaciones para sus características/funcionalidades y su seguridad. Esto contrasta con las implementaciones, que dependen de la configuración del XML en VoIP para poder funcionar, lo que representa una vulnerabilidad.

El software VoIP reside en el equipo del usuario junto con otras aplicaciones y activos y los sistemas operativos más comunes utilizados. Un ataque realizado con éxito puede resultar caro, ya que los equipos del usuario contienen numerosos activos valiosos, incluidas las aplicaciones y los datos personales, financieros y de la empresa. Lo más común es utilizar una o varias aplicaciones de seguridad diseñadas par alas plataformas PC, con cortafuegos personales, detección antivirus y clientes VPN IP. Para el software VoIP pueden utilizarse los mismos mecanismos que para los datos.

III.2.3 Protección de la VoIP en el armario de cableado y en el complejo

Hay dos maneras de conectar los dispositivos IP a la red de un complejo: por medios compartidos y por Ethernet conmutado dedicado. La industria en general se decanta por el Ethernet conmutado dedicado, dado el crecimiento del tráfico y los requisitos de gestionabilidad. Además, de la seguridad y la gestionabilidad también depende la implantación de VLAN (véase [b-ISO/CEI 18028-5]) en las redes de empresa. Las LAN inalámbricas son la tercera alternativa, muy popular en entornos tales como la educación y la sanidad.

Con la introducción de la telefonía IP, se recomienda vivamente que los clientes de software VoIP y los dispositivos VoIP estén conectados a entornos de Ethernet conmutado directamente en el escritorio, lo que cumple los siguientes requisitos:

– Se minimiza la variación de latencia VoIP eliminando el funcionamiento CDMA del funcionamiento Ethernet de los medios compartidos.
– Se mejora la seguridad de la VoIP al eliminar la posibilidad de que otros escritorios escuchen ilegalmente las llamadas VoIP.

Además, las empresas pueden optar por agrupar lógicamente los teléfonos VoIP en sus propias VLAN a fin de facilitar su gestión.

La telefonía IP puede mejorar en gran medida la productividad de los usuarios de las LAN inalámbricas de la empresa ampliando la característica/funcionalidad de telefonía del escritorio a, por ejemplo, una sala de conferencias o un aula. Dada la naturaleza hostil de estas WLAN, se

recomienda proteger los planos de señalización y voz en el segmento inalámbrico, lo que puede hacerse configurando los clientes de software copresidentes con un cliente VPN IP en un ordenador portátil. Si no, hay teléfonos IP WLAN con criptación y autentificación incorporadas. Con ambos métodos se logra la autentificación y criptación robustas que requieren los entornos WLAN.

III.2.4 Protección de sucursales para la telefonía IP

Hay diversos métodos para soportar las soluciones VoIP en oficinas distantes y sucursales, entre las que se cuentan los teléfonos VoIP y clientes de software que soportan las soluciones todo en uno. Otras opciones se aprovechan de la naturaleza distribuida de la VoIP instalando los clientes fuera del servidor centralizado. En cualquier caso, se recomienda que el tráfico VoIP en las sucursales atraviese de manera segura las VPN IP establecidas para datos.

III.2.5 Protección del acceso a distancia para la telefonía IP

La telefonía IP puede mejorar en gran medida la productividad de los usuarios a distancia, ya trabajen desde sus hogares, un hotel o la calle, ampliando, en todos los casos, la característica/funcionalidad de telefonía del escritorio a la ubicación distante. Los clientes de software VoIP serán copresidentes con un cliente VPN IP en un ordenador portátil, en el caso de los empleados con mucha movilidad. Esta misma configuración puede utilizarse para aprovechar los puntos de acceso WLAN en hoteles, aeropuertos y centros de conferencias. Los teléfonos VoIP pueden ofrecer comunicaciones complejas a los telecomunicadores y agentes de centros de contacto, siendo la VPN IP central la que se encargue de la seguridad.

III.2.6 Seguridad de gestión de red para la telefonía IP

Desde el punto de vista de la gestión, debe configurarse un puerto Ethernet dedicado físicamente. Esto debe ser parte de una VLAN de gestión que bloquee todo el tráfico ajeno a la gestión al nivel del encaminador gracias a listas de acceso y a la seguridad del perímetro. Las VPN IP pueden proporcionar acceso fuera de red a los proveedores, integradores de sistema y/o VAR. Los puertos no utilizados (por ejemplo, para consolas o acceso por módem a distancia) deben estar desactivados. En estos servidores sólo deberán ejecutarse los software de aplicación autorizados. Habrá de utilizarse una seguridad multinivel con diversos niveles de privilegio (supervisar, configurar, controlar) para el personal operativo autentificado. Las contraseñas de usuario se almacenan de manera segura y se controla estrictamente el formateo de las contraseñas y la gestión de cambios. Es posible criptar el tráfico de gestión (como la información de facturación) incluso para la transmisión interna con tecnología VPN IP.

III.3 Protección de la oficina distante

Una oficina distante puede oscilar entre el escritorio de un trabajador en su casa a un complejo empresarial importante. Aunque hay numerosos elementos comunes entre la "oficina distante" y el "acceso a distancia", se diferencian por la persistencia de capacidades de comunicación bidireccional entre la ubicación distante y el resto de la empresa. La oficina distante es un lugar de trabajo constantemente conectado al resto de la empresa y que puede intercambiar mensajes con el resto de la empresa durante las horas de trabajo. Por otro lado, el acceso a distancia es una conexión temporal con la empresa establecida a petición del usuario de acceso distante.

