Unión Internacional de Telecomunicaciones

UIT-T M.3016.1

(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: Requisitos de seguridad

Recomendación UIT-T M.3016.1

UIT-T

ITU 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.3016.1

Seguridad en el plano de gestión: Requisitos de seguridad

Resumen

Esta Recomendación, en la que se determinan los requisitos 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.3016.1 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.

© UIT 2005

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

ÍNDICE

Introducción

La infraestructura de las telecomunicaciones es crucial para las comunicaciones y la economía mundial. 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 requisitos de seguridad mediante los cuales los proveedores, organismos y proveedores de servicio podrán implementar una infraestructura segura de gestión de las telecomunicaciones. Aunque el conjunto de requisitos 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 requisitos para responder a sus necesidades concretas aparte de los ya indicados en la presente Recomendación.

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

– Rec. UIT-T M.3016.0 – Seguridad en el plano de gestión: Perspectiva general
– Rec. UIT-T M.3016.1 – Seguridad en el plano de gestión: Requisitos de seguridad
– Rec. UIT-T M.3016.2 – Seguridad en el plano de gestión: Servicios de seguridad
– Rec. UIT-T M.3016.3 – Seguridad en el plano de gestión: Mecanismo de seguridad
– Rec. UIT-T M.3016.4 – Seguridad en el plano de gestión: Formulario del perfil de seguridad

Recomendación UIT-T M.3016.1

Seguridad en el plano de gestión: Requisitos de seguridad

1 Alcance

En las Recs. UIT-T M.3016.1 a M.3016.3 se especifica un conjunto de requisitos, servicios y mecanismos para lograr la seguridad de 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 requisitos 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 requisitos 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 aplicar sus políticas de seguridad.

1.1 Finalidad

En la Rec. UIT-T M.3016.0 se determinan diversos objetivos que permitirán asegurar la red de gestión y determinar también las amenazas que ponen en peligro el cumplimiento de dichos objetivos. Esta Recomendación deduce los requisitos a partir de los objetivos contra las amenazas planteadas e identifica los servicios de seguridad que podrán contrarrestarlas. Al definir los servicios, se utilizan mecanismos basados en algunos algoritmos. El resto de las Recomendaciones de esta serie aprovechan esta estructura indicada en la perspectiva general de la Rec. UIT-T M.3016.0. Ésta aumenta las diversas etapas necesarias para asegurar el plano de gestión.

1.2 Relación con la arquitectura de seguridad X.805

En la Rec. UIT-T X.805 se define la arquitectura necesaria para proporcionar seguridad de red extremo a extremo. Esta arquitectura divide lógicamente un conjunto complejo de prestaciones relacionadas con la seguridad de red extremo a extremo en tres componentes arquitecturales independientes, denominados dimensiones de seguridad, capas de seguridad y planos de seguridad (véase la figura 2/X.805). Una dimensión de seguridad es un conjunto de medidas de seguridad concebidas para abordar un aspecto particular de la seguridad de la red. En la Rec. UIT-T X.805 se definen tres capas de seguridad: la de infraestructura, la de servicios y la de aplicaciones, las cuales se aprovechan entre sí para proporcionar soluciones basadas en la red. Un plano de seguridad es un determinado tipo de actividad de red protegida por las dimensiones de seguridad. En la Rec. UIT-T X.805 pueden identificarse tres planos de seguridad, concretamente: de gestión, de control y de usuario de extremo. Para ofrecer una solución completa, deberían aplicarse medidas de seguridad (por ejemplo, de control de acceso, de autenticación) a cada tipo de actividad de red (es decir, actividad del plano de gestión, del plano de control y del plano de usuario de extremo) en relación con la infraestructura, los servicios y las aplicaciones. Esta Recomendación se centra específicamente en el aspecto de seguridad en el plano de gestión de los elementos de red (NE) y los sistemas de gestión (MS), los cuales forman parte de la infraestructura de la red.

1.3 Relación con los requisitos de seguridad de las redes de telecomunicaciones E.408

En la Rec. UIT-T E.408 se presentan una síntesis de los requisitos de seguridad y un marco que identifica las amenazas a la seguridad de las redes de telecomunicaciones en general (fijas y móviles; voz y datos) y se dan orientaciones para planificar las contramedidas que se pueden prever para disminuir los riesgos provocados por las amenazas. Esta Recomendación es de carácter genérico y no determina ni aborda los requisitos de redes específicas. La serie M.3016.x identifica los requisitos, servicios y mecanismos de seguridad para la red de telecomunicaciones, es decir, el plano de gestión en general en la gestión de las telecomunicaciones.

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 E.408 (2004), *Requisitos de seguridad para las redes de telecomunicaciones*.

– 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.3013 (2000), *Consideraciones sobre 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 del perfil de seguridad*.

– Recomendación UIT-T X.509 (2000), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marco para certificados de claves públicas y atributos,* más corrigendum técnico 1 (2001), corrigendem técnico 2 (2002) y corrigendum técnico 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), *servicios y mecanismos de seguridad de capa 2 de las redes de área local*.

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

– IETF RFC 1750 (1994), *Randomness Recommendations for Security*.

3 Términos y definiciones

En esta Recomendación se utilizan los siguientes términos de la Rec. UIT-T G.8080/Y.1304:

– plano de control;

– plano de gestión;

– plano de transporte.

En esta Recomendación se utilizan los siguientes términos de la Rec. UIT-T M.3010:

– sistema de gestión;

– elemento de red.

En esta Recomendación se utiliza el siguiente término de la Rec. UIT-T M.3013:

– sistema de gestión de elementos.

En esta Recomendación se utiliza el siguiente término de la Rec. UIT-T X.509:

– autenticación fuerte.

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

– control de acceso;

– autenticación.

En esta Recomendación se define el término siguiente.

3.1 medidas cruciales de administración de la seguridad, que incluyen aunque no sean las únicas:

a) definir y asignar privilegios de usuario;

b) añadir y suprimir identificadores (ID) de usuario;

c) inhabilitar la utilización de ID de usuario específicos como ID de acceso;

d) inicializar y reactivar contraseñas de acceso;

e) inicializar y modificar claves criptográficas;

f) establecer el umbral de prescripción del sistema relativo a las contraseñas de acceso;

g) establecer el límite del sistema en cuanto al número de intentos de acceso fallidos por cada ID de acceso;

h) suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema;

i) fijar el valor del temporizador de inactividad del sistema;

j) establecer el registro de seguridad del sistema y la configuración de las alarmas;

k) gestionar los procesos de registro de seguridad;

l) mejorar la versión del soporte lógico de seguridad;

m) terminar cualquier sesión de usuario o de sistema.

4 Abreviaturas, siglas o acrónimos

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

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

ACS Servidor de control de acceso (*access control server*)

ALE Pérdida anualizada prevista (*annualized loss expectancy*)

ANSI Instituto Nacional de Normas de los Estados Unidos (*American National Standards Institute*)

CO Central (*central office*)

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

CSI Interoperabilidad segura común (*common secure interoperability*)

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*)

HAZMAT Materiales peligrosos (*hazardous materials*)

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*)

LAES Supervisión electrónica autorizada legalmente (*lawfully authorized electronic surveillance*)

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 (*NE or MS*)

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

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

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

OASIS Organización para la promoción de normas de información estructurada (*organization for the advancement of structured information standards*)

OEM Vendedor de equipo original (*original equipment manufacturer*)

ORB Mediador de petición de objetos (*object request broker*)

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 etiquetado de enunciados de seguridad (*security assertion markup language*)

---

[1] Por lo general, OSS puede emplearse en el mismo contexto de los MS en cualquier capa de la jerarquía de la red de gestión de las telecomunicaciones.

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

SOAP Protocolo simple de acceso a objetos (*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 capa de transporte (*transport layer security*)

UIT-T Unión Internacional de Telecomunicaciones – Sector de Telecomunicaciones

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

5 Convenios

En las Recs. UIT-T M.3016.1 a M.3016.3 se emplea un descriptor para identificar los diferentes requisitos, servicios y mecanismos, que consiste en una de las siguientes etiquetas de tres letras seguida de un número:

– REQ para requisito;
– SER para servicio;
– MEC para mecanismo.

