Unión Internacional de Telecomunicaciones

UIT-T M.3016.3

(04/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE M: GESTIÓN DE LAS TELECOMUNICACIONES, INCLUIDA LA RGT Y EL MANTENIMIENTO DE REDES

Red de gestión de las telecomunicaciones

Seguridad en el plano de gestión: Mecanismo de seguridad

Recomendación UIT-T M.3016.3

UIT-T

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE M

GESTIÓN DE LAS TELECOMUNICACIONES, INCLUIDA LA RGT Y EL MANTENIMIENTO DE REDES

Introducción y principios generales de mantenimiento y organización del mantenimiento	M.10–M.299
Sistemas internacionales de transmisión	M.300–M.559
Circuitos telefónicos internacionales	M.560–M.759
Sistemas de señalización por canal común	M.760–M.799
Circuitos internacionales utilizados para transmisiones de telegrafía y de telefotografía	M.800–M.899
Enlaces internacionales arrendados en grupo primario y secundario	M.900–M.999
Circuitos internacionales arrendados	M.1000–M.1099
Sistemas y servicios de telecomunicaciones móviles	M.1100–M.1199
Red telefónica pública internacional	M.1200–M.1299
Sistemas internacionales de transmisión de datos	M.1300–M.1399
Designaciones e intercambio de información	M.1400–M.1999
Red de transporte internacional	M.2000–M.2999
Red de gestión de las telecomunicaciones	**M.3000–M.3599**
Redes digitales de servicios integrados	M.3600–M.3999
Sistemas de señalización por canal común	M.4000–M.4999

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

Recomendación UIT-T M.3016.3

Seguridad en el plano de gestión: Mecanismo de seguridad

Resumen

Esta Recomendación, en la que se determinan los mecanismos de seguridad en el plano de gestión de las telecomunicaciones, se refiere específicamente al aspecto de seguridad en el plano de gestión de los elementos de red (NE) y los sistemas de gestión (MS), que forman parte de la infraestructura de telecomunicaciones.

Orígenes

La Recomendación UIT-T M.3016.3 fue aprobada el 13 de abril de 2005 por la Comisión de Estudio 4 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Introducción

La infraestructura de las telecomunicaciones es crucial para las comunicaciones y la economía mundiales. En consecuencia, resulta esencial disponer de una seguridad apropiada para las funciones de gestión que permita controlar esa infraestructura. Ya existen muchas normas sobre seguridad aplicadas a la gestión de la red de telecomunicaciones. No obstante, se considera que la conformidad es reducida y que las implementaciones de los diversos equipos de telecomunicaciones y componentes de soporte lógico son incompatibles. Esta Recomendación define los mecanismos de seguridad mediante los cuales los fabricantes, organismos y proveedores de servicio podrán implementar una infraestructura segura de gestión de las telecomunicaciones. Aunque el conjunto de mecanismos de seguridad que se propone en esta Recomendación representa la mejor interpretación de los últimos adelantos, las tecnologías seguirán avanzando y las condiciones cambiarán. Para obtener los resultados previstos, esta Recomendación deberá evolucionar si las condiciones lo justifican. El objetivo de esta Recomendación será sentar las bases correspondientes en la materia. Los proveedores de servicio podrán incluir otros mecanismos de seguridad para responder a sus necesidades concretas aparte de las ya indicadas en la presente Recomendación.

Esta Recomendación forma parte de las Recomendaciones de la serie M.3016.x del UIT-T que tiene por objeto formular directrices y recomendaciones para la seguridad en el plano de gestión de las redes en evolución:

Recomendación UIT-T M.3016.0 – *Seguridad en el plano de gestión: Visión general*.

Recomendación UIT-T M.3016.1 – *Seguridad en el plano de gestión: Requisitos de seguridad*.

Recomendación UIT-T M.3016.2 – *Seguridad en el plano de gestión: Servicios de seguridad*.

Recomendación UIT-T M.3016.3 – *Seguridad en el plano de gestión: Mecanismo de seguridad*.

Recomendación UIT-T M.3016.4 – *Seguridad en el plano de gestión: Formulario de los perfiles*.

Recomendación UIT-T M.3016.3

Seguridad en el plano de gestión: Mecanismo de seguridad

1 Alcance

En las Recs. UIT-T M.1316.1 a M.3016.3 se especifica un conjunto de requisitos, servicios y mecanismos para lograr la seguridad que exigen las funciones de gestión necesarias para soportar la infraestructura de telecomunicaciones. En ellas no se señala si un determinado requisito/servicio/mecanismo es obligatorio o facultativo ya que las distintas administraciones y organizaciones requieren niveles diferentes de soporte de seguridad.

Esta Recomendación permite identificar los mecanismos de seguridad en el plano de gestión de las telecomunicaciones, centrándose específicamente en el aspecto de seguridad en el plano de gestión de los elementos de red (NE, *network elements*) y los sistemas de gestión (MS, *management systems*), que forman parte de la infraestructura de telecomunicaciones.

Esta Recomendación es de carácter genérico y por lo tanto no determina ni hace alusión a los mecanismos de seguridad de una interfaz específica de la red de gestión de las telecomunicaciones (RGT).

El formulario definido en la Rec. UIT-T M.3016.4 está previsto para ayudar a las organizaciones, administraciones y otros organismos nacionales e internacionales a especificar el soporte obligatorio y facultativo de los requisitos, así como las gamas de valores, valores, etc., necesarios para implementar sus políticas de seguridad.

2 Referencias

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

– Recomendación UIT-T G.8080/Y.1304 (2001), *Arquitectura de la red óptica con conmutación automática,* más enmienda 2 (2005).

– Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones*.

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

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

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

– Recomendación UIT-T M.3016.4 (2005), *Seguridad en el plano de gestión: Formulario de los perfiles*.

– Recomendación UIT-T X.509 (2000), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos,* más Corrigendum 1 (2001), Corrigendum 2 (2002) y Corrigendum 3 (2003).

– Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT,* más enmienda 1 (1996).

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

3 Definiciones

En esta Recomendación no se definen términos nuevos.

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos:

CORBA Arquitectura de intermediario de petición de objeto común (*common object request broker architecture*)

DoS Denegación de servicio (*denial of service*)

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

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

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

IETF Grupo de tareas especiales de ingeniería en Internet (*Internet engineering task force*)

IP Protocolo Internet (*Internet protocol*)

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

ISO/CEI Organización Internacional de Normalización/Comisión Electrotécnica Internacional (*International Organization for Standardization/International Electrotechnical Commission*)

MS Sistema de gestión; cualquier EMS, NMS u OSS[1] (*management system; any EMS, NMS, or OSS*)

NE Elemento de red (*network element*)

NE/MS NE o MS

NMS Sistema de gestión de red (*network management system*)

NTP Protocolo de señales horarias de red (*network time protocol*)

NTPv3 NTP versión 3

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

OS Sistema de operaciones (*operating system*)

OSS Sistema de soporte de operaciones (*operations support system*)

RFC Petición de comentarios (*request for comments*)

RGT Red de gestión de las telecomunicaciones

SAML Lenguaje de marcaje de aserción de seguridad (*security assertion markup language*)

---

[1] Por lo general se puede emplear OSS en el mismo contexto que MS en cualquiera de las capas de la jerarquía de la red de gestión de telecomunicaciones.

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

SNMPv3 Protocolo simple de gestión de red, versión 3 (*simple network management protocol version 3*)

SOAP Protocolo simple de acceso a objeto (*simple object access protocol*)

SSH Intérprete de comandos seguro (*secure shell*)

SSL Capa de zócalo segura (*secure socket layer*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TLS Seguridad de la capa de transporte (*transport layer security*)

UIT-T Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones

XML Lenguaje de marcaje extensible (*extensible markup language*)

5 Convenios

En las Recs. M.3016.1, M.3016.2 y M.3016.3 se utiliza un descriptor con el fin de identificar los diferentes requisitos, servicios y mecanismos. Este descriptor está integrado por una de las siguientes etiquetas de tres letras, seguida por un número:

– REQ para indicar requisito.

– SER para indicar servicio.

– MEC para indicar mecanismo.

6 Mecanismos de seguridad

En la presente cláusula se exponen los mecanismos que sirven específicamente para garantizar la seguridad de las operaciones, administración, mantenimiento y aprovisionamiento (OAM&P, *operations, administration, maintenance, and provisioning*) y para la seguridad del sistema de soporte de operaciones (OSS, *operations support system*), en la medida en que se aplican concretamente a la seguridad del plano de gestión y tratándose de la infraestructura, los servicios y las aplicaciones.

El cuadro 1 siguiente se extrae de la Rec. UIT-T M.3016.0 (cuadro 4 de dicha Recomendación). El cuadro, en el que puede verse un panorama general de la relación entre los requisitos y los servicios de seguridad, se utiliza como punto de partida para organizar las demás Recomendaciones de la serie. Por ejemplo, en la Rec. UIT-T M.3016.1 se tratan los requisitos funcionales de seguridad, la Rec. UIT-T M.3016.2 versa sobre los servicios de seguridad y en esta Recomendación (Rec. UIT-T M.3016.3) se abordan los mecanismos de seguridad específicos relacionados con los servicios de seguridad.