La interconexión de las sucursales es el método de prestación de servicios más rentable de muchas empresas, como la banca privada, la sanidad y el gobierno. Los entornos de interconexión de sucursales tradicionales se basan en diversas tecnologías LAN y en encaminadores multiprotocolo dentro de redes de retransmisión de tramas respaldadas por la conmutación de circuitos RDSI. Hay cuatro elementos que han contribuido a transformar la interconexión de sucursales: 1) la convergencia en Ethernet como norma para la LAN, 2) la aceptación universal de IP como protocolo preferido, 3) Internet y 4) el aumento de servicios VPN de capa 2 y capa 3. No obstante, estos elementos también presentan problemas de seguridad para las empresas más grandes, como se muestra en la figura III.3.

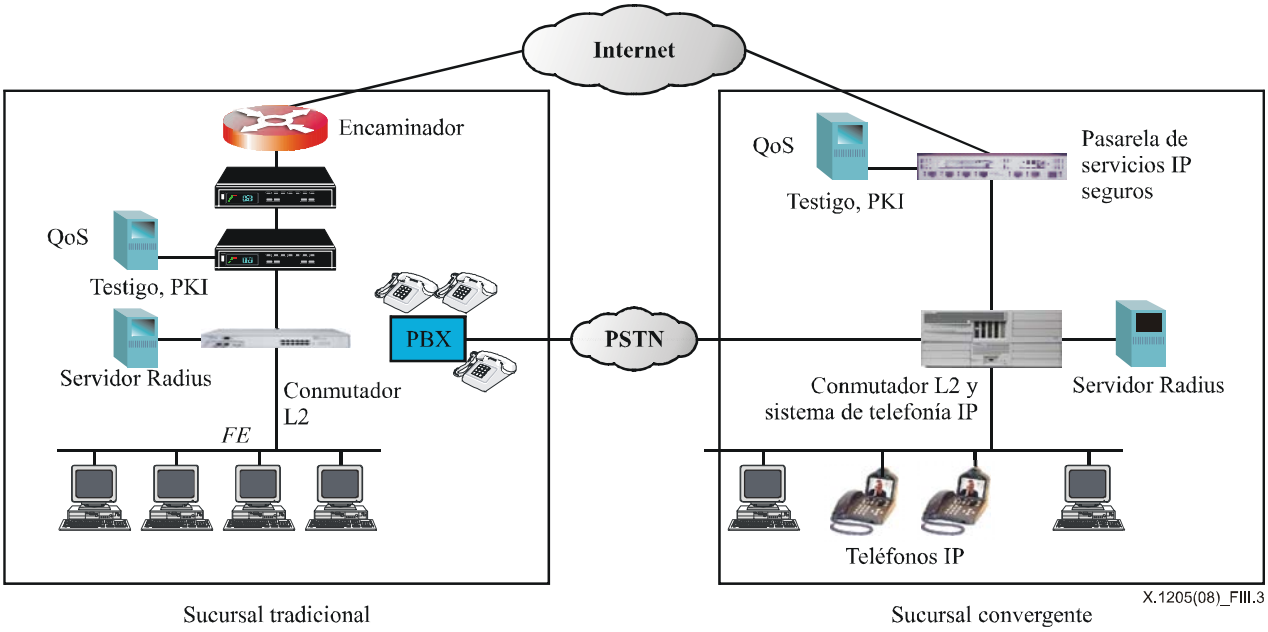

Figura III.3 – Protección de la oficina distante

Los requisitos de la WAN en cuanto a las sucursales incluyen el encaminamiento local entre VLAN y en la red, la gestión de la calidad de servicio y la anchura de banda y la posibilidad de adaptar las interfaces con la red WAN. Esto implica soportar el esquema de encapsulación necesario en la WAN y alcanzar el nivel de fiabilidad adecuado. La seguridad rentable por Internet (e incluso con la retransmisión de tramas) es un requisito clave. También resulta problemático gestionar la transición de las tecnologías WAN relativamente seguras tradicionales a las VPN IP. Algunas empresas desean tener acceso directo a Internet desde cualquier oficina distante, lo que hace surgir la necesidad de contar con cortafuegos distantes. Otras quieren disponer de conectividad con encaminamiento dinámico muy fiable entre las sucursales y la red principal de la empresa, con cortafuegos centralizados en Internet, utilizando en ocasiones la retransmisión de tramas como método principal con respaldo Internet, o se dirigen hacia las VPN IP como configuración principal. El encaminamiento dinámico se emplea para mejorar la adaptabilidad y fiabilidad gracias a:

- Aprendizaje automático de la topología de red.
- Aprendizaje automático de las direcciones de los usuarios extremos en toda la empresa.
- Adaptación automática a los cambios en la topología de red.

Sin embargo, normalmente la seguridad de las redes con encaminamiento no ha sido una prioridad. Por ejemplo, no se ha encontrado una manera eficaz de llevar a cabo el encaminamiento dinámico por túneles con criptación VPN y su gestión ha resultado muy difícil.

Por norma general, esto ha hecho que las empresas adquieran, instalen, mantengan y gestionen múltiples dispositivos de seguridad e interconexión de redes de oficina distante y sucursal, lo que las ha hecho complejas y caras de gestionar.

Al pasar a las VPN IP por Internet, es necesario cumplir una serie de requisitos de seguridad de la manera más rentable posible, lo que incluye las funciones de seguridad de red, como el encaminamiento IP por túneles seguros, la interconexión de redes privadas virtuales y la criptación, la inspección de cortafuegos por estados en la capa asistida por la red y la autentificación de la oficina distante y los servicios de directorio en la capa de gestión de acceso segura, requisitos todos que han de cumplirse de manera integrada. También ha de incluirse la gestión de la política de seguridad a fin de que se cree para cada usuario un perfil de seguridad exclusivo que le pertenece, ya se conecte desde su equipo desde casa a través de Internet pública o a nivel local dentro de la

sucursal. La seguridad de la gestión de red también ha de cubrir la oficina distante, sin puertas traseras que puedan poner en compromiso la seguridad de la red. Por ultimo, ha de contarse con seguridad para las aplicaciones si en la oficina distante se implantan servidores de datos y/o telefonía IP.