6 Requisitos de seguridad

Esta cláusula contiene los requisitos de seguridad relativos a las operaciones, administración, mantenimiento y aprovisionamiento (OAM&P) y el sistema de soporte de operaciones (OSS) del **plano de gestión**.

En la figura 1 de M.3016.0 se describen las relaciones entre objetivos de seguridad, amenazas, riesgos, requisitos de seguridad y servicios. También se describe el proceso en que pueden obtenerse los "requisitos de seguridad" a partir de las "amenazas" y los "objetivos de seguridad" que, a su vez, se deducen de un conjunto de servicios de seguridad. Estos "servicios", que sirven para contrarrestar las amenazas, harán uso de "mecanismos" que a su vez utilizan "algoritmos de seguridad". En el cuadro 1 (que corresponde al cuadro 4/M.3106.0) se presenta la relación entre requisitos de seguridad y servicios de seguridad. Los requisitos de seguridad que se describen en esta cláusula están organizados siguiendo el cuadro 1, de la siguiente manera:

– verificación de identidades;
– acceso controlado y autorización;
– protección de la confidencialidad;
– protección de la integridad de los datos;
– imputabilidad;
– registro y auditoría de seguridad;
– notificación de alarmas de seguridad.

NOTA – La recuperación a partir de una violación de seguridad es una esfera queda en estudio.

Cuadro 1/M.3016.1 – Correspondencia entre requisitos de seguridad y servicios de seguridad (cuadro 4/M.3016.0)

Requisito funcional	Servicio de seguridad
Verificación de identidades	Autenticación de 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 alarmas de seguridad	Alarma de seguridad
Auditoría de seguridad	Registro de auditoría

6.1 Verificación de identidades

La **autenticación** tiene dos finalidades en cuanto a la seguridad en el **plano de gestión**:

1) asegura la identidad de las partes que intervienen en la comunicación, proporcionando la base para establecer comunicaciones privadas con plena integridad y confidencialidad de los datos entre dos sistemas; y

2) proporciona un mecanismo básico para acceder mediante una clave a un sistema de gestión y/o auditar las actividades de gestión en cualquier sistema.

6.1.1 Autenticación de usuario, contraseñas e identificadores de usuario

La **autenticación** del usuario tiene por objeto la **autenticación** de los clientes que participan en la gestión de la red. En este caso, la **autenticación** verifica la identidad del usuario legítimo e impide ataques sinuosos de usuarios ilegítimos. Con una **autenticación** apropiada se pueden rastrear las actividades y circunscribir a los usuarios a actividades o funciones autorizadas previamente, como se indica en 6.3.

Los requisitos mínimos de la **autenticación** consisten en la utilización de un ID de usuario y de una **contraseña compleja** estática. Pueden emplearse otros mecanismos siempre que los administradores de NE/MS confíen en que el nivel de seguridad es por lo menos tan estricto como el que proporcionan un ID de usuario y una **contraseña compleja** estática. Entre otros mecanismos que podrían considerarse se incluyen:

– ID de usuario y **autenticación de dos factores** aplicando un generador de contraseñas de un solo uso,[2] y

– **Autenticación de dos factores** mediante una tarjeta inteligente con almacenamiento de la información relativa a la identidad protegida.

---

[2] Esta cláusula no trata de las contraseñas dinámicas ya que se consideran fuera del alcance de la presente Recomendación.

REQ 1: Para efectos de acceso a los NE/MS, registro y auditoría, debería soportarse la autenticación fuerte.

REQ 1 representa el requisito de seguridad. En la Rec. UIT-T M.3016.3 se presenta la descripción del mecanismo de autenticación general. Se prevé que las técnicas de **autenticación** y las tecnologías de contraseña única seguirán mejorando.

Cuando se utiliza seguridad de contraseña única, el protocolo sigue impugnando a la entidad o entidades en cuanto a la información relativa a su identidad; sin embargo, puede ser que un usuario no tenga necesidad de entregar este tipo de información ya que puede estar almacenada en una memoria asociada (caché) y en cierto modo segura (por ejemplo, Kerberos).

Los siguientes requisitos resultan útiles para mantener la complejidad de la contraseña y a efectos de auditoría y registro.

REQ 2: Todo NE/MS debería exigir el cumplimiento de la **Autenticación** conforme a la política de la organización.

REQ 3: Todo NE/MS debería soportar las reglas de complejidad mínimas establecidas para la **autenticación** conforme a la política de la organización.

REQ 4: El NE/MS debería impedir que otro usuario pueda modificar una contraseña de acceso de un usuario sin su consentimiento.

REQ 5: Cada NE/MS debería garantizar automáticamente que cada nueva contraseña de acceso sea diferente de la contraseña anterior. El grado de diferencia debería ser configurable conforme a la política de la organización.

Como las contraseñas son almacenadas por lo general a través de criptación unidireccional, se exige también la introducción de la antigua contraseña a fin de que el NE/MS pueda determinar el grado de diferencia existente entre las dos contraseñas.

REQ 6: Todo NE/MS debería soportar la prevención de la reutilización de contraseñas. Los parámetros correspondientes deberían ser configurables conforme a la política de la organización.

REQ 7: Todo ID de usuario debería poder fijar sus propias contraseñas de acceso.

REQ 8: El usuario debería poder modificar sus contraseñas a su conveniencia, respetando un intervalo mínimo a partir de la última modificación. El intervalo mínimo debe ser configurable conforme a la política de la organización y fijarse a través del **administrador de seguridad del sistema**.

REQ 9: Todo NE/MS debería soportar el control de contraseñas en multiniveles. Algunos usuarios podrán quedar bloqueados (por ejemplo, debido a la prescripción de la contraseña o a algún fallo de la clave de acceso) mientras que a otros no les sucederá lo mismo.

6.1.2 Autenticación mediante contraseñas por defecto

La utilización apropiada de contraseñas por defecto se ha discutido extensamente en las publicaciones sobre seguridad. Históricamente, estas contraseñas han ido de las codificadas en el soporte físico del programa a las contraseñas por defecto asociadas con cada versión o actualización del soporte lógico. A continuación, se señalan los siguientes requisitos de la **autenticación** mediante contraseñas por defecto.

REQ 10: Debería aplicarse uno de los siguientes:

- El soporte lógico de configuración debería crear una contraseña de inicialización única por cada aplicación en la nueva versión o actualización[3] del soporte lógico.
- Si se utiliza una contraseña por defecto, el sistema debería exigir su sustitución por una contraseña única antes de que el dispositivo se ponga en servicio.
- Si un dispositivo es entregado sin una contraseña o una contraseña nula, debería asignarse una contraseña única durante el proceso de instalación antes de que el dispositivo se ponga en servicio.

REQ 11: El umbral de prescripción del sistema en cuanto a las contraseñas de acceso debería ser configurable si la funcionalidad está integrada también en la aplicación. Cuando se alcanza el umbral de prescripción la contraseña de acceso a una aplicación afectada debería ser reactivada al estado por defecto original definido en REQ 10. Todos los privilegios de modificación de contraseñas deberían ser revocados a todos los usuarios excepto para el papel de usuario, el cual tiene el nivel más alto de autoridad de seguridad para un sistema o una aplicación dados.

REQ 12: El valor del temporizador de inactividad del sistema debería ser configurable si la funcionalidad también está integrada en la aplicación. Cuando dicho temporizador esté habilitado, debería impedirse el acceso de un determinado ID de usuario al sistema y el proceso de acceso al sistema de este usuario debería inhabilitarse.

REQ 13: El límite del sistema por lo que se refiere a los intentos consecutivos fallidos de acceso al sistema de un determinado ID de usuario debería ser configurable si la funcionalidad también está integrada en la aplicación. Cuando se alcanza dicho límite para un determinado ID de usuario, deberá invocarse el temporizador de inactividad del sistema definido en REQ 12.