En esta cláusula se definen sólo los servicios de seguridad que se tienen en cuenta en las soluciones normales; se omiten otros servicios posibles (por ejemplo, la detección de negación de servicio).

Cuadro 1/M.3016.3 – Correspondencia entre los requisitos de seguridad y los servicios de seguridad

Requisito funcional de seguridad	Servicio de seguridad
Verificación de identidades	autenticación del usuario autenticación de la entidad par autenticación del origen de los datos
Acceso controlado y autorización	control de acceso
Protección de la confidencialidad – datos almacenados	control de acceso confidencialidad
Protección de la confidencialidad – datos transferidos	confidencialidad
Protección de la integridad de los datos – datos almacenados	control de acceso
Protección de la integridad de los datos – datos transferidos	integridad
Imputabilidad	no repudio
Registro de actividades	registro de auditoría
Notificación de alarma de seguridad	alarma de seguridad
Auditoría de seguridad	registro de auditoría
Protección de la RCD	inspección de paquetes

En el cuadro 2, a continuación, se esboza la manera en que se organiza esta cláusula:

Cuadro 2/M.3016.3 – Disposición de la presente cláusula

Cláusula	Contenido
6.1	Se examinan los mecanismos de seguridad relacionados con la autenticación, incluidas la autenticación del usuario y la autenticación de la entidad par.
6.2	Se examina la autenticación del origen de los datos.
6.3	Se examinan los mecanismos de seguridad del control de acceso.
6.4	Se examinan los mecanismos de seguridad de la confidencialidad de los datos.
6.5	Se examinan los mecanismos de seguridad de la integridad de los datos.
6.6	Se examinan los mecanismos de seguridad del registro de auditoría.

6.1 Autenticación del usuario

La autenticación del usuario es el acto de verificar la identidad declarada de una persona. La autenticación del usuario puede basarse en mecanismos de seguridad que incluyen:

– Una combinación del identificador del usuario y la contraseña (con contraseñas convenientemente complejas) en donde la contraseña puede ser una contraseña que se da una sola vez (por ejemplo, SecureID).

– La autenticación con múltiples factores.

– La autenticación única al inicio de la sesión.

En la presente cláusula se abordan los mecanismos de seguridad relacionados con la autenticación del usuario.

6.1.1 Autenticación empleando el identificador de usuario y contraseñas

Cabe utilizar un identificador de usuario y contraseñas estáticas para la autenticación del usuario. Mediante la autenticación del usuario se comprueba la verdadera identidad del usuario legítimo del sistema y se evita que haya impostores que usurpen su identidad. Mediante una autenticación

adecuada es posible llevar un registro de las actividades y aplicar el control de acceso con el fin de limitar las actividades y actuaciones de los usuarios a las previamente autorizadas, como se señala en 6.2.

Gracias a la autenticación mediante el identificador de usuario y contraseña, se asigna un identificador de usuario único a cada usuario y acto seguido se asigna una contraseña secreta con el grado de complejidad necesario que se utiliza en combinación con el identificador de usuario para comprobar la identidad.

Las contraseñas deben incluir los suficientes caracteres y otros elementos aleatorios para evitar la adivinación por parte de personas o con técnicas automatizadas. En cuanto a contraseñas complejas, cabe citar requisitos tales como los siguientes:

MEC 1: Puede exigirse que las contraseñas tengan un número mínimo de caracteres (por ejemplo, ocho caracteres).

MEC 2: Puede evitarse que las contraseñas incluyan ciertos caracteres.

MEC 2a: Puede evitarse que las contraseñas incluyan una repetición o el inverso del identificador de usuario asociado.

MEC 2b: Puede exigirse que las contraseñas no incluyan en ninguna parte un conjunto de secuencias configuradas de caracteres (por ejemplo, palabras de un diccionario o nombres de productos).

MEC 3: Puede exigirse que las contraseñas contengan un número máximo de ocurrencias consecutivas de un mismo carácter.

MEC 4: Puede exigirse que las contraseñas incluyan al menos un cierto número de caracteres alfabéticos en minúsculas y/o en mayúsculas.

MEC 5: Puede exigirse que las contraseñas incluyan por lo menos un cierto número de caracteres numéricos.

MEC 6: Puede exigirse que las contraseñas incluyan al menos un cierto número de caracteres especiales.

Con el fin de garantizar un sistema seguro de autenticación es también muy importante gestionar las contraseñas. Por ejemplo, convendría contar con las siguientes capacidades de gestión del sistema de contraseñas:

MEC 7: El sistema de gestión de contraseñas podría exigir que se ingrese la contraseña anterior con el fin de evitar que otro usuario modifique la contraseña de un usuario registrado, sin su conocimiento.

MEC 8: El sistema podría verificar automáticamente que toda nueva contraseña de ingreso sea diferente de la contraseña anterior. (Dado que por lo general las contraseñas se almacenan empleando criptación de una vía, podría exigirse el ingreso de la contraseña anterior con el fin de permitir que al sistema determine qué tan diferentes resultan la contraseña anterior y la nueva[2].)

MEC 9: El sistema podría llevar una lista histórica de las contraseñas con el fin evitar la reutilización de contraseñas.

MEC 10: El sistema puede obligar hacer necesario modificar contraseñas después de cierto tiempo.

---

[2] Como una excepción la criptación de una vía, las contraseñas criptadas simétricamente se pueden emplear cuando se requiera contraseñas que necesitan ser descriptadas para usos internos transitorios en comunicaciones confiables de sistema a sistema o inicio de sesión único.

MEC 11: Tras una cierta cantidad de intentos fallidos de contraseña, el sistema puede restringir otros intentos de contraseña durante un cierto tiempo (por ejemplo, 60 minutos) o forzar un bloqueo de usuarios. Cabría la posibilidad de que los usuarios bloqueados deban señalar al personal de gestión de seguridad la necesidad de eliminar el estado de bloqueo.

6.1.2 Autenticación mediante múltiples factores

La autenticación mediante múltiples factores remite al proceso de autenticación que requiere de dos o más tipos de información o factores con el fin de comprobar la identidad para la autenticación del usuario. La exigencia de múltiples factores aumenta la seguridad del sistema de autenticación, pues no depende más que de un solo factor, que puede ser más fácilmente burlado.

Los factores de autenticación que se utilizan típicamente en sistemas de autenticación de usuarios de múltiples factores incluyen:

Algo que el usuario **conoce**: Por ejemplo, conocimiento de una contraseña o de una frase secretas.

Algo que el usuario **tiene**: Por ejemplo, un testigo, una tarjeta inteligente, un generador de contraseñas por una sola vez.

Algo que el usuario **es**: Por ejemplo, su huella digital u otra característica biométrica.

Un mecanismo muy común de autenticación mediante múltiples factores, es la autenticación con dos factores, la cual exige dos elementos credenciales para la autenticación. Un ejemplo típico de autenticación mediante dos factores es el sistema de tarjeta bancaria, en virtud del cual el usuario no sólo debe poseer la tarjeta sino que también comprobar que conoce el número de identificación personal (PIN, *personal identification number*) asociado a la tarjeta.

MEC 12: Autenticación mediante múltiples factores con un número especificado de factores.

6.1.3 Autenticación de usuario mediante inicio de sesión único

La autenticación de usuario puede incluir métodos para inicio de sesión único seguro e infraestructura de clave pública del certificado X.509. En inicio de sesión único seguro, el protocolo también le solicita las credenciales a la(s) entidad(es). Ahora bien, el usuario podría no tener que ingresar las credenciales por estar éstas grabadas de manera segura (por ejemplo, mediante Kerberos). Las técnicas de inicio de sesión único seguro sirven para que el usuario no tenga necesidad de autenticarse varias veces ante el sistema, lo que podría ser un inconveniente.

MEC 13: Autenticación única al inicio de sesión.

6.2 Autenticación de la entidad par y del origen de los datos

Se utilizan los mecanismos de autenticación de la entidad par con el fin de verificar la identidad declarada entre sistemas pares. Se utilizan los mecanismos de seguridad de autenticación del origen de los datos con el fin de garantizar que los mensajes provienen del sistema que declara haberlos enviado. La autenticación de la entidad par y la autenticación del origen de los datos están relacionadas cercanamente y pueden utilizar mecanismos de seguridad que incluyen:

– Mecanismos de autenticación criptográfica.

– Mecanismos de autenticación con trayecto confiable.

En la presente cláusula se analizan estos mecanismos de seguridad de autenticación.

6.2.1 Autenticación criptográfica

Los mecanismos de autenticación criptográfica permiten la autenticación durante la comunicación de datos entre sistemas (por ejemplo, de sistema a sistema o de aplicación a aplicación) y constituyen la base de las comunicaciones privadas con integridad total de datos. La autenticación

criptográfica de la entidad remitente permite al receptor autenticar la identidad del remitente (autenticación de la entidad par) y determinar el origen del mensaje (autenticación del origen de los datos) durante la comunicación de datos. En un canal de comunicación seguro, la autenticación de la entidad par y del origen de los datos puede basarse en el uso de información criptográfica asociada a cada mensaje, con el fin de vincular al mensaje la identidad de la entidad remitente. El receptor revisará la información criptográfica que se suministra con el mensaje, con el fin de verificar la verdadera identidad de la entidad remitente.