III.4 Protección de la WLAN

Las posibilidades de comunicación entre la sede de la empresa, las sucursales, los empleados a distancia, los consultores y los socios comerciales están evolucionando. Hoy es posible que las empresas adopten las nuevas tecnologías inalámbricas IEEE 802.11 (véase [b-IEEE 802.11]) para llevar a cabo sus transacciones en cualquier momento y desde cualquier lugar. Estas soluciones conllevan, no obstante, la necesidad de gestionar centralizada y eficazmente el acceso de los usuarios protegiendo al mismo tiempo los recursos de la organización.

Las WLAN son particularmente vulnerables a los fallos de seguridad. Para interceptar comunicaciones en una LAN normal se necesita acceso físico al cableado. Sin embargo, las transmisiones inalámbricas pueden interceptarse por el aire y exponer la red a intrusiones de cualquiera que disponga de una tarjeta LAN inalámbrica.

Las WLAN amplían las redes de empresa con dispositivos inalámbricos y el protocolo IEEE 802.11. Los equipos de las WLAN incluyen tarjetas de interfaz de red inalámbrica (NIC, *network interface cards*) para los equipos móviles, como ordenadores portátiles y de escritorio, que se denominan en su conjunto unidades móviles (MU, *mobile unit*) o estaciones móviles (STA, *mobile station*). Las NIC permiten el transporte de las señales de red de los dispositivos conectados a través de un dispositivo intermediario, la pasarela LAN inalámbrica, o una central conocida como punto de acceso inalámbrico (AP, *access point*), que convierte las señales inalámbricas en señales alámbricas que circularán por la red alámbrica.

Gracias a una central o conmutador Ethernet, las empresas pueden conectar los puntos de acceso a la LAN inalámbrica con la LAN alámbrica tan fácilmente como un usuario de línea. Al conectar los puntos de acceso a un conmutador, se garantiza que el punto de acceso tiene 10/100 Mbit/s dedicados, permitiendo que todos los puntos de acceso disponibles se comporten como un conmutador sin tener que rivalizar por la anchura de banda de la central alámbrica.

La norma [b-IEEE 802.11] original es una serie de especificaciones, de las cuales IEEE 802.11a, IEEE 802.11b, IEEE 802.11g e IEEE 802.11i están disponibles en la actualidad y se utilizan en el entorno de señal de la red, equilibrándose la distancia y la anchura de banda.

III.4.1 Cuestiones de seguridad de la WLAN

Independientemente de los mecanismos de seguridad de la WLAN, las señales WLAN siguen transmitiéndose y recibiéndose por el aire por ondas radioeléctricas y no hay barreras físicas que frenen a los usuarios no autorizados. Por desgracia, estas señales se interceptan y es posible introducirse en las redes de empresa. Por tanto, al añadir un nodo inalámbrico en la red de empresa han de tomarse las precauciones de seguridad necesarias y seguir las prácticas recomendadas en materia de seguridad para proteger todos los activos de la red WLAN.

La capa de infraestructura de las redes WLAN consta de todos los componentes de la red, cables, interconexiones y medios de transmisión (espacio de cobertura), por ejemplo, puntos de acceso, estaciones móviles, pasarelas y servidores que acogen los servicios conexos tales como RADIUS, DNS, etc.

La capa de servicio consiste en servicios de acceso LAN inalámbrico y otros servicios que permiten el acceso inalámbrico, entre los que puede citarse la autentificación, la autorización y la contabilidad (AAA), los servicios de gestión de claves, etc.

Amenazas de seguridad que presentan las WLAN:

- Fallos de confidencialidad e integridad del tráfico inalámbrico. Cualquier agresor puede interceptar comunicaciones entre un ordenador móvil y un AP inalámbrico y recibir información sensible o clasificada no prevista para terceros. También es posible que un agresor introduzca información en una transacción real, sin que los usuarios legítimos sean conscientes de ello.
- Exposición de la LAN de empresa. A menos que las plataformas móviles estén autenticadas de forma segura, puede resultar sencillo para un agresor conectarse a la WLAN gracias a un dispositivo IEEE 802.11 y convertirse en una estación "autorizada" de la WLAN, pudiendo acceder así a la LAN de empresa.

Según el modelo de amenazas de la Recomendación X.800, los ataques pueden clasificarse del modo siguiente:

Modelo de amenazas de la X.800	**Método de ataque**
Destrucción de la información y/o otros recursos	Intrusión de AP
Corrupción o modificación de la información	Pirateo de la clave, intromisión
Hurto, supresión o pérdida de la información y/o recursos	Intrusión de AP, pirateo de la clave WEP, intromisión, falsificación de la dirección MAC, dispositivos maliciosos, el "war driving", apropiación de la capa 3, redes con fines específicos
Revelación de información	Intrusión de AP, pirateo de claves WEP, intromisión, falsificación de dirección MAC, dispositivos maliciosos, war driving, apropiación de la capa 3, redes con fines específicos
Interrupción del servicio	Interferencia radioeléctrica, inundación de datos, apropiación de la capa 2, AP falso, trama de desautentificación falsificada, denegación del servicio FATA-Jack

Al igual que pasa con la red alámbrica, las WLAN requieren controles de confidencialidad, integridad y acceso. El principal problema de seguridad en el entorno inalámbrico es que los extraños pueden fácilmente recibir o transmitir información desde o hacia la WLAN, independientemente de que se considere que está fuera de alcance.