6.2 Acceso controlado y autorización

Todo NE/MS debe soportar el concepto de "privilegio mínimo" (es decir, una persona contará con un determinado papel y autorización para visualizar datos, modificar datos o iniciar **acciones de gestión** únicamente para aquellas funciones autorizadas para ese papel). Esta cláusula define los requisitos básicos para aplicar el "privilegio mínimo" a través de un buen sistema de administración de seguridad.

6.2.1 Administración de seguridad

Todo NE/MS debe velar por que únicamente los usuarios autorizados tengan permiso para gestionar recursos de seguridad del sistema. Todas las medidas administrativas están relacionadas con papeles de usuario que están asignados a individuos específicos. No obstante, sólo se examinan algunos tipos de papeles de usuario, aunque pueden existir muchos otros con distintos grados de privilegios, especialmente con respecto a **medidas de gestión** de seguridad cruciales. El objetivo es garantizar que únicamente usuarios autorizados y con privilegios puedan gestionar recursos de seguridad cruciales.

REQ 14: Todo NE/MS debería estar en condiciones de soportar múltiples tipos de papeles de usuario definidos por el usuario, y las **medidas de gestión** deberían poder asignarse a cada papel de usuario.

Los papeles de usuario podrían dar por resultado una jerarquía de papeles de manera que cada uno de ellos tenga diferentes o menos tareas asignadas lo que se traduce en menor autoridad con relación al papel de usuario con más privilegios. Un ejemplo de ese tipo de jerarquía es aquel en el

---

[3] Esta situación es similar a la práctica en la que cada disco compacto adquirido comercialmente dispone de una contraseña habilitadora única.

que el papel de usuario permite realizar **medidas de gestión**, lo que resulta similar a un "super usuario" de un ordenador. Otro papel de usuario soporta únicamente el acceso en la modalidad de sólo lectura para poder desempeñar funciones de supervisión de los dispositivos, como ocurre cuando se trata de un operador.

REQ 15: Todo NE/MS debería soportar un tipo de usuario por defecto, que pueda desempeñar **medidas de gestión** mínimas o restringidas.

REQ 16: Todo NE/MS debería soportar las siguientes **medidas de administración de seguridad cruciales**, aunque no sean las únicas:

- Definir y asignar privilegios de usuario y de grupo.
- Conservar un registro de todas las peticiones de ID de acceso al sistema.
- Añadir y suprimir ID de usuario.
- Inhabilitar y habilitar la utilización de ID de usuario específicos como ID de acceso.
- Inicializar y reactivar contraseñas de acceso al sistema.
- Inicializar y modificar claves criptográficas.
- Establecer el umbral de prescripción del sistema en cuanto a las contraseñas de acceso.
- Establecer el límite del sistema con relación al número de intentos de acceso fallidos por cada ID de acceso.
- Suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema.
- Fijar el valor del temporizador de inactividad del sistema.
- Establecer el procedimiento de registro de las actividades de seguridad del sistema y la configuración de alarmas.
- Supervisar todos los registros de seguridad del sistema.
- Gestionar los procesos de registro de las actividades de seguridad del sistema.
- Actualizar el soporte lógico de seguridad.
- Terminar cualquier sesión de usuario o de sistema.
- Delegar autorizaciones de seguridad a personas especificas con otras funciones.
- Fijar reglas complejas para las contraseñas.

REQ 17: Todo NE/MS debería soportar las siguientes **medidas de gestión** de seguridad de aplicación, aunque no sean las únicas:

- Definir y asignar nuevos privilegios de usuario y de grupo al nivel de aplicación.
- Conservar un registro de todas las peticiones de ID de acceso a la aplicación.
- Añadir y suprimir usuarios en el nivel de aplicación.
- Supervisar todos los registros de seguridad de la aplicación.
- Configurar los registros de las actividades de seguridad de la aplicación y las alarmas.
- Gestionar los procesos de registro de las actividades de seguridad de la aplicación.
- Terminar la sesión de aplicación de usuario.

6.2.2 Utilización y funcionamiento del NE/MS

Los requisitos consignados en esta cláusula pueden aplicarse tanto al acceso a distancia como a través de una consola al NE/MS. Estos requisitos obligatorios representan una base para el NE/MS que es el que se encarga en realidad de almacenar los ID y las contraseñas de usuario. Muchos

NE/MS hacen referencia a un sistema de control de acceso (ACS, *access control system)* centralizado para efectos de almacenar los ID y las contraseñas de usuario. Los requisitos obligatorios expresados en esta Recomendación pueden aplicarse a un NE/MS si éste mantiene los ID y las contraseñas de usuario almacenados en el ACS.

REQ 18: El NE/MS debería sincronizar el tiempo de una manera autenticada (por ejemplo, versión 3 de NTP).

REQ 19: Para un NE/MS, cada **medida de gestión** debería estar asociada con una única SESIÓN autorizada.

REQ 20: Toda SESIÓN debería establecerse a través de una **autenticación** apropiada, según se describe con detalle en el requisito REQ 1.

REQ 21: Las comunicaciones entre un NE/MS y un ACS necesarias con el fin de transportar la información de **autenticación** deberían tener lugar a través de un **trayecto de confianza**.

REQ 22: El NE/MS debería utilizar **control de acceso** y particiones para autorizar, negar o, por el contrario, controlar un usuario, grupo de usuarios o el acceso de un sistema distante al NE/MS y debería disponer de la funcionalidad necesaria para restringir el acceso de los usuarios a los datos, transacciones y equipos necesarios para que puedan cumplir con sus papeles. Los permisos de acceso deberían incluir, aunque no sean los únicos, sólo lectura y lectura-escritura.

6.2.3 Proceso de acceso al sistema

REQ 23: El NE/MS debería soportar la capacidad para asignar a cada individuo un ID de usuario único para acceder a una aplicación o a un sistema de cómputo.

REQ 24: El NE/MS debería disponer, en su caso, de la capacidad para obligar automáticamente al usuario a modificar su contraseña durante el primer acceso, después de que se haya establecido la cuenta, y durante el primer acceso una vez reactivada la contraseña.

NOTA – El siguiente requisito (REQ 25) exige hacer una distinción, ya que corresponde a la gestión de un elemento de red (NE) y no así a un sistema de gestión (MS). La gestión de elementos de red requiere la supervisión de un dispositivo mediante una serie de mecanismos, quizá simultáneamente, mientras se efectúan las modificaciones de configuración. Esto no es necesario en el caso de un MS.

El objetivo de este requisito es gestionar la capacidad de los usuarios en cuanto al consumo de todos los recursos disponibles de un NE/MS. El personal de explotación debería ajustar por defecto en cuanto al NE conforme sea necesario habida cuenta de la situación, y supervisar e investigar los intentos por sobrepasar esos límites, ya que esto puede indicar una deficiencia operacional o un intento de actividad maliciosa.

REQ 25: El NE/MS debería impedir, controlar o limitar la utilización activa simultánea del mismo ID de usuario, si así se estima oportuno. El número de sesiones activas simultáneas debería ser configurable por parte de cada usuario.

REQ 26: La aplicación del NE/MS no debería requerir privilegios de acceso como **superusuario** para funcionar adecuadamente.

REQ 27: El NE/MS debería disponer de la capacidad para que el usuario pueda visualizar, cuando así se estime conveniente, durante el proceso de acceso al sistema, la hora y la fecha de la última **autenticación** satisfactoria del usuario.

REQ 28: En la pantalla inicial y antes de que se permita cualquier acceso lógico debería visualizarse una declaración de información propietaria personalizada y una advertencia de acceso prohibido. El equipo debería soportar una longitud mínima de 1600 caracteres. Convendría disponer de un mensaje por defecto.

A continuación se presenta un ejemplo de una insignia de advertencia.