Entre las técnicas criptográficas utilizadas para la autenticación de la entidad par y del origen de los datos se encuentran la criptación de clave pública, la criptación de clave simétrica, las firmas digitales y las técnicas digitales de troceo[3]. La autenticación criptográfica puede ser unidireccional: se autentica uno solo de los extremos de la conversación; o bidireccional: se autentican los dos extremos. La autenticación bidireccional es más segura y puede utilizarse para contribuir a evitar ataques activos.

MEC 14: Autenticación de la entidad par y del origen de los datos, mediante criptación de clave pública.

MEC 15: Autenticación de la entidad par y del origen de datos, mediante criptación de clave simétrica.

MEC 16: Autenticación de la entidad par y del origen de datos, mediante firmas digitales.

MEC 17: Autenticación de la entidad par y del origen de datos, mediante técnicas digitales de troceo.

MEC 18: Autenticación criptográfica bidireccional.

6.2.2 Autenticación de usuario con trayecto fiable

La autenticación con trayecto fiable es un mecanismo de seguridad mediante el cual se aseguran las interacciones de autenticación de sistema a sistema, recurriendo a un trayecto seguro de comunicaciones. Este mecanismo, que no es posible imitar, sólo puede ser activado por el sistema. El trayecto confiable puede ser un trayecto físico dedicado (es decir, un terminal conectado directamente al sistema) o un trayecto criptado que incluya protección de la integridad y antirreproducción (por ejemplo, una red privada virtual IPSec, un túnel capa de zócalo seguro/seguridad de la capa de transporte (SSL/TLS) o un intérprete de comandos seguro (SSH, *secure shell*))[4]. En el apéndice I se abordan los protocolos de seguridad IPSec, SSL/TLS y SSH.

MEC 19: Autenticación de la entidad par y del origen de los datos basada en un trayecto confiable.

6.3 Control de acceso

La RGT puede ofrecer capacidades para garantizar que los actores no autorizados puedan acceder a la información o a los recursos del caso. Mediante los mecanismos de seguridad de control de acceso se garantiza que sólo los usuarios autorizados estén en condiciones de gestionar los recursos de seguridad del sistema.

Cabe la posibilidad de que los mecanismos de seguridad para controlar el acceso sean proporcionados por un sistema centralizado, a menudo aunado a un sistema de autenticación. Por ejemplo, se puede utilizar un servidor centralizado de sistemas de usuario para acceso a distancia por marcación directa de extensiones (RADIUS, *remote access dial-in user system*) junto con una

---

[3] Instituto Nacional de Normas de los Estados Unidos T1.243-1995, *Operations, Administration, Maintenance*.

[4] Adaptación del National Computer Security Centre, NCSC-TG-004-88, *Glossary of Computer Security Terms*, octubre de 1998 (se encuentra en http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

base de datos protocolo ligero de acceso al directorio (LDAP, *lightweight directory access protocol*) con el fin de ofrecer un sistema centralizado para la autenticación y el control de acceso.

Los mecanismos de seguridad de control de acceso pueden tener algunas de las siguientes características:

MEC 20: Acciones administrativas vinculadas a individuos específicos.

MEC 21: El mecanismo de seguridad de control soporta el concepto de "privilegio menor" (es decir que se autoriza a una persona a visualizar datos, modificar datos o iniciar acciones de gestión, sólo para desempeñar las funciones que permite la actuación de esa persona).

MEC 22: No se permite bloquear al menos algunas de las cuentas de administrador por causa de actividades relacionadas con contraseñas, por ejemplo, fallidos o caducidad de un temporizador.

MEC 23: Cabe definir un cierto número de actuaciones de administrador con diversos grados de privilegio en cuanto a las acciones cruciales de gestión de seguridad. Así, en un sistema podrían definirse cinco actuaciones de usuario administrador, mientras que en otro sistema se podrían definir tres actuaciones de usuario administrador. En cada caso se pueden definir las actuaciones de manera que tengan privilegios diferentes con respecto a las siguientes acciones relacionadas con la seguridad:

MEC 23a: Definir y asignar privilegios de usuario.

MEC 23b: Añadir y borrar identificadores de usuario.

MEC 23c: Inicializar y reiniciar contraseñas de ingreso.

MEC 23d: Inicializar y modificar claves criptográficas.

MEC 23e: Fijar el umbral de envejecimiento del sistema para las contraseñas de ingreso.

MEC 23f: Fijar el límite del sistema en cuanto a la cantidad de ingresos fallidos para cada identificador de usuario.

MEC 23g: Eliminar un bloqueo o modificar el valor del temporizador de bloqueo del sistema.

MEC 23h: Fijar el valor del temporizador de inactividad del sistema.

MEC 23i: Fijar el registro de la seguridad del sistema y la configuración de alarmas.

MEC 23j: Gestionar los procesos de registro de seguridad del sistema.

MEC 23k: Actualizar el software de seguridad.

MEC 23l: Finalizar cualquier sesión de usuario o de sistema.

MEC 23m: Definir y asignar los privilegios de un nuevo usuario o grupo al nivel de aplicación.

MEC 23n: Llevar un registro de todas las solicitudes de acceso a la aplicación.

MEC 23o: Añadir o borrar usuarios al nivel de aplicación.

MEC 23p: Supervisar todos los registros cronológicos de seguridad de las aplicaciones.

MEC 23q: Configurar el registro y las alarmas de la seguridad de las aplicaciones.

MEC 23r: Gestionar los procesos de registro de seguridad de las aplicaciones.

MEC 23s: Finalizar cualquier sesión de las aplicaciones de los usuarios.

6.4 Confidencialidad de los datos

Se utilizan los mecanismos de seguridad para proteger la confidencialidad de los datos y evitar así su recepción no autorizada. En la presente cláusula se abordan los mecanismos de seguridad criptográficos que garantizan la confidencialidad de los datos.

La confidencialidad de los datos se basa en fundamentos criptográficos. La criptografía utiliza algoritmos especiales públicamente disponibles y que se basan en normas lo que permite un examen amplio y una fácil implementación. La "resistencia" criptográfica depende del algoritmo criptográfico y del tamaño de la clave a los que se recurren (por resistencia se entiende el tiempo necesario para invertir el proceso de ingeniería y encontrar o adivinar así el valor o los valores de las claves que están siendo utilizadas con determinado algoritmo).

Los protocolos de seguridad (por ejemplo IPSec, SSL/TLS, SSH) ofrecen por lo general autenticación del origen de los datos, integridad de los datos y confidencialidad de los datos (en el apéndice I se tratan los protocolos de seguridad IPSec, SSL/TLS y SSH). Se diseñan extensiones de seguridad a otros protocolos como el protocolo simple de gestión de red versión 3 (SNMPv3)[5], la arquitectura de intermediario de petición de objeto común (CORBA, *common object request broker architecture*), el protocolo de pasarela de frontera y el primer trayecto más corto abierto, con el fin de ofrecer autenticación del origen de los datos e integridad de los datos.

Son de suma importancia los métodos utilizados para generar, almacenar, distribuir, destruir y revocar claves criptográficas para la confidencialidad de los datos. Hay otros factores adicionales que inciden directamente en la resistencia de la seguridad de un determinado sistema criptográfico, como la longitud de la clave, la selección de la clave y la selección del algoritmo.

6.4.1 Confidencialidad simétrica de los datos

La criptación simétrica o de clave secreta remite a sistemas criptográficos en los que coinciden las claves de cifrado y de descifrado. Los criptosistemas simétricos exigen una preparación inicial para que los interesados compartan una clave secreta única (es decir, la clave de criptación). La clave se debe distribuir a los interesados a través de un medio seguro, o bien debe generarse internamente (por ejemplo, utilizando una clave raíz secreta compartida) debido a que el conocimiento de la clave de cifrado hace necesario conocer la clave de descifrado y viceversa.

Los mecanismos de seguridad para garantizar la confidencialidad de los datos pueden basarse en algoritmos criptográficos simétricos, como la norma de criptación de datos (DES, *data encryption standard*), la norma de encriptación avanzada (AES, *advanced encryption standard*), el algoritmo de criptación de datos triple (3DES, *triple data encryption algorithm*) y otros algoritmos.

DES es un algoritmo de encriptación simétrico de 56 bits que se ha utilizado durante muchos años. Dada la corta longitud de su clave, DES es vulnerable al ataque por agotamiento de claves, si se utilizan cómputos masivos en paralelo, por lo que ahora se considera débil. El Instituto Nacional de Normalización y Tecnología (NIST, *National Institute of Standards and Technology*) de los Estados Unidos desechó este algoritmo.

El NIST escogió la norma AES como algoritmo de criptación simétrico normalizado para reemplazar DES en las aplicaciones oficiales de Estados Unidos. La norma AES permite procesar longitudes de clave de 128, 192 y 256 bits.