Así, los agresores pueden escuchar e insertar AP no autorizados (denominados AP maliciosos) para lanzar ataques como los ataques por intromisión y el pirateo de sesión, y pueden fácilmente atacar a los usuarios de la WLAN desde su interior. Por tanto, un agresor puede engañar a un usuario para que se conecte a su AP, se presente como un nodo legítimo de la red y, así, compartir libre e inconscientemente los ID de usuario, las contraseñas y otro tipo de información privada.

Con las siguientes técnicas se puede proteger el entorno inalámbrico:

- Nombres de red: identificaciones de conjunto de servicios (SSID, *service set identifications*).
- Inscripción de tarjeta: listas de control de acceso MAC (ACL, *MAC access control lists*).
- Criptación de claves compartidas: con diversos protocolos de seguridad (como WPA/WPA2).

Además, pueden emplearse los siguientes tipos de autentificación:

- Autentificación de sistema abierto: da acceso a cualquier persona con el SSID del AP.
- Autentificación de clave compartida: el usuario conoce un secreto compartido para poder autentificarse.

En la norma [b-IEEE 802.11] original, la itinerancia segura se realiza gracias a la preautentificación de la unidad móvil (MU) ante los AP circundantes. No hay transmisión de mensajes entre los AP, pues todos los AP y MU utilizan la misma clave compartida, lo que permite al nuevo AP suponer la validez de la autentificación del MU. La transmisión de mensajes es rápida, pero la autentificación es menos segura, porque no se autentican las tramas de gestión.

III.4.2 Requisitos y mecanismos de seguridad en el punto de acceso inalámbrico y frente al mismo

La única manera de proteger realmente el entorno inalámbrico, naturalmente abierto, es mediante criptografía y adoptando las medidas de autentificación que validan al usuario extremo. El tráfico se encripta cuando se dirige a una pasarela cuyo identificador se puede validar criptográficamente.

Los dos principales requisitos de una WLAN segura es que se protejan el tráfico y la itinerancia. A fin de lograr comunicaciones seguras, el requisito básico es el empleo de criptación para el tráfico procedente del dispositivo móvil hacia el AP, hacia la pasarela detrás del AP (por ejemplo, utilizando una pasarela IPSec) o hacia el servidor de aplicación (sitio web seguro). Para proteger la itinerancia, los usuarios móviles han de poder pasar de un AP a otro sin perder las sesiones activas y sin tener que reautenticarse ante un nuevo AP. La itinerancia presenta estrictas restricciones en cuanto al tiempo de manera que repercuta lo menos posible en la aplicación del usuario. Los usuarios esperan y suponen que sus credenciales se protegen adecuadamente cuando pasa de un dominio a otro.

III.4.3 Mejoras de seguridad para la norma IEEE 802.11

Los riesgos de seguridad mencionados han provocado mejoras de la norma [b-IEEE 802.11] original a fin de proporcionar medios más eficaces de proteger las LAN inalámbricas. IEEE 802.11i introduce el control de acceso IEEE 802.1X (véase [b-IEEE 802.1X]), la creación dinámica de claves, mecanismos de distribución de claves por sesión y algoritmos criptográficos fuertes. [b-IEEE 802.1X] introduce más control de autentificación/acceso para los AP gracias al empleo del protocolo de autentificación extensible (EAP, *extensible authentication protocol*), que es un conjunto de mensajes para la negociación de la autentificación y un método de transporte de autentificación entre el cliente y el servidor (véase [b-IETF RFC 2716], [b-IETF RFC 3748] y [b-IETF RFC 4017]). EAP soporta diversos métodos de autentificación, incluido MD5, siendo la seguridad de capa de transporte (TLS) con MD5 el método más soportado y disponible. Independientemente de la opción EAP, los tres componentes IEEE 802.1X (véase [b-IEEE 802.1X]) tienen que soportar el mismo método (véase la figura III.4.3).

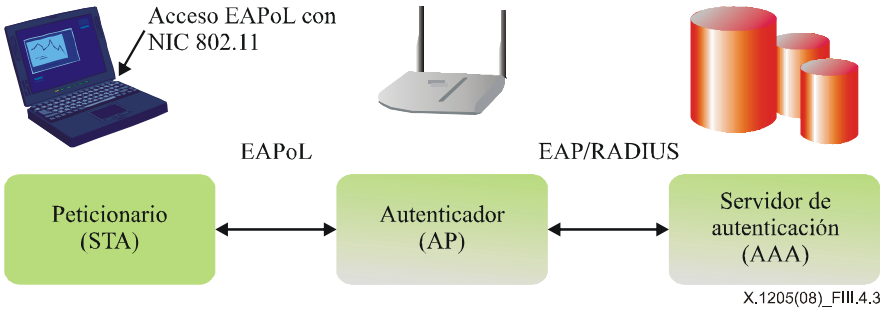

Figura III.4.3 – Componentes de IEEE 802.1X

La protección de la itinerancia IEEE 802.1X requiere que el usuario se reautentique siempre ante el nuevo AP al que se dirige. Las claves por sesión y la lentitud de las operaciones de infraestructura de clave pública (PKI) dificultan la rapidez de la reautentificación, por lo que se experimentarán dificultades en la transmisión entre AP en itinerancia con estas opciones de autentificación.