> ¡ADVERTENCIA! Este sistema y red de computadores es PRIVADO y PROPIETARIO y sólo usuarios autorizados pueden acceder al mismo. Queda estrictamente prohibido el uso no autorizado de este sistema o red de computadores ya que puede ser objeto de una sanción penal o de un procedimiento laboral disciplinario que podría redundar incluso en el despido del empleado encausado o la denuncia de contratos de proveedor/servicios. El propietario o sus agentes, pueden supervisar toda actividad o comunicación y recuperar cualquier información almacenada en el sistema o red de computadoras. El acceso y la utilización del sistema o la red de computadores, entraña necesariamente que usted acepta dicha supervisión y recuperación de información con propósitos de observancia de la ley y para otras finalidades. Los usuarios no han de esperar ninguna privacidad en cuanto a las comunicaciones o a la información almacenada en el sistema o red de computadores, incluida la información almacenada en forma local o distante en un disco duro o en otros medios utilizados en el sistema o la red de computadores.

Sería recomendable que cada entidad diseñe la correspondiente insignia de advertencia.

REQ 29: Cualquier intento fallido de acceso al sistema debe generar una notificación sólo al usuario indicando que el proceso de acceso ha fallado o que es no válido. No debería notificarse información tal como "ID de usuario no válido" o "contraseña no válida".

REQ 30: El NE/MS debe **bloquear** una cuenta de usuario a fin de que éste no pueda seguir intentando acceder al sistema una vez que se ha alcanzado un determinado número de intentos fallidos de acceso en relación con un umbral configurable. El **bloqueo** debería incluir la interfaz de la consola. El **bloqueo** NO debe incluir la cuenta por defecto original que soporta todas las medidas de gestión.

REQ 31: El NE/MS NO debe disponer de un mecanismo para obviar los procesos de **autenticación** del acceso al sistema y del propio acceso al sistema.

REQ 32: En ningún caso, un NE/MS debe visualizar la información correspondiente a la identidad en texto normal, por ejemplo, una contraseña, en ningún tipo de medio, incluyendo visualización en pantallas de los terminales, impresiones y almacenamiento en ficheros de registro cronológico.

REQ 33: El NE/MS debe exigir el cumplimiento de la prescripción de las contraseñas con un umbral configurable.

Una aplicación común y aceptable de REQ 33 es aquella que permite que el sistema solicite al usuario la inmediata creación de una nueva contraseña una vez autenticada su antigua contraseña. Por otra parte, el sistema puede exigir que un administrador modifique la contraseña adecuadamente. Si una cuenta no ha sido utilizada por un determinado periodo, ésta se considerará aletargada.

REQ 34: Si una contraseña de acceso al sistema ha sobrepasado el límite de prescripción del sistema, el NE/MS debe **bloquear** la clave de acceso de ese ID de usuario hasta que la contraseña se modifique adecuadamente.

REQ 35: Si una cuenta ha estado aletargada por un periodo de umbral configurable, cada uno de los NE/MS debería generar una alerta.

REQ 36: Si una cuenta ha estado aletargada por un periodo de umbral configurable, el NE/MS debe inhabilitar esa cuenta tras la generación de una alerta de inhabilitación. El proceso de INHABILITACIÓN NO debe incluir las cuentas de: **administrador del sistema**, **administrador de seguridad del sistema** y **superusuario**.

REQ 37: Para habilitar nuevamente un ID de acceso **inhabilitado** es necesario que intervenga un administrador que se haya registrado adecuadamente y que esté autorizado para ejecutar las medidas de administración de seguridad cruciales a fin de inicializar y reactivar las contraseñas de acceso.

Las opciones para habilitar nuevamente los ID de acceso podrán ser configuradas como parámetros en todo el sistema en el nivel de papeles.

REQ 38: Para reactivar un ID de acceso BLOQUEADO y suprimir la condición de **bloqueo**, es necesaria la intervención de un administrador registrado adecuadamente y que esté autorizado para ejecutar las medidas de administración de seguridad cruciales a fin de suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema.

Las opciones para suprimir un **bloqueo** de ID de acceso podrán ser configuradas como parámetros en todo el sistema en el nivel de papeles.

6.2.4 Proceso de fin de sesión

REQ 39: Toda **sesión** inicializada adecuadamente debe finalizar mediante inactividad del usuario o del sistema.

REQ 40: El NE/MS debe finalizar una **sesión** inicializada adecuadamente cuando el tiempo transcurrido desde la última actividad de esa **sesión** sobrepase el valor del temporizador de inactividad configurable del sistema.

6.2.5 Aplicaciones

REQ 41: Un tipo de papel de usuario debería permanecer sin modificaciones durante la ejecución y la conclusión de una aplicación NE/MS.

El usuario no debe tener la posibilidad de utilizar un mecanismo de secuencia de control, por ejemplo, escape hacia el intérprete de comandos para pasar a un modo de **superusuario**. O, si la aplicación falla, no ha de permitirse que el usuario pase a desempeñar otro papel con más privilegios. Para poder asumir un papel distinto, el usuario debe ser autenticado nuevamente (reinicio de sesión).

6.3 Protección de la confidencialidad

Esta cláusula especifica los requisitos de los algoritmos criptográficos y la gestión de claves para ayudar a garantizar la seguridad del sistema y de la red. Por lo general, se emplean algoritmos simétricos para los servicios de confidencialidad e integridad. Las claves de los algoritmos simétricos deben intercambiarse normalmente mediante un proceso rigurosamente vinculado a la autenticación. Los algoritmos asimétricos pueden utilizarse también para soportar los servicios de autenticación y de intercambio de claves. Los métodos aplicados para generar, almacenar, distribuir, destruir y revocar dichas claves tienen una importancia primordial. Además, factores tales como la longitud de la clave y la selección de la clave y del algoritmo tienen una relevancia directa en la rigidez de la seguridad de un sistema criptográfico específico.

La **protección de la autenticación** y la confidencialidad de los datos se basan en un fundamento criptográfico. La criptografía utiliza algoritmos especiales orientados a normas y disponibles públicamente, lo que permite una inspección rigurosa generalizada y facilita su aplicación. La "resistencia" criptográfica se basa en el algoritmo criptográfico y el tamaño de la clave que se

utilicen (es decir, la resistencia remite a la cantidad de tiempo necesario para aplicar ingeniería inversa (es decir, encontrar o tratar de adivinar) el valor o valores de las claves que se utilizan con un algoritmo específico).

Los protocolos de seguridad (por ejemplo, IPsec, SSL, SSH) ofrecen típicamente **autenticación**, integridad y confidencialidad. Las extensiones de seguridad a otros protocolos tales como la versión 3 del protocolo de gestión de red simple (SNMPv3)[4], 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 (OSPF, *open shortest path first*) se han diseñado para proporcionar **autenticación** e integridad. La **protección de la autenticación** y de la integridad entre NE/MS son esenciales y, en su caso, la confidencialidad resulta también indispensable.

6.3.1 Algoritmos de criptación simétrica

La criptación simétrica o por claves secretas remite a un sistema criptográfico en el que las claves de criptación y descriptación son idénticas. Los sistemas criptográficos simétricos exigen que se tomen las disposiciones iniciales necesarias para que los interesados compartan una clave secreta única (por ejemplo, la clave de criptación). La clave debe distribuirse a los interesados a través de medios seguros o generarse internamente (por ejemplo, basándose en una clave raíz secreta compartida) ya que el conocimiento de la clave de criptación implica a su vez el conocimiento de la clave de descriptación y viceversa.

REQ 42: Para todas las aplicaciones de criptación simétrica, la fortaleza de los algoritmos deberá ser congruente con la política nacional, industrial u organizacional.

6.3.2 Algoritmos de criptación asimétrica

Un sistema de criptación asimétrica es aquel en el que las claves de criptación y descriptación están relacionadas pero son distintas. Una de ellas es del dominio público, mientras que la otra se mantiene en secreto. La clave pública es distinta de la clave privada, y no existe ninguna forma viable de obtener la clave privada a partir de la clave pública. Las claves públicas son distribuidas de manera generalizada; no obstante, la clave privada se mantiene siempre en secreto. Por lo general, la utilización de la criptación asimétrica está limitada a la criptación de claves simétricas para el intercambio de claves y a la firma de resúmenes de mensajes para las firmas digitales. Para el intercambio de claves se utiliza la clave pública del destinatario y para la firma de los resúmenes de mensajes se emplea la clave privada del firmante.