3DES es básicamente el mismo algoritmo que DES, ejecutado tres veces, sea con dos claves de 56 bits o tres claves de 56 bits. En la publicación sobre normas federales de tratamiento de la información (FIPS, *federal information processing standard*) 46-3, *Data Encryption Standard*, de octubre de 1999, apéndice 2, página 22 (véase: http://csirc.nist.gov/publications/fips/fips46-3/fips46-3.pdf), se especifica la norma 3DES.

La norma 3DES puede ejecutarse empleando dos claves independientes de 56 bits o tres claves independientes de 56 bits, de las que se esperaría una resistencia de 112 y 168 bits, respectivamente. Sin embargo el ataque "encuentro en el centro" puede disminuir la resistencia de 3DES de dos claves a tan sólo 57 bits en vez de los 112 bits previstos. Ese ataque puede disminuir la resistencia de 3DES, haciéndola pasar así de tres claves a tan sólo 112 bits en vez de los 168 bits esperados.

---

[5] SNMPv3 también puede ofrecer confidencialidad.

Para lograr una seguridad mayor debe utilizarse 3DES con tres claves independientes y habría que suponer una resistencia de 112 bits en la situación más desfavorable.

El algoritmo DES puede ejecutarse con relativa rapidez, ya que tiene una clave corta de 56 bits, mientras que el 3DES es, por su parte, mucho más lento, puesto que ejecuta tres veces DES. AES, que consta de una longitud de clave mínima de 128 bits, es criptográficamente más resistente que 3DES y aun así se puede ejecutar muy rápidamente tanto en equipo como en soporte lógico. Por ejemplo, una implementación en soporte lógico de AES puede procesarse aproximadamente a la misma velocidad en las mismas condiciones que DES, pero obteniendo una resistencia criptográfica mucho mayor que la de DES.

MEC 24: Confidencialidad simétrica de los datos con el algoritmo criptográfico DES.

MEC 25: Confidencialidad simétrica de los datos utilizando el algoritmo criptográfico AES.

MEC 26: Confidencialidad simétrica de los datos utilizando el algoritmo criptográfico 3DES.

6.4.2 Confidencialidad asimétrica de los datos

Un sistema de criptación asimétrico es aquel en el que, si bien las claves de cifrado y de descifrado se relacionan entre sí, son diferentes. Una de las claves es pública, mientras que la otra se mantiene secreta. La clave pública es diferente de la privada y hasta hoy se desconoce la forma de deducir la clave privada a partir de la clave pública. Las claves públicas se distribuyen de manera generalizada, mientras que la clave privada se mantiene secreta en todo momento.

Los mecanismos de seguridad aplicables para lograr la confidencialidad de los datos pueden utilizar algoritmos criptográficos asimétricos como Rivest Shamir Adleman (RSA), criptosistema de curva elíptica (ECC, *elliptic curve cryptography*) y otros.

El algoritmo RSA es un algoritmo asimétrico de uso común que puede utilizarse para la criptación de firmas digitales. RSA se basa en la dificultad matemática inherente a la factorización en grandes números primos. Entre las longitudes de clave típicas para el algoritmo RSA, cabe citar 1024 bits y 2048 bits. Es posible señalar que con una longitud de clave de 2048 bits, RSA tiene una resistencia criptográfica aproximadamente equivalente a la la criptación simétrica de 128 bits.

El criptosistema de curva elíptica (ECC) es un nuevo método de criptografía de clave pública (motivo por el cual puede compararse al algoritmo RSA). Al utilizar ECC, se define una curva elíptica en un cierto campo y ulteriormente se resuelve el problema que suscita el logaritmo discreto de la curva elíptica en este campo. La ventaja principal de ECC frente a otros algoritmos de clave pública es la longitud de la clave. Una clave de 160 bits de ECC posee aproximadamente la misma seguridad que una clave de 1024 bits del algoritmo RSA, y una clave de ECC de 210 bits es aproximadamente equivalente a un algoritmo RSA de 2048 bits. La clave más pequeña de ECC redunda en una tara de computación menor y un sistema criptográfico[6] más eficiente.

MEC 27: Confidencialidad asimétrica de datos utilizando el algoritmo criptográfico RSA con una longitud de clave específica.

MEC 28: Confidencialidad asimétrica de datos utilizando el algoritmo criptográfico ECC con una longitud de clave específica.

6.4.3 Confidencialidad de los datos – Resumen

En el cuadro 3 se presentan en un formato tabular ejemplos de algoritmos que pueden utilizarse para garantizar la confidencialidad de los datos. También se deben tener en cuenta temas como el formateo, el relleno, el tratamiento de condiciones de error, la selección de los números primos

---

[6] Para mayor información acerca de los algoritmos RSA, Diffie-Hellman y ECC, véase *Digital Signature Standard* de noviembre de 2002 (se encuentra disponible en http://csrc.nist.gov/cryptval/dss.htm).

adecuados, el tamaño del exponente público y, en el caso de ECC, también el campo base y la curva. Sin embargo, estos temas no se abordan en la presente Recomendación.

Cuadro 3/M.3016.3 – Ejemplos de algoritmos criptográficos para garantizar la confidencialidad de los datos

Categoría	Algoritmo	Comentarios
Algoritmos de criptación simétrica	AES	Norma de criptación avanzada
	3-DES	Algoritmo de criptación de datos triple
	DES	Norma de criptación de datos
Algoritmos de criptación simétrica	RSA	Rivest, Shamir, Adleman
	ECC	Criptografía de curva elíptica

6.5 Integridad de los datos

Los mecanismos de seguridad en cuanto a la integridad de los datos se utilizan para garantizar que no se modifiquen los datos transmitidos.

La integridad de los datos se basa en principios de criptografía. La criptografía utiliza algoritmos especiales puestos a disposición del público y basados en normas, lo que permite su supervisión generalizada y fácil implementación. Los protocolos de seguridad (como por ejemplo, IPSec, SSL/TLS, SSH) ofrecen normalmente servicios de integridad de datos basados en algoritmos criptográficos y otros servicios de seguridad como la confidencialidad de los datos y la autenticación del origen de los datos. (En el apéndice I se tratan los protocolos de seguridad IPSec, SSL/TLS y SSH.)

Revisten suma importancia los métodos que se aplican para generar, almacenar, distribuir, destruir y revocar claves criptográficas destinadas a velar por la integridad de los datos. Asimismo, hay factores como la longitud y la clave, la selección de la clave y el algoritmo de selección que inciden directamente en la resistencia de la seguridad de un criptosistema específico.

6.5.1 Integridad de datos simétrica

La integridad de datos simétrica o de clave secreta remite a sistemas criptográficos en los que las claves que se utilizan para velar por la integridad de los datos son las mismas tanto para el transmisor como para el receptor de información. Los criptosistemas simétricos exigen que las partes interesadas se pongan inicialmente de acuerdo para compartir una clave secreta única (por ejemplo, la clave de verificación). La clave debe ser distribuida a los interesados sirviéndose de un medio seguro o debe ser generada internamente (por ejemplo, sobre la base en una clave raíz secreta compartida).

Cuando se trata de mensajes de longitud indeterminada, los mecanismos de seguridad de integridad de datos simétrica podrán utilizar algoritmos del tipo Message Digest con clave junto con funciones de troceo. Entre los algoritmos Message Digest con clave se encuentran el algoritmo "código de autenticación de mensaje troceado" con Message Digest 5 (HMAC-MD5-96, *hashed message authentication code with message digest 5*)[7] y el "código de autenticación de mensaje troceado" con "algoritmo de troceo seguro 1" (HMAC-SHA-1-96, *hashed message authentication code with secure hash algorithm 1*)[8].

---

[7] Grupo de tareas especiales de ingeniería en Internet, petición de comentarios 2403, *The Use of HMAC-MD5-96 within ESP and AH*, C. Madson, R. Glenn, noviembre de 1998.

[8] Grupo de tareas especiales de ingeniería en Internet, petición de comentarios 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*, C. Madson, R. Glenn, noviembre de 1998.

MEC 29: Integridad de datos simétrica basada en el algoritmo criptográfico HMAC-MD5-96.

MEC 30: Integridad de datos simétrica basada en el algoritmo criptográfico HMAC-SHA-1-96.

6.5.2 Integridad de datos asimétrica

Un sistema de integridad de datos asimétrica es aquel en el que las claves de firma y de verificación son diferentes aunque estén relacionadas. La clave de verificación es pública, mientras que la clave de firma se mantiene secreta. La clave de firma es diferente de la clave de verificación y no se conoce ningún método que sirva para deducir la clave de firma a partir de la clave de verificación. Las claves de verificación se distribuyen de manera generalizada, pero la clave de firma siempre se mantiene secreta.

Los mecanismos de seguridad para garantizar la integridad de los datos pueden utilizar algoritmos criptográficos asimétricos, como el algoritmo de la signatura digital (DSA, *digital signature algorithm*) y el algoritmo Rivest, Shamir, Adleman (RSA).