Para [b-IEEE 802.1X], EAP-TTLS y PEAP proporcionan una reautentificación rápida en caso de itinerancia, lo que puede efectuarse aprovechando el mecanismo de reestablecimiento de conexión previsto por el protocolo de toma de contacto TLS. No se requiere la plena autentificación, pues se supone el conocimiento del secreto, como lo demuestra que la capacidad de retomar la sesión TLS es suficiente autentificación.

III.4.4 Método por capas para la protección de las LAN inalámbricas

Las buenas arquitecturas WLAN seguras requieren un método por capas que aplique diversas tecnologías, al igual que las LAN normales. La solución definitiva debe ser una arquitectura WLAN/LAN integrada. Siempre que sea posible, los mecanismos de seguridad de la LAN existentes deben aplicarse también a la WLAN.

III.4.4.1 Punto de acceso

Pueden utilizarse ESSID y ACL MAC aunque proporcionan una seguridad muy frágil. Todas las unidades móviles (MU) y AP configurados con el mismo ESSID pueden asociarse libremente. La [b-IEEE 802.11] soporta un "ESSID de radiodifusión" que permite a una MU asociarse a un AP sin conocimiento del ESSID. La seguridad puede mejorarse si esta característica está inhabilitada. ACL MAC contiene una lista de direcciones MAC permitidas y puede contener una lista de direcciones prohibidas, teniendo en cuenta la dificultad de gestionarlas cuando participan numerosos ordenadores.

En la actualidad, pueden utilizarse fácilmente AP con mecanismos de seguridad privados y prenormalizados, como WPA, WPA2, la norma de criptación avanzada (AES, *advanced encryption standard*) WEP dinámica, el protocolo de integridad de clave temporal (TKIP, *temporal key integrity protocol*), y la criptación de 128 bits. El WEP dinámico es un medio de modificar más a menudo la clave WEP a intervalos predeterminados. AES es la nueva norma aprobada por FIPS para sustituir el algoritmo de criptación DES. TKIP refuerza el algoritmo de programación de claves para contrarrestar ataques de recuperación de claves al WEP clásico. A causa de su debilidad, [b-IEEE 802.11] recomienda no utilizar TKIP excepto como parche en equipos antiguos.

NOTA – El acceso protegido a Wi-Fi (WPA, *Wi-Fi protected access*) es una iniciativa de la industria que especifica mejoras para la seguridad de la interconexión de red de área local (LAN) inalámbrica. WPA-PSK es un tipo especial de WPA para usuarios residenciales sin servidor de autentificación de empresa y proporciona una fuerte protección de criptación. En WPA-PSK, las claves de criptación se modifican automáticamente (creación de claves) y se autentican entre dispositivos tras un periodo determinado de tiempo o después de la transmisión de un número específico de paquetes. WPA-PSK utiliza un secreto compartido que debe introducirse tanto en el punto de acceso inalámbrico exterior como en los clientes WPA. El secreto compartido puede tener una longitud de entre 8 y 63 caracteres. El protocolo de integridad de claves temporal (TKIP) se utiliza después de que se introduzca el secreto compartido inicial en los dispositivos inalámbricos y se encarga de la criptación y creación automática de claves. WPA está diseñado como una actualización de software. Los vendedores de productos inalámbricos y profesionales de la seguridad esperan que WPA y WPA-PSK actuales sean útiles durante largo tiempo. WPA define la utilización de la norma de criptación avanzada (AES) como otra de las opciones para sustituir la criptación WEP.

III.4.4.2 Espacio aéreo

Con una antena direccional de alta ganancia, cualquier extraño que quiera acceder de manera no autorizada a la WLAN puede alcanzarla desde una gran distancia. Sería preferible impedir que esto ocurriera. Un posible método para impedir que usuarios no autorizados aprovechen la disponibilidad aérea de la señal con antenas direccionales de alta ganancia es rodear el perímetro de la empresa o de la red WLAN con AP que no estén conectados a la red interna (véase la figura III.4.4.2). Se impide a los usuarios extraños ver la WLAN interna, dado que los AP exteriores funcionan con la misma frecuencia portadora que los internos, por lo que la señal es más resistente al exterior y se hace más "opaca" al usuario externo. Esta configuración puede mejorarse conectando los AP externos a una red aislada y añadiendo un sistema de detección de intrusión (IDS) y un señuelo para detectar intrusiones y obtener pruebas.