REQ 43: En todas las aplicaciones de criptación asimétrica, la resistencia de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.

REQ 44: En todas las aplicaciones de intercambio de claves, la fortaleza de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.

6.3.3 Gestión de las claves criptográficas

La gestión apropiada del material de claves criptográficas es difícil y a menudo compleja, puesto que incluye la expiración y el intercambio y la publicación seguros, además de la generación de las mismas. En la Norma RFC 1750 del IETF, *Randomness Recommendations for Security*, figuran directrices adicionales.

6.3.4 Comunicaciones

Las comunicaciones seguras son el fundamento necesario para asegurar el **plano de gestión** de una red moderna. En el anexo A se examinan arquitecturas y protocolos para aplicar **comunicaciones de gestión** segura. Los requisitos obligatorios que se definen en esta cláusula podrán aplicarse a

---

[4] SNMPv3 también puede ofrecer confidencialidad.

todas las interfaces de una RGT, como se describe en la Rec. UIT-T M.3010, *Principios para una red de gestión de las telecomunicaciones.*

REQ 45: Para cada interfaz física o lógica que conduzca cualquier tipo de **tráfico de gestión** en un NE/MS, el NE/MS debería ser configurable para poder asegurar dicho tráfico con **autenticación resistente** y protección criptográfica a fin de proporcionar confidencialidad, integridad y protección antirreproducción.

REQ 46: Cualquier transmisión de una contraseña en texto normal debería efectuarse únicamente a través de un **trayecto de confianza** a menos que se utilice un mecanismo de contraseña de un solo uso. Si se emplean contraseñas de un solo uso, podrán enviarse en texto normal, siempre que no exista un anfitrión intermedio.

6.4 Protección de la integridad de los datos

6.4.1 Algoritmos de integridad de los datos

Podrían utilizarse algoritmos de resumen de mensajes codificados junto con funciones de troceo para garantizar la integridad de los datos de mensajes de longitud arbitraria.

REQ 47: En todas las aplicaciones de integridad de datos seguras y simétricas, la resistencia de los algoritmos deberá ser compatible con las políticas nacionales, industriales u organizacionales.

REQ 48: En todas las aplicaciones de integridad de datos seguras asimétricas, la resistencia de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.

6.4.2 Evolución y entrega de NE/MS

La seguridad de un NE/MS depende del ciclo completo de vida útil. La seguridad representa un problema durante el diseño conceptual y lo sigue siendo durante el diseño detallado, la evolución, el despliegue y la supresión de un producto. Los controles y la prueba adecuados durante el ciclo completo de vida útil revisten crucial importancia para ofrecer niveles de seguridad aceptables. En las cláusulas I.5.2 e I.5.3 se examinan otras consideraciones en torno al ciclo de vida útil.

REQ 49: Todos los programas lógicos entregados a un proveedor de servicio o a otro cliente deben incluir, cuando proceda, mecanismos de **autenticación** criptográfica y mecanismos de protección de la integridad tales como firmas digitales o **autenticación** simétrica del mensaje conforme a la Rec. UIT-T M.3016.3.

REQ 50: Todos los NE/MS que reciben programas informáticos han de ser capaces de interpretar los mecanismos de **autenticación** criptográfica y de protección de la integridad y de verificar el origen y la integridad del soporte lógico, cuando proceda.

REQ 51: Todas las actualizaciones del soporte lógico, incluidas las correcciones, deben ser transmitidas al NE/MS a través de un **trayecto de confianza**.

El NE/MS debe estar en condiciones de determinar electrónicamente sus actuales versiones de soporte lógico y soporte físico y de validar las configuraciones pertinentes del soporte lógico/microprogramas.

6.5 Imputabilidad

El objetivo de la imputabilidad es velar por que cualquier entidad sea responsable de cualquier acción que inicie.

REQ 52: Todos los NE/MS deben disponer de la capacidad para verificar que una entidad no pueda denegar su responsabilidad por cualquiera de las acciones que realice así como por sus efectos.

En cuanto a los requisitos de imputabilidad relacionados con la evolución y la entrega del NE/MS, véanse los REQ 49 y REQ 50.

6.6 Acceso al sistema y auditoría de la seguridad

Es importante que todo NE/MS disponga de las capacidades adecuadas para facilitar las actividades de investigación, auditoría, detección en tiempo real, análisis y protección, de manera que puedan adoptarse las medidas de rehabilitación apropiadas. En esta cláusula se examinan los registros cronológicos de auditoría de seguridad; no obstante, los detalles específicos del contenido y el formato de dichos registros cronológicos quedan fuera del alcance de esta Recomendación.

Obsérvese que las actividades de investigación y de análisis pormenorizado pueden incluir la investigación de mensajes OAM&P relacionados con la falta de seguridad y de la información almacenada en los registros cronológicos de auditoría de seguridad que se describen en esta cláusula. El registro de mensajes OAM&P que tienen que ver con la falta de seguridad, que algunas veces se denominan mensajes "de modificación reciente", es necesario en lo que respecta a algunas acciones que puedan estar sujetas a auditoría.

REQ 53: El NE/MS debe ser capaz de registrar cronológicamente cualquier acción que modifique los atributos y los servicios de seguridad, los controles de acceso, los parámetros de configuración de los dispositivos.

REQ 54: El NE/MS debe disponer de la capacidad para configurar las **medidas de administración de seguridad cruciales** que habrán de incluirse en el registro cronológico de seguridad.

REQ 55: El NE/MS debe ser capaz de registrar cronológicamente cada intento de acceso al sistema y su resultado, cada fin o terminación de sesión (sea a distancia o a través de una consola) y cada intento de acceso y el resultado de dicho intento que provoque la invocación del temporizador de inactividad del sistema que se define en REQ 12.

Se recomienda que las entradas al registro cronológico de auditoría se envíen a un servidor de auditoría inalterable, tras haber sido etiquetadas en secuencia y autenticadas criptográficamente (firmadas) por el NE/MS.

REQ 56: El NE/MS debe tener la capacidad de efectuar un registro a distancia a través de un **trayecto de confianza**.

REQ 57: Cada entrada al registro cronológico debería contener la siguiente información:

- Una descripción de la acción o de la acción real que está siendo registrada.
- El nivel de identidad y de seguridad del usuario o proceso que inició la acción.
- La fecha y hora en que ocurrió la acción.
- Información de origen y destino de red, si procede (por ejemplo, cuando se accede al sistema).
- Una indicación del éxito o fracaso de la actividad.

6.7 Notificación de alarmas de seguridad

Algunos eventos deberán notificarse como alarmas de seguridad, véase por ejemplo REQ 35. No obstante, queda fuera del alcance de esta Recomendación identificar los eventos específicos que han de ser notificados.

REQ 58: Todos los NE/MS deben disponer de la capacidad de generar notificaciones de alarmas relativas a eventos seleccionados.

REQ 59: Todos los NE/MS deben disponer de la capacidad de permitir que el usuario defina los criterios de selección de los eventos que generan notificaciones de alarma.

6.8 Protección de la red de comunicación de datos (RCD)

Para proteger la infraestructura de gestión y la RCD en general, resulta útil que el operador de la red supervise y tome las acciones necesarias sobre cierto tráfico recibido de la RCD o destinado a algún lugar fuera de la misma (por ejemplo, desde redes y clientes pares). Por ejemplo, los paquetes con direcciones IP de origen que concuerdan con el espacio de dirección de la RCD no deberían estar autorizados a acceder a la RCD si provienen de redes externas.

REQ 60: Todos los NE/MS con conectividad basada en paquetes deben impedir que se curse tráfico incompatible con la política de seguridad de la RCD.

Anexo A

Correspondencia entre los requisitos, servicios y mecanismos de seguridad

En este anexo se expone la correspondencia entre los requisitos y los servicios de seguridad que se definen en la Rec. UIT-T M.3016.2 y los mecanismos de seguridad que se definen en la Rec. UIT-T M.3016.3.