Cuando se utiliza el mecanismo de seguridad para la integridad de los datos asimétrica, el remitente firma un compendio del mensaje con la clave de firma (privada) y el receptor utiliza la clave de verificación (pública) con el fin de verificar que el compendio del mensaje fue firmado por quien se supone lo originó.

MEC 31: Integridad de los datos asimétrica utilizando el algoritmo criptográfico DSA con longitud de clave determinada.

MEC 32: Integridad de datos asimétrica utilizando el algoritmo criptográfico RSA con longitud de clave determinada.

6.5.3 Integridad de los datos – Resumen

En el cuadro 4 se presenta en formato tabular algunos algoritmos que pueden utilizarse para velar por la integridad de los datos. Habrá que tener en cuenta también aspectos tales como el formateo, el relleno, el tratamiento de condiciones de error y la selección de los números primos adecuados. Sin embargo, éstos no son temas que se examinen en la presente Recomendación.

Cuadro 4/M.3016.3 – Ejemplos de algoritmos criptográficos para velar por la confidencialidad de los datos

Categoría	Algoritmo	Comentarios
Algoritmos asimétricos para la verificación de mensajes	DSA	Algoritmo de la signatura digital
Algoritmos simétricos para la verificación de mensajes	HMAC-MD5-96	Código de autenticación de mensaje troceado con Message Digest 5
	HMAC-SHA-1-96	Código de autenticación de mensaje troceado con algoritmo troceado asegurado 1

6.6 Registro de auditoría

Los elementos de red y los sistemas de gestión deben ofrecer las capacidades idóneas en cuanto a la investigación, la auditoría y la realización en tiempo real de actividades de detección, análisis y protección, si se desea poder efectuar acciones correctivas. En la presente cláusula se abordan los mecanismos de seguridad utilizados para dichos registros de auditoría de seguridad. Los detalles concretos del contenido y el formato de los registros de auditoría de seguridad no se tratan en esta Recomendación.

Los elementos de red y los sistemas de gestión pueden llevar los registros de auditoría de seguridad. Estos registros de auditoría de seguridad pueden almacenarse de manera local o transmitirse a un almacén centralizado de registros y/o dispositivo centralizado para el análisis de registros.

Syslog es un mecanismo ordinario que se utiliza para transmitir registros de auditoría de seguridad desde un almacén local a un almacén de registros centralizado.

Por lo general, sería necesario poder llevar un registro de toda acción que modifique los atributos y servicios de seguridad, los controles de acceso u otros parámetros de configuración de los dispositivos, así como de los intentos de registro y su resultado, y de toda salida de sistema o finalización de la sesión, sea que ésta se efectúe a distancia o desde la consola. Tratándose de algunas acciones sujetas a auditoría puede ser necesario llevar el registro de mensajes OAM&P que no estén relacionados con la seguridad y que a veces se denominan mensajes "de cambios recientes".

Una vez etiquetadas con las correspondientes secuencia y autenticación criptográfica (mediante firma) por parte del elemento de red o del sistema de gestión, las entradas del registro de auditoría pueden enviarse a un servidor de auditoría no modificable. Los registros de auditoría de seguridad pueden ser enviados a un almacén centralizado a través de un trayecto seguro. Si se desea que se realicen análisis precisos de las acciones, es menester sincronizar de manera rigurosa y segura (por ejemplo con NTPv3) las numerosas fuentes del registro.

MEC 33: Registro de auditorías de seguridad basados en Syslog.

MEC 34: Entrada del registro de auditoría de seguridad con la siguiente información:

MEC 34a: Una descripción de la acción o de la acción real que se está registrando.

MEC 34b: La identidad y nivel de seguridad del usuario o proceso que inició la acción.

MEC 34c: La fecha y hora a la que ocurrió la acción.

MEC 34d: Información del origen y destino de la red, si es pertinente (por ejemplo, al ingreso).

MEC 34e: Indicación del éxito o fracaso de la actividad.

MEC 34f: Cualquier acción que implica auditoría.

MEC 35: Los registros de auditoría de seguridad son enviados a un servidor de auditoría no modificable.

MEC 36: Los registros de auditoría de seguridad son firmados criptográficamente.

MEC 37: Los registros de auditoría de seguridad son enviados a un almacén centralizado a través de un trayecto seguro.

6.7 Intercambio de claves

En el caso de aplicaciones con confidencialidad simétrica de datos o con integridad simétrica de datos, las claves criptográficas deben intercambiarse de manera segura entre los puntos extremos. Por regla general, las claves para dichos algoritmos simétricos deben intercambiarse mediante un proceso estrechamente vinculado a la autenticación para evitar que un atacante se interponga entre los procesos de autenticación y de distribución de claves.

Los métodos utilizados para generar, almacenar, distribuir, destruir y revocar estas claves criptográficas son de suma importancia. Por lo demás, aspectos tales como la longitud de la clave, la elección de la clave y la elección del algoritmo inciden directamente sobre el nivel de seguridad que ofrece un criptosistema.

Existen varios métodos para el aprovisionamiento y/o el intercambio de claves criptográficas. Un método de concepción sencilla es el intercambio de claves previamente compartidas, intercambio mediante el cual, se entregan las claves a los puntos extremos por un medio externo, cuando así se estime oportuno. Por ejemplo, es posible ordenar a los administradores de red que seleccionen y configuren las claves en los puntos extremos. El intercambio de claves previamente compartidas puede resultar el adecuado cuando se trata de un número reducido de puntos extremo, pero deja de serlo si es grande el número de puntos extremo, ya que resulta engorroso generar y configurar una gran cantidad de claves.

En cuanto a los servicios de intercambio de claves, cabe utilizar algoritmos asimétricos como Rivest, Shamir, Adleman (RSA). Con RSA, uno de los puntos extremo elige las claves criptográficas simétricas y las distribuye a los otros puntos extremo, protegidas con el algoritmo de criptación RSA. Si se recurre a este método, el algoritmo asimétrico debe tener la longitud de clave necesaria para proteger las claves simétricas que se envían. Por ejemplo, para proteger una clave simétrica de 128 bits, el algoritmo RSA debe emplear una clave con una longitud de al menos 2048 bits para lograr una resistencia criptográfica equivalente en general a la de la criptación de claves simétricas de 128 bits.

El algoritmo para el convenio de claves de Diffie-Hellman es un método ordinario de distribución de claves. Mediante el algoritmo Diffie-Hellman, los puntos extremos deducen de manera independiente las claves criptográficas simétricas secretas a través de una red pública. Con el proceso Diffie-Hellman, sólo se transmiten los resultados intermedios entre los puntos extremos y la clave secreta no se revela en ningún caso. Si se escoge adecuadamente el número primo, el algoritmo Diffie-Hellman hace que sea computacionalmente inviable que los atacantes deduzcan la clave secreta a partir de los resultados intermedios.

En los casos de los algoritmos RSA y Diffie-Hellman, hay que tener en cuenta, asimismo, temas como la elección de los números primos adecuados, la elección de los exponentes públicos y el manejo de las condiciones de error.

MEC 38: El intercambio de claves criptográficas se basa en claves previamente compartidas.

MEC 39: El intercambio de claves criptográficas se basa en el algoritmo asimétrico RSA con una longitud de clave de RSA determinada.

MEC 40: El intercambio de claves criptográficas se basa en el algoritmo de convenio de claves de Diffie-Hellman con un grupo determinado de números primos de Diffie-Hellman.

6.8 Informe de alarmas

Tras la detección de cualquier violación de la seguridad o ante la imposibilidad de continuar escribiendo los registros de auditoría, deben enviarse alarmas de seguridad a los administradores.

MEC 41: Mecanismos para el informe de alarmas de seguridad, como X.736.

6.9 Filtrado de paquetes

En dispositivos con conectividad basada en paquetes, debe utilizarse el filtrado de paquetes para proteger a la RCD de los ataques y evitar la pérdida de información sobre la RCD.

MEC 42: Se realiza un filtrado de paquetes en base a uno o varios de los siguientes criterios de inspección:

MEC 42a: Dirección IP de origen.

MEC 42b: Dirección IP de destino.

MEC 42c: Protocolo.

MEC 42d: Puerto de origen.

MEC 42e: Puerto de destino.

Y mediante la aplicación de una o varias de las siguientes acciones:

MEC 42f: Dejar pasar.

MEC 42g: Descartar.

MEC 42h: Modificar.

MEC 42i: Enviar.

Junto con la posibilidad de tener en cuenta las decisiones anteriores (es decir, dependiendo del estado).

Apéndice I

Mecanismos de seguridad IPSec, SSL/TLS y SSH

I.1 IPSec

IPSec aborda la seguridad en la capa IP utilizando una combinación de mecanismos criptográficos y de seguridad de protocolos. El protocolo IPSec se ejecuta entre la capa de red (capa 3) y la capa de transporte (capa 4), puede utilizarse para proteger cualquier tipo de tráfico de datos (TCP o UDP) y es independiente de las aplicaciones. El IPSec se diseñó para ofrecer seguridad compatible, de alta calidad y basada en criptografía para IPv4 e IPv6. El conjunto de servicios de seguridad que ofrece IPSec incluye:

a) Integridad de los datos.

b) Autenticación del origen de los datos con base en la dirección IP.

c) Autenticación de máquina a máquina.

d) Protección contra la reproducción.

e) Confidencialidad de los datos.

f) Intercambio de claves criptográficas.