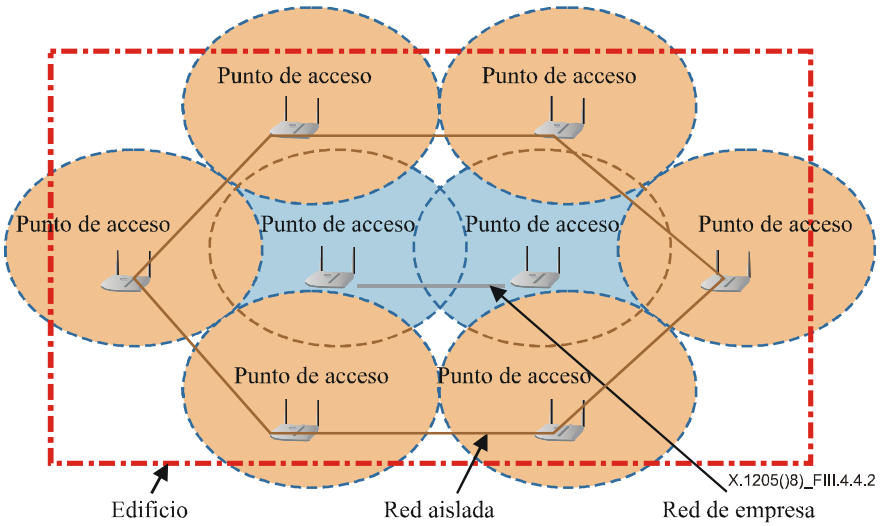

Figura III.4.4.2 – AP centinelas para la protección del perímetro

III.4.4.3 Segmentación

Siempre que sea posible, los mecanismos de seguridad de la LAN existentes deben cubrir también la WLAN. También son eficaces, independientemente de otras mejoras a [b-IEEE 802.1X], otros mecanismos como la criptación por VPN y TLS, la segmentación de segmentos inalámbricos por LAN virtuales (VLAN), y la defensa del perímetro con un cortafuegos. En la figura III.4.4.3 se muestran los AP de la WLAN IEEE 802.11 genérica con SSID común o una subred conectados al conmutador de capa 2. El conmutador de capa 2 tiene la capacidad inteligente de limitar el tráfico hacia otros AP y algunos también pueden a la VLAN. En el caso de los AP residentes en otra subred o SSID, la conexión puede hacerse mediante un conmutador de encaminamiento de capa 2/3. En esta arquitectura, ha de considerarse que las comunicaciones seguras, la itinerancia y transmisión seguras y la defensa del perímetro forman parte del entorno de red WLAN/LAN seguro e integrado.

IPSec ha demostrado ser un protocolo fiable para proteger las comunicaciones. En los entornos que soportan los clientes IPSec en los dispositivos móviles o que tienen aplicaciones con más de un extremo hacia la red, IPSec es el medio más adecuado de proteger las comunicaciones. El principal beneficio de una VPN IPSec es que la empresa tiene pleno control sobre la política de seguridad robusta, de manera que cualquiera que accede a la LAN tiene todos los privilegios de un usuario LAN local.

Las mismas técnicas son aplicables a los "hot spot" WLAN. Por ejemplo, un empleado distante que acceda a la red desde un ISP de un hotel puede conectarse a través de una DSL empleando un cliente PPPoE y un ID de usuario/contraseña proporcionados por el hotel para el acceso al ISP. Así, el empleado puede conectarse a su red de empresa utilizando un cliente IPSec.

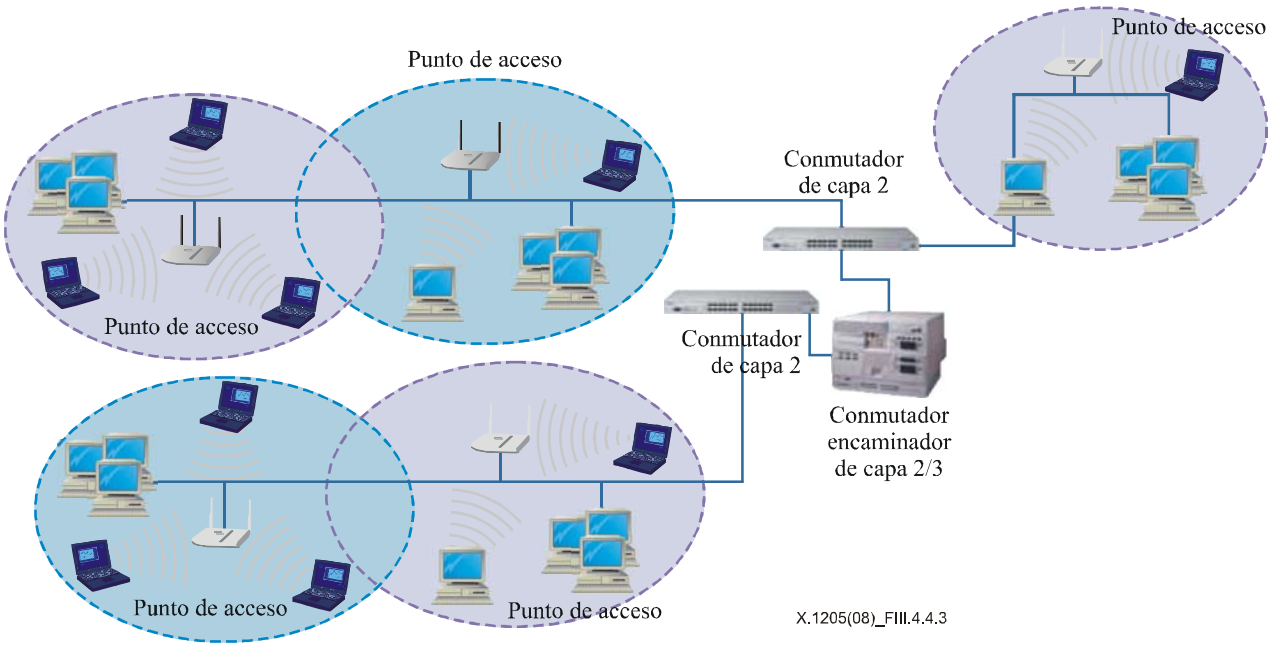

Figura III.4.4.3 – AP de WLAN IEEE 802.11 genérica con SSID común

III.4.4.4 Capa de gestión

También pueden emplearse contramedidas administrativas y operacionales para proteger la WLAN, por ejemplo ampliando la política de seguridad de la organización para comprender también la WLAN. Siempre que sea posible, los mecanismos de seguridad de la LAN existentes deben abarcar asimismo la WLAN; o habrán de integrarse mecanismos nuevos en los existentes. Por ejemplo, IPSec da a la empresa una gestión centralizada de los usuarios de la WLAN, los usuarios distantes y las reglas de los cortafuegos, y no necesita una aplicación de gestión adicional, si ya se está utilizando para el acceso extranet. Los vendedores están incorporando las WLAN en mecanismos tales como el descubrimiento de red, los analizadores de vulnerabilidad y los IDS.