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 1: Para efectos de acceso a los NE/MS, registro y auditoría, debería soportarse la autenticación fuerte.	**SER 1, SER 2, SER 3, SER 8**	**MEC 1-MEC 13**
REQ 2: Todo NE/MS debería exigir el cumplimiento de la **autenticación** conforme a la política de la organización.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 3: Todo NE/MS debería soportar las reglas de complejidad mínimas establecidas para la **autenticación** conforme a la política de la organización.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 6**
REQ 4: El NE/MS debería impedir que otro usuario pueda modificar una contraseña de de un usuario sin su consentimiento.	**SER 8**	**MEC 7-MEC 11**
REQ 5: Cada NE/MS debería garantizar automáticamente que cada nueva contraseña de acceso sea diferente de la contraseña anterior. El grado de diferencia debería ser configurable conforme a la política de la organización.	**SER 1**	**MEC 7-MEC 11**
REQ 6: Todo NE/MS debería soportar la prevención de la reutilización de contraseñas. Los parámetros correspondientes deberían ser configurables conforme a la política de la organización.	**SER 1**	**MEC 7-MEC 11**
REQ 7: Todo ID de usuario debería poder fijar sus propias contraseñas de acceso.	**SER 1**	**MEC 7-MEC 11**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 8: El usuario debería poder modificar sus contraseñas a su conveniencia, respetando un intervalo mínimo a partir de la última modificación. El intervalo mínimo debe ser configurable conforme a la política de la organización y fijarse a través del **administrador de seguridad del sistema**.	**SER 1**	**MEC 7-MEC 11**
REQ 9: Todo NE/MS debería soportar el control de contraseñas en multiniveles. Algunos usuarios podrán quedar bloqueados (por ejemplo, debido a la prescripción de la contraseña o a algún fallo de la clave de acceso) mientras que a otros no les sucederá lo mismo.	**SER 1, SER 2, SER 3, SER 4**	**MEC 20-MEC 23**
REQ 10: Debería aplicarse uno de los siguientes: • El soporte lógico de configuración debería crear una contraseña de inicialización única por cada aplicación en la nueva versión o actualización del soporte lógico. • Si se utiliza una contraseña por defecto, el sistema debería exigir su sustitución por una contraseña única antes de que el dispositivo se ponga en servicio. • Si un dispositivo es entregado sin una contraseña o una contraseña nula, debería asignarse una contraseña única durante el proceso de instalación antes de que el dispositivo se ponga en servicio.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 11: El umbral de prescripción del sistema en cuanto a las contraseñas de acceso debería ser configurable si la funcionalidad está integrada también en la aplicación. Cuando se alcanza el umbral de prescripción la contraseña de acceso a una aplicación afectada debería ser reactivada al estado por defecto original definido en REQ 10. Todos los privilegios de modificación de contraseñas deberían ser revocados a todos los usuarios excepto para el papel de usuario, el cual tiene el nivel más alto de autoridad de seguridad para un sistema o un ejemplar dados.	**SER 4**	**MEC 7-MEC 11**
REQ 12: El valor del temporizador de inactividad del sistema debería ser configurable si la funcionalidad también está integrada en la aplicación. Cuando dicho temporizador esté habilitado, debería impedirse el acceso de un determinado ID de usuario al sistema y el proceso de acceso al sistema de este usuario debería inhabilitarse.	**SER 4**	**MEC 7-MEC 11**
REQ 13: El límite del sistema por lo que se refiere a los intentos consecutivos fallidos de acceso al sistema de un determinado ID de usuario debería ser configurable si la funcionalidad también está integrada en la aplicación. Cuando se alcanza dicho límite para un determinado ID de usuario, deberá invocarse el temporizador de inactividad del sistema definido en REQ 12.	**SER 4**	**MEC 7-MEC 11**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 14: Todo NE/MS debería estar en condiciones de soportar múltiples tipos de papeles de usuario definidos por el usuario, y las **medidas de gestión** deberían poder asignarse a cada papel de usuario.	**SER 4**	**MEC 20-MEC 23**
REQ 15: Todo NE/MS debería soportar un tipo de usuario por defecto, que pueda desempeñar **medidas de gestión** mínimas o restringidas.	**SER 4**	**MEC 20-MEC 23**
REQ 16: Todo NE/MS debería soportar las siguientes **medidas de administración de seguridad cruciales**, aunque no sean las únicas: • Definir y asignar privilegios de usuario y de grupo. • Conservar un registro de todas las peticiones de ID de acceso al sistema. • Añadir y suprimir ID de usuario. • Inhabilitar y habilitar la utilización de ID de usuario específicos como ID de acceso. • Inicializar y reactivar contraseñas de acceso al sistema. • Inicializar y modificar claves criptográficas. • Establecer el umbral de prescripción del sistema en cuanto a las contraseñas de acceso. • Establecer el límite del sistema con relación al número de intentos de acceso fallidos por cada ID de acceso. • Suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema. • Fijar el valor del temporizador de inactividad del sistema. • Establecer el procedimiento de registro de las actividades de seguridad del sistema y la configuración de alarmas. • Supervisar todos los registros de seguridad del sistema. • Gestionar los procesos de registro de las actividades de seguridad del sistema. • Actualizar el soporte lógico de seguridad. • Terminar cualquier sesión de usuario o de sistema. • Delegar autorizaciones de seguridad a personas especificas con otras funciones. • Fijar reglas complejas para las contraseñas.	**SER 4, SER 8**	**MEC 20-MEC 23**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 17: Todo NE/MS debería soportar las siguientes **medidas de gestión** de seguridad de aplicación, aunque no sean las únicas: • Definir y asignar nuevos privilegios de usuario y de grupo al nivel de aplicación. • Conservar un registro de todas las peticiones de ID de acceso a la aplicación. • Añadir y suprimir usuarios en el nivel de aplicación. • Supervisar todos los registros de seguridad de la aplicación. • Configurar los registros de las actividades de seguridad de la aplicación y las alarmas. • Gestionar los procesos de registro de las actividades de seguridad de la aplicación. • Terminar la sesión de aplicación de usuario.	**SER 4, SER 8**	**MEC 20-MEC 23**
REQ 18: El NE/MS debería sincronizar el tiempo de una manera autenticada (por ejemplo, versión 3 de NTP).	**SER 8**	**N/A**
REQ 19: Para un NE/MS, cada **medida de gestión** debería estar asociada con una única SESIÓN autorizada.	**SER 4**	**MEC 20-MEC 23**
REQ 20: Toda SESIÓN debería establecerse a través de una **autenticación** apropiada, según se describe con detalle en el requisito REQ 1.	**SER 1, SER 2, SER 3**	**MEC 1-MEC 12**
REQ 21: Las comunicaciones entre un NE/MS y un ACS necesarias con el fin de transportar la información de **autenticación** deberían tener lugar a través de un **trayecto de confianza**.	**SER 5, SER 6**	**MEC 19**
REQ 22: El NE/MS debería utilizar **control de acceso** y particiones para autorizar, negar o, por el contrario, controlar un usuario, grupo de usuarios o el acceso de un sistema distante al NE/MS y debería disponer de la funcionalidad necesaria para restringir el acceso de los usuarios a los datos, transacciones y equipos necesarios para que puedan cumplir con sus papeles. Los permisos de acceso deberían incluir, aunque no sean los únicos, sólo lectura y lectura-escritura.	**SER 4**	**MEC 20-MEC 23**
REQ 23: El NE/MS debería soportar la capacidad para asignar a cada individuo un ID de usuario único para acceder a una aplicación o a un sistema de cómputo.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 24: El NE/MS debería disponer, en su caso, de la capacidad para obligar automáticamente al usuario a modificar su contraseña durante el primer acceso, después de que se haya establecido la cuenta, y durante el primer acceso una vez reactivada la contraseña.	**SER 4**	**MEC 7-MEC 11**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 25: El NE/MS debería impedir, controlar o limitar la utilización activa simultánea del mismo ID de usuario, si así se estima oportuno. El número de sesiones activas simultáneas debería ser configurable por parte de cada usuario.	**SER 1, SER 2, SER 3, SER 4**	**MEC 7-MEC 11**
REQ 26: La aplicación del NE/MS no debería requerir privilegios de acceso como **superusuario** para funcionar adecuadamente.	**SER 4**	**MEC 20-MEC 23**
REQ 27: El NE/MS debería disponer de la capacidad para que el usuario pueda visualizar, cuando así se estime conveniente, durante el proceso de acceso al sistema, la hora y la fecha de la última **autenticación** satisfactoria del usuario.	**SER 4, SER 8**	**MEC 7-MEC 11**
REQ 28: En la pantalla inicial y antes de que se permita cualquier acceso lógico debería visualizarse una declaración de información propietaria personalizada y una advertencia de acceso prohibido. El equipo debería soportar una longitud mínima de 1600 caracteres. Convendría disponer de un mensaje por defecto.	**SER 4**	**N/A**
REQ 29: Cualquier intento fallido de acceso al sistema debe generar una notificación sólo al usuario indicando que el proceso de acceso ha fallado o que es no válido. No debería notificarse información tal como "ID de usuario no válido" o "contraseña no válida".	**SER 8**	**MEC 7-MEC 11**
REQ 30: El NE/MS debe **bloquear** una cuenta de usuario a fin de que éste no pueda seguir intentando acceder al sistema una vez que se ha alcanzado un determinado número de intentos fallidos de acceso en relación con un umbral configurable. El **bloqueo** debería incluir la interfaz de la consola. El **bloqueo** NO debe incluir la cuenta por defecto original que soporta todas las medidas de gestión.	**SER 4**	**MEC 7-MEC 11**
REQ 31: El NE/MS NO debe disponer de un mecanismo para obviar los procesos de **autenticación** del acceso al sistema y del propio acceso al sistema.	**SER 1, SER 2, SER 3**	**MEC 7-MEC 11**
REQ 32: En ningún caso, un NE/MS debe visualizar la información correspondiente a la identidad en texto normal, por ejemplo, una contraseña, en ningún tipo de medio, incluyendo visualización en pantallas de los terminales, impresiones y almacenamiento en ficheros de registro cronológico.	**SER 8**	**MEC 7-MEC 11**
REQ 33: El NE/MS debe exigir el cumplimiento de la prescripción de las contraseñas con un umbral configurable.	**SER 4**	**MEC 7-MEC 11**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 34: Si una contraseña de acceso al sistema ha sobrepasado el límite de prescripción del sistema, el NE/MS debe **bloquear** la clave de acceso de ese ID de usuario hasta que la contraseña se modifique adecuadamente.	**SER 4**	**MEC 7-MEC 11**
REQ 35: Si una cuenta ha estado aletargada por un periodo de umbral configurable, cada uno de los NE/MS debería generar una alerta.	**SER 4, SER 8, SER 9**	**MEC 7-MEC 11** **MEC 33-MEC 37**
REQ 36: Si una cuenta ha estado aletargada por un periodo de umbral configurable, el NE/MS debe inhabilitar esa cuenta tras la generación de una alerta de inhabilitación. El proceso de INHABILITACIÓN NO debe incluir las cuentas de: **administrador del sistema**, **administrador de seguridad del sistema** y **superusuario**.	**SER 4, SER 8**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 37: Para rehabilitar nuevamente un ID de acceso inhabilitado es necesario que intervenga un administrador que se haya registrado adecuadamente y que esté autorizado para ejecutar las medidas de administración de seguridad cruciales a fin de inicializar y reactivar las contraseñas de acceso.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 38: Para reactivar un ID de acceso BLOQUEADO y suprimir la condición de **bloqueo**, es necesaria la intervención de un administrador registrado adecuadamente y que esté autorizado para ejecutar las medidas de administración de seguridad cruciales a fin de suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema.	**SER 4**	**MEC 7-MEC 11** **MEC 20-MEC 23**
REQ 39: Toda **sesión** inicializada adecuadamente debe finalizar mediante inactividad del usuario o del sistema.	**SER 4**	**MEC 33-MEC 37**
REQ 40: El NE/MS debe finalizar una **sesión** inicializada adecuadamente cuando el tiempo transcurrido desde la última actividad de esa **sesión** sobrepase el valor del temporizador de inactividad configurable del sistema.	**SER 4**	**MEC 7-MEC 11**
REQ 41: Un tipo de papel de usuario debería permanecer sin modificaciones durante la ejecución y la conclusión de una aplicación NE/MS.	**SER 4**	**MEC 20-MEC 23**
REQ 42: Para todas las aplicaciones de criptación simétrica, la fortaleza de los algoritmos deberá ser congruente con la política nacional, industrial u organizacional.	**SER 5, SER 6**	**MEC 24-MEC 26**
REQ 43: En todas las aplicaciones de criptación asimétrica, la resistencia de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.	**SER 5, SER 6**	**MEC 27-MEC 28**
REQ 44: En todas las aplicaciones de intercambio de claves, la fortaleza de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.	**SER 5, SER 6**	**MEC 38-MEC 40**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 45: Para cada interfaz física o lógica que conduzca cualquier tipo de **tráfico de gestión** en un NE/MS, el NE/MS debería ser configurable para poder asegurar dicho tráfico con **autenticación resistente** y protección criptográfica a fin de proporcionar confidencialidad, integridad y protección antirreproducción.	**SER 2, SER 3, SER 5, SER 6**	**MEC 24-MEC 32**
REQ 46: Cualquier transmisión de una contraseña en texto normal debería efectuarse únicamente a través de un **trayecto de confianza** a menos que se utilice un mecanismo de contraseña de un solo uso. Si se emplean contraseñas de un solo uso, podrán enviarse en texto normal, siempre que no exista un anfitrión intermedio.	**SER 1, SER 2, SER 3, SER 5, SER 6**	**MEC 19**
REQ 47: En todas las aplicaciones de integridad de datos seguras y simétricas, la resistencia de los algoritmos deberá ser compatible con las políticas nacionales, industriales u organizacionales.	**SER 5**	**MEC 29-MEC 30**
REQ 48: En todas las aplicaciones de integridad de datos seguras asimétricas, la resistencia de los algoritmos debe ser compatible con las políticas nacionales, industriales u organizacionales.	**SER 5**	**MEC 31-MEC 32**
REQ 49: Todos los programas lógicos entregados a un proveedor de servicio o a otro cliente deben incluir, cuando proceda, mecanismos de **autenticación** criptográfica y mecanismos de protección de la integridad tales como firmas digitales o **autenticación** simétrica del mensaje conforme a la Rec. UIT-T M.3016.3.	**SER 7**	**MEC 29-MEC 32**
REQ 50: Todos los NE/MS que reciben programas informáticos han de ser capaces de interpretar los mecanismos de **autenticación** criptográfica y de protección de la integridad y de verificar el origen y la integridad del soporte lógico, cuando proceda.	**SER 7**	**MEC 29-MEC 32**
REQ 51: Todas las actualizaciones del soporte lógico, incluidas las correcciones, deben ser transmitidas al NE/MS a través de un **trayecto de confianza**.	**SER 5, SER 6**	**MEC 19**
REQ 52: Todos los NE/MS deben disponer de la capacidad para verificar que una entidad no pueda denegar su responsabilidad por cualquiera de las acciones que realice así como por sus efectos.	**SER 7**	**MEC 29-MEC 32**
REQ 53: El NE/MS debe ser capaz de registrar cronológicamente cualquier acción que modifique los atributos y los servicios de seguridad, los controles de acceso, los parámetros de configuración de los dispositivos y cada intento de acceso y el resultado de dicho intento que provoque la invocación del temporizador de inactividad del sistema que se define en REQ 12.	**SER 8**	**MEC 33-MEC 37**