El protocolo cumple con esos objetivos mediante la utilización de dos servicios de seguridad de tráfico: encabezamiento de autenticación (AH, *authentication header*) y cabida útil de seguridad de encapsulado (ESP, *encapsulating security payload*); y utilizando procedimientos y protocolos para la gestión de claves criptográficas. El servicio AH ofrece autenticación del origen de los datos, autenticación de máquina a máquina e integridad de datos para los paquetes IP. Gracias al servicio ESP, se obtiene el servicio de confidencialidad de los datos y la autenticación del origen de los datos, la autenticación de máquina a máquina y la integridad de los datos para los paquetes IP. Por otra parte, los mecanismos de IPSec se han diseñado para que sean independientes del algoritmo criptográfico y permitir así que puedan elegirse conjuntos diferentes de algoritmos sin que queden afectadas otras partes de la implementación.

La gestión de claves se obtiene mediante el protocolo intercambio de claves Internet (IKE, *internet key exchange*). Existen mecanismos tanto automáticos como manuales para la negociación de claves entre los puntos extremos. La negociación automática de claves puede basarse en claves previamente compartidas (por ejemplo, contraseñas) o en certificados X.509.

Referencias [RFC 2401], [RFC 2402], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 2406], [RFC 2407], [RFC 2408], [RFC 2409], [RFC 2410], [RFC 2411], [RFC 2412], [RFC 3602], [RFC 2451], [FIPS-197].

I.2 SSL/TLS

El protocolo de seguridad capa de zócalo segura (SSL, *secure socket layer*) ofrece criptación de datos, autenticación del servidor, integridad de los mensajes y autenticación facultativa del cliente en conexiones TCP/IP de la capa de transporte (capa 4). Actualmente se dispone de la revisión 3.0 de SSL y seguridad de la capa de transporte (TLS, *transport layer security*) es la versión de SSL normalizada por el IETF, que incluye mejoras en la seguridad con respecto a SSL, entre las que figuran:

- Exigencia de soporte de Diffie-Hellman y del algoritmo de firmas digitales (DSA) junto con soporte facultativo de RSA.
- Utilización del algoritmo más resistente que constituye el código de autenticación de mensaje troceado (HMAC, *hashed message authentication code*), en lugar de un algoritmo MAC no normalizado definido para SSL.

- Un algoritmo de generación de claves modificado que utiliza MD5 (compendio de mensajes 5) y SHA-1 (algoritmo de troceo seguro 1) junto con HMAC.

El protocolo SSL/TLS se ejecuta por encima de la capa de red (capa 4) y funciona únicamente con el protocolo de control de transmisión (TCP, *transport control protocol*) y no con el protocolo de datagrama de usuario (UDP, *user datagram protocol*). Entre los protocolos de capa de aplicación que normalmente se ejecutan sobre SSL/TLS figuran el protocolo de transferencia de hipertexto (HTTP, *hypertext transport protocol*), el protocolo ligero de acceso al directorio (LDAP, *lightweight directory access protocol*), y el protocolo de acceso de mensajes de Internet. Los protocolos superiores de nivel de aplicación pueden ejecutarse sobre SSL/TLS sin tomar en consideración a SSL/TLS; sin embargo, el nivel de aplicación debe vincularse a SSL/TLS mediante la utilización de solicitudes de llamado I/O.

Mediante el protocolo SSL/TLS se ofrecen tres funciones de seguridad para tráfico TCP: confidencialidad de los datos, integridad de los datos y autenticación.

En la arquitectura del protocolo de seguridad SSL/TLS hay dos capas que se ejecutan sobre TCP:

- Los protocolos de capa superior SSL/TLS.
- El protocolo de registro SSL/TLS.

Entre los protocolos de capa superior SSL/TLS figuran el protocolo de puesta en contacto de SSL/TLS, el protocolo de cambio de cifrado de SSL/TLS y el protocolo de alertas de SSL/TLS para las notificaciones. Las sesiones de SSL/TLS se crean inicialmente mediante el protocolo de puesta en contacto de SSL/TLS que ofrece:

a) Negociación de la autenticación y de los mecanismos de seguridad.

b) Autenticación del cliente y del servidor. (Utilizando las claves privadas y públicas de los clientes y servidores.)

c) El establecimiento de claves de seguridad.

Una vez iniciada la sesión SSL/TLS, el protocolo de registro de SSL/TLS se utiliza para los servicios de transporte masivo de datos. Mediante el protocolo de registro de SSL/TLS se obtiene:

a) Autenticación del origen de los datos basada en las claves del servidor.

b) Integridad de los datos.

c) Confidencialidad.

Hay que señalar que las versiones actuales de SSL y TSL son respectivamente la versión 3 (SSLv3) y la versión 1 de TSL. No se recomienda la utilización de versiones anteriores de SSL y de TLS.

Con SSL/TLS se dispone de autenticación unidireccional, mediante la cual sólo se autentica el servidor ante el cliente, o de autenticación bidireccional que permite la mutua autenticación del cliente y el servidor. La autenticación unidireccional es el método más utilizado en la Internet pública. Se recomienda la autenticación bidireccional en aplicaciones de gestión de red con el fin de permitir que las dos partes sepan que están comunicando con el punto extremo deseado.

Referencias: [RFC 2246], [RFC 3546], [SSL V3].

I.3 SSH

SSH es un protocolo de seguridad de la capa de aplicación (capa 7) frecuentemente empleado para reemplazar directamente los protocolos no seguros: Telnet y protocolo de transferencia de ficheros (FTP, *file transfer protocol*). Telnet y FTP son protocolos no seguros que transmiten contraseñas y otros datos en claro. Cabe también la posibilidad de utilizar SSH para proteger otros protocolos mediante el reenvío de puertos, motivo por el cual puede emplearse como un protocolo de seguridad de red generalizado.

Existen dos versiones de SSH: SSHv1 y SSHv2. SSHv1, que se creó en 1998, se considera hoy inseguro y obsoleto.

Las características de "Intérprete de comandos seguro 2" son las siguientes:

- Reemplaza íntegramente los protocolos Telnet, Rlogin, Rsh, Rcp y FTP, y de este modo permite unas transferencia y copia de ficheros seguras.
- Autenticación automática de usuarios (no se transmiten contraseñas en texto claro).
- Autenticación bidireccional (se autentican tanto el servidor como el cliente).
- Tunelización de aplicaciones indeterminadas TCP/IP mediante reenvío de puertos.
- Criptación de datos para velar por la confidencialidad de los datos.
- Muchas opciones de autenticación, que incluyen contraseñas, claves públicas y autenticación SecureID.
- Disponibilidad de varios conjuntos de cifrado.

La arquitectura de SSHv2 consta de los siguientes componentes básicos:

- El protocolo de la capa de transporte [SSH-TRANS] que ofrece autenticación del servidor, confidencialidad de los datos e integridad de los datos. Opcionalmente, proporciona también compresión.
- El protocolo de autenticación de usuario [SSH-USERAUTH] mediante el cual se autentica ante el servidor al usuario del lado cliente.
- El protocolo de conexión [SSH-CONNECT] que multiplexa el túnel criptado en varios canales lógicos.

Mediante el protocolo de conexión se obtienen canales que pueden utilizarse para diversos propósitos. Existen métodos normalizados para establecer sesiones interactivas seguras del intérprete de comandos y para reenviar ("tunelizar") conexiones y puertos indeterminados TCP/IP.

El número de puerto 22 se registró ante la IANA como el puerto normalizado para aplicaciones SSHv2.

Referencias: [SSH-ARCH], [SSH-TRANS], [SSH-USERAUTH], [SSH-CONNECT].

Apéndice II

En este apéndice se describe un mecanismo de filtrado de paquetes con el fin de mejorar la seguridad de la red de comunicación de datos (RCD). La red de comunicación de datos (RCD) es la red que se utiliza para conectar las aplicaciones de gestión (normalmente ubicadas en el centro de operaciones de la red) con los elementos de red destinados a centralizar el servicio de aprovisionamiento, supervisión de alarmas, pruebas, facturación y otras actividades de gestión de la red. En las secciones 2.8–2.10 de RFC 3871 se consigna un conjunto de requisitos para el filtrado de paquetes en las grandes infraestructuras de red IP de los proveedores de servicio de Internet. La presente contribución se inspira en la RFC 3871 para definir recomendaciones de filtrado respecto a la RCD.

El filtrado de paquetes es el proceso mediante el cual se determina el destino de cada paquete que atraviesa un elemento de red, basándose en los correspondientes criterios especificados[9]. Puede

[9] La descripción del filtrado de paquetes es muy parecida a la del encaminamiento de paquetes. Sin embargo, el presente apéndice se centra en el filtrado de paquetes y no se aborda el encaminamiento de paquetes.

haber varias disposiciones; entre otras, dejar pasar, descartar, reenviar (dirigiéndolo a otra parte), etc. El filtrado de paquetes es el mecanismo de protección básico que determina el tráfico que ingresa al elemento de red o sistema de gestión de que se trate o que lo atraviesa.