III.4.4.5 Análisis de los protocolos de acceso WLAN

La robustez o debilidad de los diversos protocolos Wi-Fi presentados en las cláusulas anteriores, a saber, IEEE 802.11i, WPA2[2], WPA y WEP pueden analizarse con arreglo a las dimensiones de seguridad mencionadas en la Recomendación UIT-T X.805. El análisis que se ilustra para dos dimensiones, puede ampliarse hasta las ocho dimensiones.

---

2 Si bien WPA2 y IEEE 802.11i presentan características similares en cuanto a la seguridad, el hecho de que WPA2 pueda interfuncionar con un WPA menos seguro implica que los puntos débiles de WPA también afectan a la seguridad de WPA2.

Los resultados cualitativos de cada dimensión se presentan en los cuadros mediante las siguientes leyendas:

√	Satisfactorio
P	Parcial
X	No abarcado por la norma

Control de acceso

Las especificaciones originales [b-IEEE 802.11], incluida la WEP, no integran un mecanismo de control de acceso, por lo que las instalaciones de WLAN grandes utilizan una pasarela WLAN para efectuar el control de acceso a nivel de servicio. Habida cuenta de este hecho, el control de acceso del servicio WLAN para los usuarios se ha calificado como parcialmente adecuado.

La norma [b-IEEE 802.1X] es el mecanismo de control de acceso de usuarios para el servicio Wi-Fi de IEEE 802.11i, WPA y WPA2.

Cuadro III.2 – Cobertura para la dimensión control de acceso

Dimensión de seguridad: control de acceso								
Plano de seguridad	**Capas de seguridad**							
	Infraestructura				**Servicios**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Usuario	√	√	√	X	√	√	√	P
Control	√	X	X	X	√	√	√	X
Gestión	X	X	X	X	X	X	X	X

Autentificación

IEEE 802.11i, WPA2 y WPA utilizan IEEE 802.1X/EAP para la autentificación. En cambio, WEP recurre a una autentificación "abierta" o de "secreto compartido", que utiliza la misma clave estática que para la criptación. Así pues, la autentificación WEP se considera "parcial". En las otras normas, la autentificación podría recibir la misma calificación si se selecciona un protocolo EAP débil, por ejemplo el MD5, para [b-IEEE 802.1X].

La autentificación de la información de control que atraviesa puntos de acceso y otros elementos de red (para permitir la itinerancia) sólo se contempla en la IEEE 802.11i. Los protocolos de acceso que admiten otras normas suelen recurrir a mecanismos específicos para intercambiar esta información durante la itinerancia. La validación de la seguridad en estas aplicaciones queda fuera del alcance de la presente.

Cuadro III.3 – Cobertura para la dimensión autentificación

Dimensión de la seguridad: autentificación								
Plano de seguridad	**Capas de seguridad**							
	Infraestructura				**Servicios**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Usuario	√	√	√	P	√	√	√	P
Control	√	X	X	X	√	√	√	X
Gestión	X	X	X	X	X	X	X	X

Disponibilidad

Los ataques DoS, tales como la interferencia radioeléctrica (RF Jamming), desbordamiento de datos y apropiación de la sesión de capa 2, son ataques dirigidas contra la disponibilidad. Ninguna de las normas de seguridad de WLAN puede impedir los ataques dirigidos a la capa física, sencillamente porque actúan en la capa 2 y en capas superiores. Análogamente, ninguna de las normas abarca los fallos en el protocolo de acceso.

Cuadro III.4 – Cobertura para la dimensión disponibilidad

Dimensión de seguridad: disponibilidad								
Plano de seguridad	**Capas de seguridad**							
	Infraestructura				**Servicios**			
	IEEE 802.11i	**WPA2**	**WPA**	**WEP**	**IEEE 802.11i**	**WPA2**	**WPA**	**WEP**
Usuario	P	P	P	X	P	P	P	X
Control	P	P	P	X	P	P	P	X
Gestión	X	X	X	X	X	X	X	X

Al parecer, es posible diseñar, realizar y mantener redes WLAN relativamente protegidas utilizando la norma IEEE 802.11i o WPA2. Sin embargo, la mera aplicación de estas normas no garantiza la seguridad de extremo a extremo para WLAN. Como se ha indicado en este estudio de caso, la dimensión "disponibilidad" no se contempla en estas normas.

Bibliografía

[b-ITU-T G.729] Recomendación UIT-T G.729 (2007), *Codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico de estructura conjugada (CS-ACELP)*.

[b-ITU-T X.509] Recomendación UIT-T X.509 (2005), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

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

[b-IETF RFC 854] IETF RFC 854 (1983), *TELNET Protocol Specification* <http://www.ietf.org/rfc/rfc0854.txt?number=854>.

[b-IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)* <http://www.ietf.org/rfc/rfc0959.txt?number=959>.

[b-IETF RFC 1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm* <http://www.ietf.org/rfc/rfc1321.txt?number=1321>.

[b-IETF RFC 1510] IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* <http://www.ietf.org/rfc/rfc1510.txt?number=1510>.

[b-IETF RFC 1661] IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP)* <http://www.ietf.org/rfc/rfc1661.txt?number=1661>.

[b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats* <http://www.ietf.org/rfc/rfc1991.txt?number=1991>.

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* <http://www.ietf.org/rfc/rfc2104.txt?number=2104>.

[b-IETF RFC 2196] IETF RFC 2196 (1997), *Site Security Handbook* <http://www.ietf.org/rfc/rfc2196.txt?number=2196>.