Requisitos de seguridad de M.3016.1	Servicios de seguridad de M.3016.2	Mecanismos de seguridad de M.3016.3
REQ 54: El NE/MS debe disponer de la capacidad para configurar las **medidas de administración de seguridad cruciales** que habrán de incluirse en el registro cronológico de seguridad.	**SER 4**	**MEC 33-MEC 37**
REQ 55: El NE/MS debe ser capaz de registrar cronológicamente cada intento de acceso al sistema y su resultado, cada fin o terminación de sesión (sea a distancia o a través de una consola).	**SER 8**	**MEC 33-MEC 37**
REQ 56: El NE/MS debe tener la capacidad de efectuar un registro a distancia a través de un **trayecto de confianza**.	**SER 5, SER 6, SER 8**	**MEC 33-MEC 37** **MEC 19**
REQ 57: Cada entrada al registro cronológico debería contener la siguiente información: • Una descripción de la acción o de la acción real que está siendo registrada. • El nivel de identidad y de seguridad del usuario o proceso que inició la acción. • La fecha y hora en que ocurrió la acción. • Información de origen y destino de red, si procede (por ejemplo, cuando se accede al sistema). • Una indicación del éxito o fracaso de la actividad.	**SER 8**	**MEC 33-MEC 37**
REQ 58: Todos los NE/MS deben disponer de la capacidad de generar notificaciones de alarmas relativas a eventos seleccionados.	**SER 9**	**MEC 41**
REQ 59: Todos los NE/MS deberían disponer de la capacidad para permitir que el usuario defina los criterios de selección de los eventos que generan notificaciones de alarma.	**SER 9**	**MEC 41**
REQ 60: Todos los NE/MS con conectividad basada en paquetes deben impedir que se curse tráfico incompatible con la política de seguridad de la RCD.	**SER 10**	**MEC 42**