El principal problema consiste en filtrar el tráfico proveniente de otras redes (por ejemplo de redes que transportan tráfico de los clientes o redes pares de gestión) y que ingresa a la RCD. Puede ser necesario, además, aislar algunos de los elementos de la RCD, por lo que podría utilizarse el filtrado entre diferentes subredes (o dominios) de la RCD.

II.1 Objetivos

Los objetivos globales del mecanismo de filtrado de paquetes son:

1) Proteger la infraestructura de la RCD del tráfico del cliente. En la protección debe tenerse en cuenta la compartición adecuada de recursos comunes con el fin de evitar la degradación o la denegación del servicio.

2) Proteger la infraestructura de la RCD de las redes de pares.

3) Evitar que se propague a través de la infraestructura de la RCD el tráfico de la RCD que no cumpla con la política de seguridad del caso.

II.2 Consideraciones en torno al diseño de la red que afectan el filtrado de paquetes

En este apéndice no se implican requisitos para el diseño de la RCD. Ahora bien, el diseño y la puesta en funcionamiento de la RCD afectará los requisitos y puesta en servicio del filtrado de paquetes en la red. En la figura II.1 puede verse el diseño de una RCD típica.

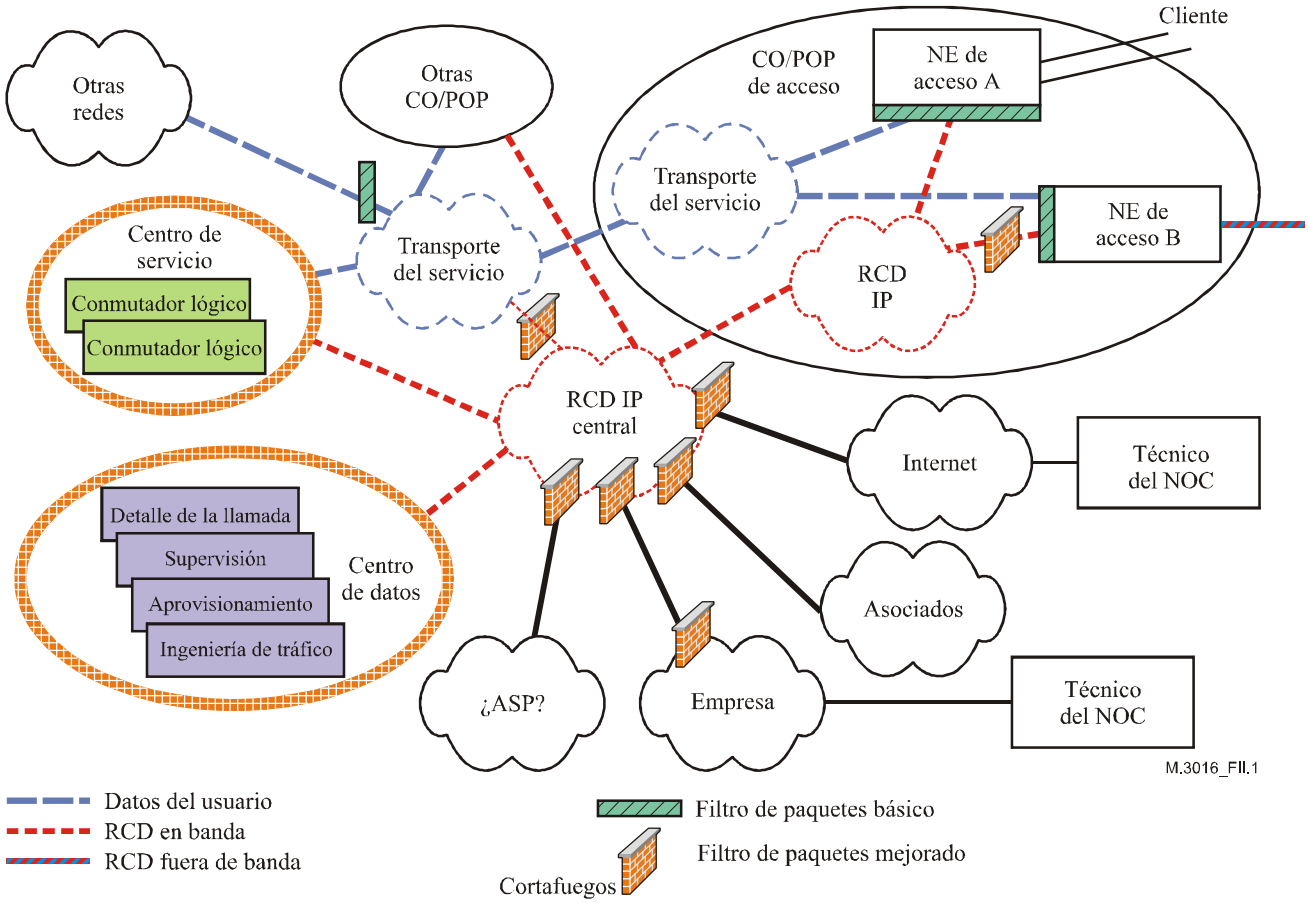

Figura II.1/M.3016.3 – Ilustración de una RCD genérica

Por lo general se distinguen tres tipos de diseño de RCD:

- De gestión en banda: esta RCD utiliza ancho de banda reservado de la red de servicio para transportar los datos del cliente. Así, por ejemplo, puede dedicarse una VLAN en un enlace de Ethernet a la gestión del tráfico o podría utilizarse una conexión de IPSec o de SSH para conectarse a través de Internet (por ejemplo, el técnico de la NOC en la figura II.1 podría conectarse por Internet).
- De gestión fuera de banda: la RCD es una red completamente diferente de la red de servicio que transporta el tráfico de los clientes. Esta red puede superponerse sobre la red física que también transporta tráfico de datos del usuario.
- Híbrida: combina los enfoques en banda y fuera de banda.

  Aunque en esta Recomendación no se realizan comparaciones ni un examen general con respecto a este tipo de arquitecturas de gestión (véase la sección 2.2 de RFC 3871), la selección de la arquitectura afectará los requisitos de filtrado.

La lógica utilizada para crear las RCD dependerá del tipo de elementos de red que se desea soportar, de los procedimientos y preferencias de explotación, de las topologías de red, de los aspectos financieros, etc. En cada diseño se habrá de tener en cuenta la capacidad de la red, la flexibilidad y la seguridad.

Las ofertas de servicio de gestión de próxima generación se implementarán utilizando equipos de transporte basados en paquetes (por ejemplo, retransmisión de tramas, ATM, IP, MPLS, Ethernet). El advenimiento de este tipo de servicios obliga a gestionar el equipo de acceso (CPE).

Podría ser necesario utilizar un modelo híbrido con gestión fuera de banda hacia los puntos de presencia (POP, *points of presence*) y gestión en banda entre el POP y los dispositivos de acceso CPE, ya que podría ser inviable desde el punto de vista financiero gestionar fuera de banda hasta el dispositivo de acceso CPE. El NE de acceso B de la figura II.1 es un ejemplo sobre el particular. En este caso, cabe la posibilidad de recurrir a filtrado mejorado (por ejemplo un cortafuegos) para proteger la RCD del CPE. Otros ejemplos de la utilización de una conexión en banda son la gestión de un POP remoto y aislado, donde sea inviable instalar una red independiente, y la utilización de la red de servicio como respaldo de la RCD.

Por otra parte, el recurso al filtrado de paquetes supone que el espacio de direcciones utilizado por la RCD es independiente del asignado a los clientes y que no hay necesidad de flujo de tráfico entre estos dos dominios. La separación de espacios de direcciones simplifica el diseño de filtros de paquetes para bloquear el tráfico del cliente y así evitar que éste acceda a los recursos de gestión. El método más sencillo consiste en bloquear todo el tráfico destinado hacia la RCD que se origina fuera de la RCD, para proteger la infraestructura de gestión del tráfico del cliente. No obstante, a veces podría resultar necesario intercambiar tráfico entre las redes externas y la RCD; por ejemplo, cuando dos proveedores de servicio intercambian información de gestión (éste el caso cuando el DCC se encuentra en un punto intermedio entre dos SP).

En consecuencia, habrá que permitir el flujo restringido de tráfico entre dominios y prever un mayor control (por ejemplo, mediante el filtrado de paquetes mejorado) si se desea que la RCD cuente con la seguridad adecuada.

En la figura II.1 puede verse un diseño de RCD que tiene en cuenta los supuestos mencionados. El transporte de servicio (en azul) lleva el tráfico del cliente. La RCD (en rojo) lleva el tráfico de gestión. En el centro de servicio se encuentran los servidores, etc., que suministran servicios a los clientes y a los que éstos tienen acceso (por ejemplo, los conmutadores lógicos). En el centro de datos hay servidores y otros sistemas de explotación que se utilizan para gestionar y supervisar la red y a los que los clientes no tienen acceso directo. La conexión de la RCD a los elementos de red puede utilizar IP, X.25, asíncrono o CLNS de ISO.