[b-IETF RFC 2311] IETF RFC 2311 (1998), *S/MIME Version 2 Message Specification* <http://www.ietf.org/rfc/rfc2311.txt?number=2311>.

[b-IETF RFC 2411] IETF RFC 2411 (1998), *IP Security Document Roadmap* <http://www.ietf.org/rfc/rfc2411.txt?number=2411>.

[b-IETF RFC 2427] IETF RFC 2427 (1998), *Multiprotocol Interconnect over Frame Relay* <http://www.ietf.org/rfc/rfc2427.txt?number=2427>.

[b-IETF RFC 2459] IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* <http://www.ietf.org/rfc/rfc2459.txt?number=2459>.

[b-IETF RFC 2510] IETF RFC 2510 (1999), *Internet X.509 Public Key Infrastructure Certificate Management Protocols* <http://www.ietf.org/rfc/rfc2510.txt?number=2510>.

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol -- HTTP/1.1* <http://www.ietf.org/rfc/rfc2616.txt?number=2616>.

[b-IETF RFC 2631] IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method* <http://www.ietf.org/rfc/rfc2631.txt?number=2631>.

[b-IETF RFC 2661] IETF RFC 2661 (1999), *Layer Two Tunnelling Protocol "L2TP"* <http://www.ietf.org/rfc/rfc2661.txt?number=2661>.

[b-IETF RFC 2716] IETF RFC 2716 (1999), *PPP EAP TLS Authentication Protocol* <http://www.ietf.org/rfc/rfc2716.txt?number=2716>.

[b-IETF RFC 2748] IETF RFC 2748 (2000), *The COPS (Common Open Policy Service) Protocol* <http://www.ietf.org/rfc/rfc2748.txt?number=2748>.

[b-IETF RFC 2749] IETF RFC 2749 (2000), *COPS usage for RSVP* <http://www.ietf.org/rfc/rfc2749.txt?number=2749>.

[b-IETF RFC 2753] IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control* <http://www.ietf.org/rfc/rfc2753.txt?number=2753>.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary* <http://www.ietf.org/rfc/rfc2828.txt?number=2828>.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)* <http://www.ietf.org/rfc/rfc2865.txt?number=2865>.

[b-IETF RFC 2869] IETF RFC 2869 (2000), *RADIUS Extensions* <http://www.ietf.org/rfc/rfc2869.txt?number=2869>.

[b-IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture* <http://www.ietf.org/rfc/rfc3031.txt?number=3031>.

[b-IETF RFC 3084] IETF RFC 3084 (2001), *COPS Usage for Policy Provisioning (COPS-PR)* <http://www.ietf.org/rfc/rfc3084.txt?number=3084>.

[b-IETF RFC 3174] IETF RFC 3174 (2001), *US Secure Hash Algorithm 1 (SHA1)* <http://www.ietf.org/rfc/rfc3174.txt?number=3174>.

[b-IETF RFC 3377] IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification* <http://www.ietf.org/rfc/rfc3377.txt?number=3377>.

[b-IETF RFC 3579] IETF RFC 3579 (2003), *RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3579.txt?number=3579>.

[b-IETF RFC 3580] IETF RFC 3580 (2003), *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* <http://www.ietf.org/rfc/rfc3580.txt?number=3580>.

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP)* <http://www.ietf.org/rfc/rfc3748.txt?number=3748>.

[b-IETF RFC 4017] IETF RFC 4017 (2005), *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* <http://www.ietf.org/rfc/rfc4017.txt?number=4017>.

[b-IETF RFC 4252] IETF RFC 4252 (2006), *The Secure Shell (SSH) Authentication Protocol* <http://www.ietf.org/rfc/rfc4252.txt?number=4252>.

[b-IETF RFC 4366] IETF RFC 4366 (2006), *Transport Layer Security (TLS) Extensions* <http://www.ietf.org/rfc/rfc4366.txt?number=4366>.

[b-IETF RFC 4557] IETF RFC 4557 (2006), *Online Certificate Status Protocol (OCSP) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)* <http://www.ietf.org/rfc/rfc4557.txt?number=4557>.

[b-ISO/IEC 7816-x] ISO/IEC 7816-x, *Identification cards – Integrated circuit(s) cards with contacts* <http://www.iso.org/iso/search.htm?qt=7816&searchSubmit=Search&sort=rel&type=simple&published=on>.

[b-ISO/IEC 18028-2] ISO/IEC 18028-2:2006, *Information technology – Security techniques – IT network security – Part 2: Network security architecture.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40009>

[b-ISO/IEC 18028-3] ISO/IEC 18028-3:2005, *Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40010>

[b-ISO/IEC 18028-5] ISO/IEC 18028-5:2006, *Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks.* <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40012>

[b-ISO/IEC 18043] ISO/IEC 18043:2006, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35394>

[b-IEEE 802.11] IEEE 802.11-2007, *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>

[b-IEEE 802.1X] IEEE 802.1X-2004, *IEEE Standard for Local and metropolitan area networks: Port-Based Network Access Control* <http://www.ieee802.org/1/pages/802.1x.html>.

[b-W3C XML 1.0] W3C XML 1.0 (2004), *Extensible Markup Language (XML) 1.0 (Third Edition),* W3C Recommendation, Copyright © [4 February 2004] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University), <http://www.w3.org/TR/REC-xml/>.

[b-SSL3] The SSL Protocol Version 3.0, <http://wp.netscape.com/eng/ssl3/draft302.txt>

[b-WPA] Wi-Fi Alliance, *Wi-Fi Protected Access*, <http://www.wi-fi.org/white_papers/whitepaper-022705-deployingwpawpa2enterprise/>

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2009