El filtrado de paquetes de ingreso en la periferia de una red RCD o del servicio de red es un requisito básico de seguridad de la RCD en el NE de acceso. Ahora bien, este filtrado de paquetes básico puede ser insuficiente ya que es posible que se produzcan ataques provenientes de NE o equipos dentro de la RCD cuya seguridad se haya visto comprometida. Así pues, habrá que desplegar estratégicamente mecanismos de filtrado de paquetes en diversos puntos de la RCD con el fin de garantizar que se aplique la correspondiente política de seguridad. También puede ser necesario el filtrado de paquetes mejorado en los puntos donde la RCD se conecta con las redes externas (por ejemplo, Internet, la red empresarial del SP, los asociados, etc.).

El filtrado de paquetes es uno de los componentes de la estrategia de seguridad de la red, pero debe ser utilizado en el contexto de los principios y estrategias de seguridad global de la red, entre los que cabe citar la compartimentación y la defensa de controles complementarios. A pesar de que una buena estrategia de seguridad debe incluir requisitos de seguridad en los equipos mismos (por ejemplo, en los conmutadores lógicos) y compartimentación de la red, estos conceptos no se abordan en la presente Recomendación.

Con el fin de proteger la infraestructura de gestión y la RCD en general, conviene que el operador de la red descarte ciertos paquetes recibidos del exterior del perímetro de la RCD (es decir, de pares y de clientes). Por ejemplo, no se debe permitir que dentro del perímetro de la RCD haya paquetes con direcciones IP de origen no válidas ni paquetes dirigidos a direcciones IP utilizadas exclusivamente en la RCD. Esta función se denomina filtrado de ingreso. Estos requisitos derivan de [RFC 3871] y [RFC 2827].

Hay dos categorías para el filtrado de paquetes:

- El filtrado de paquetes básico, que utiliza la información del encabezamiento del paquete, y que incluye la capacidad de detectar y bloquear paquetes con direcciones de origen falsas.
- El filtrado de paquetes mejorado, que incluye:
  - El examen de los paquetes basado en el estado, en cuyo marco el contexto o la información del estado se utiliza también para la toma de decisiones de filtrado.
  - El filtrado dinámico de protocolos específicos en el que se abren dinámicamente los filtros dependiendo de la información que se transporta en la cabida útil del protocolo.
  - El examen detallado de los paquetes, en cuyo marco se analizan los protocolos de nivel de aplicación con el fin de detectar anomalías del protocolo o contenidos sospechosos o fuera de lo común.

II.3 Filtrado básico de paquetes

Los equipos que se conectan a la RCD deben estar en condiciones de descartar paquetes recibidos de interfaces que se conecten con el exterior (por ejemplo, con clientes y pares) y que contengan direcciones IP de origen no válidas. Las direcciones IP de origen no válidas pueden ser:

- Direcciones Bogon (véase la sección 1.8 de RFC 3871).
- Marcianas (véase la sección 1.8 de RFC 3871).
- Direcciones IP que no han sido asignadas al cliente (o que no es válido que las envíe un par).

El mecanismo de filtrado de paquetes debe estar en condiciones de filtrar tráfico dirigido a todos los bloques de direcciones adjudicados a la RCD y originados en el exterior (por ejemplo en los clientes), basándose en los atributos especificados en MEC 42.

El mecanismo de filtrado de paquetes debe ser capaz de llevar estadísticas precisas de tráfico para cada interfaz. El nivel de detalle de las estadísticas puede variar dependiendo del mecanismo de filtrado de paquetes.

El equipamiento debe estar en condiciones de filtrar tráfico proveniente del exterior de la RCD (por ejemplo, de los clientes) y dirigido directamente a un elemento de red a través de una de sus interfaces, incluidas las interfaces de bucle, basándose en los atributos especificados en MEC 42.

El mecanismo de filtrado de paquetes podría soportar el concepto de múltiples dominios de seguridad del modelo de la RGT, en el que todos los elementos de un mismo dominio de seguridad deben ser conformes con políticas de seguridad comunes.

El equipo puede tener la capacidad de generar las alarmas apropiadas basándose en el tráfico, las excepciones y las condiciones de funcionamiento.

II.4 Filtrado de paquetes mejorado

Habrá que tener en cuenta estas recomendaciones cuando el tráfico de usuario y de gestión se superpongan en gran medida, es decir, cuando el tráfico del usuario y el de gestión no se separan sólo en el borde de la red y donde la RCD se conecte directamente a otras redes. Estas capacidades de filtrado deben ser utilizadas en las fronteras de subredes desprotegidas (por ejemplo, entre la RCD y el centro de datos).

El mecanismo ha de examinar protocolos de aplicación utilizados en la RCD con el fin de detectar cualquier anomalía o comportamiento anormal del protocolo y a continuación bloquear este tipo de tráfico.

El mecanismo debe examinar el contenido del tráfico de la RCD para detectar contenidos maliciosos como virus, gusanos, troyanos, etc., si así se considera oportuno.

El mecanismo debe ofrecer protección contra los ataques pertinentes de denegación de servicio (DoS, *denial of service*).

El mecanismo debe estar en condiciones de filtrar de acuerdo con el estado, esto es, debe utilizar la información de la sesión para el filtrado de paquetes. En todo momento habrá que permitir el paso del tráfico de respuesta.

El mecanismo debe estar en condiciones de soportar la capacidad del microorificio dinámico para todos los protocolos utilizados en la red que transporten la dirección de los puertos en su carga útil, como por ejemplo, FTP, SIP, etc. El mecanismo de filtrado de paquetes debe examinar la información del puerto en cabida útil y abrir la comunicación a través del puerto especificado (microorificio dinámico) durante toda la sesión. Habrá que contar con un mecanismo de temporización adecuado que cierre el puerto, si la sesión termina de manera abrupta.

El mecanismo debe soportar la aplicación del protocolo, incluyendo el descarte de paquetes deformes, el establecimiento inadecuado de la sesión, etc.

En las secciones 2.7–2.10 de RFC 3871 se exponen otras capacidades recomendadas de filtrado.

BIBLIOGRAFÍA

[RFC 2827] IETF RFC 2827 (2000), *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*.

[RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*, http://www.ietf.org/rfc/rfc2401.txt?number=2401

[RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*.

[RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[NDS/IP] 3GPP TS 33.210 (2001), *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security*.

[RFC 2402] IETF RFC 2402 (1998), *IP Authentication Header*, http://www.ietf.org/rfc/rfc2402.txt?number=2402

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2403.txt?number=2403

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*, http://www.ietf.org/rfc/rfc2404.txt?number=2404

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm with Explicit IV*, http://www.ietf.org/rfc/rfc2405.txt?number=2405

[RFC 2406] IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)*, http://www.ietf.org/rfc/rfc2406.txt?number=2406

[RFC 2407] IETF RFC 2407 (1998), *The Internet IP Security Domain of Interpretation for ISAKMP*, http://www.ietf.org/rfc/rfc2407.txt?number=2407

[RFC 2408] IETF RFC 2408 (1998), *Internet Security Association and Key Management Protocol (ISAKMP)*, http://www.ietf.org/rfc/rfc2408.txt?number=2408

[RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*, http://www.ietf.org/rfc/rfc2409.txt?number=2409

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use with IPsec*, http://www.ietf.org/rfc/rfc2410.txt?number=2410

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

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*, http://www.ietf.org/rfc/rfc2412.txt?number=2412

[RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-aes-cbc-04.txt

[RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*, http://www.ietf.org/rfc/rfc2451.txt

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol, Version 1.0*, ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

[RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*, ftp://ftp.rfc-editor.org/in-notes/rfc3546.txt

[SSL V3] *Secure Socket Layer Version 3.0 Specification*, Netscape Communications. http://wp.netscape.com/eng/ssl3/

[SSH-ARCH] YLONEN (T.): *SSH Protocol Architecture*, I-D draft-ietf-architecture-15.txt, octubre de 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-15.txt

[SSH-TRANS] YLONEN (T.): *SSH Transport Layer Protocol*, I-D draft-ietf-transport-17.txt, octubre de 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-17.txt

[SSH-USERAUTH] YLONEN (T.): *SSH Authentication Protocol*, I-D draft-ietf-userauth-18.txt, septiembre de 2002. http://www.ietf.org/internet-drafts/draft-ietf-secsh-userauth-18.txt

[SSH-CONNECT] YLONEN (T.): *SSH Connection Protocol*, I-D draft-ietf-connect-18.txt, octubre de 2003. http://www.ietf.org/internet-drafts/draft-ietf-secsh-connect-18.txt

[FIPS-46-3] Data Encryption Standard. (Describes both DES and 3DES). http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-197] Advanced Encryption Standard (AES), FIPS Publication 197, National Institute of Standards and Technology, noviembre de 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[RFC 2437] IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*, http://www.ietf.org/rfc/rfc2437.txt?number=2437

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 multimedios
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	**Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes**
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie 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, 2005