Apéndice I

Consideraciones de seguridad adicionales

Los procedimientos de seguridad que se describen con detalle en las cláusulas subsiguientes son de índole didáctica y aunque quedan fuera del alcance de los requisitos detallados que se exponen en esta Recomendación, deberían considerarse para garantizar un sistema seguro. Si bien en algunos casos se emplea lenguaje obligatorio, esto se hace con propósitos de información y sólo con carácter ilustrativo. Los protocolos y recomendaciones que se incluyen en esta Recomendación están sujetos a exámenes y contribuciones futuros y no deben considerarse como un intento de incluir o excluir contenido en normas existentes o emergentes.

I.1 Aplicabilidad a las operaciones, administración, mantenimiento y aprovisionamiento de las empresas

Las empresas han evolucionado más allá de las tradicionales redes empresariales aisladas. Éstas se han expandido y se han implantado en empresas con múltiples sucursales que abarcan grandes zonas geográficas y que requieren conexiones a redes externas (extranet) de sus clientes y socios comerciales. Las empresas deben permitir que sus socios y clientes puedan acceder a los datos internos y adoptar decisiones comerciales operacionales basándose en esos datos.

Las redes empresariales son desarrolladas y administradas por la propia empresa o se adquieren con carácter de redes gestionadas de proveedores de red. Los servicios que están siendo desarrollados por los proveedores permitirán que la empresa gestione la parte que le corresponde de un entorno de red más grande.

A medida que la industria evoluciona, los requisitos de acceso a los datos relativos a las averías y la calidad de funcionamiento, y la capacidad para configurar diversos componentes de la red mediante la empresa contratada, exigen que se disponga de los mecanismos de seguridad apropiados. Esos mecanismos deben proporcionar el adecuado control para proteger no sólo la red gestionada de las empresas, sino también la propia red interna del proveedor. La red interna puede estar interconectada con esas redes empresariales y formar parte de la infraestructura de telecomunicaciones. En resumen, los requisitos de seguridad relativos al tráfico de las operaciones, administración, mantenimiento y aprovisionamiento que se describen en este apéndice son plenamente aplicables a las redes de las empresas o de proveedor de servicios/operadores.

I.2 Arquitectura de intermediario de petición de objeto común, protocolo de gestión de red simple, lenguaje de marcaje extensible y protocolo simple de acceso a objetos

Las siguientes consideraciones deberían tenerse en cuenta en lo que atañe a la seguridad de la arquitectura de intermediario de petición de objeto común (CORBA), el protocolo simple de gestión de red (SNMP, *simple network management protocol*), el lenguaje de marcaje extensible (XML, *extensible markup language*), y el protocolo simple de acceso a objetos (SOAP, *simple object access protocol*). Además, hay otros protocolos que pueden aplicarse de la misma manera como es el caso del protocolo de intercambio de bloques extensible. Aunque no se proponen modificaciones respecto a estos protocolos evolutivos, el siguiente análisis podría servir para mejorar la seguridad.

I.2.1 CORBA

El servicio de seguridad de CORBA abarca la funcionalidad de seguridad relativa a la autenticación de los elementos principales (usuarios físicos y objetos), la autorización de acceso de los elementos principales a los objetos, la auditoría de seguridad, la seguridad de la comunicación, el no rechazo y la administración. No obstante, todo esto puede resultar excesivo para muchas aplicaciones. Por el contrario, las aplicaciones podrían necesitar únicamente la funcionalidad de la seguridad de la

comunicación y la autenticación en el nivel de sistema basada en la tecnología de la seguridad de la capa de transporte (TLS, *transport layer security*) (y su precursor, la capa de zócalo segura (SSL, *secure socket layer*)) por motivos de disponibilidad y simplicidad. Por último, podría darse el caso de que algunas aplicaciones no requieran seguridad. En consecuencia, los requisitos facultativos a continuación responden a tres elecciones posibles:

– Sin seguridad.

– El mediador de petición de objetos (ORB, *object request brokers*) utiliza TLS (o SSL) para ofrecer seguridad de las comunicaciones y autenticación al nivel de sistema, lo que representa esencialmente la seguridad de la "sesión".

– El ORB emplea el servicio de seguridad CORBA para ofrecer seguridad a las comunicaciones, autenticación, no rechazo y listas de control de acceso de grupos o usuarios que acceden a objetos y operaciones individuales.

En la Rec. UIT-T Q.816, *Servicios de la RGT basados en arquitectura de intermediario de petición de objeto común* y Rec. UIT-T Q.816.1, *Servicios de la RGT basados en arquitectura de intermediario de petición de objeto común: Extensiones para el soporte de interfaces de granularidad gruesa*, puede encontrarse información adicional sobre seguridad en el marco de CORBA.

Cuando se utilice CORBA en las interfaces del elemento de red/sistema de gestión (NE/MS), deberían aplicarse los mecanismos de seguridad CORBA. Es necesario que se aclare el nivel de conformidad de la aplicación de la seguridad CORBA. El siguiente análisis proporciona una directriz en cuanto a la seguridad de CORBA y no debe entenderse como un intento de identificar normas. Cuando se suministran productos o sistemas basados en CORBA, los niveles de seguridad básicos son:

– Nivel 0: No se proporciona seguridad y los programas no se ocupan de seguridad. Es necesario proporcionar administración de la autenticación, criptación, integridad de los datos, autorización de la invocación de objetos, registro del camino de auditoría y del dominio de seguridad.

– Nivel 1: Los programas pueden ser conscientes de la seguridad, lo que significa que podrán llamar a una interfaz de programación de aplicación para acceder a servicios adicionales tales como la verificación de firmas, la verificación del acceso a objetos y la escritura en los registros de auditoría.

– Nivel 2: Se proporciona soporte mediante firmas digitales que permiten la firma y el no rechazo de las transacciones. Esto resulta particularmente importante cuando se trabaja a través de diversas organizaciones, por ejemplo, en un contexto de empresa a empresa o en una disposición de gestión de red entre pares.

La especificación de interoperabilidad segura común (CSI, *common secure interoperability*) define normas codificando la especificación de la interoperabilidad segura, cuando se utiliza el protocolo general inter-ORB/protocolo Internet Inter-ORB:

– CSI Nivel 1: La identidad del elemento principal iniciador se comunica del emisor al receptor.

– CSI Nivel 2: La identidad del elemento principal iniciador se comunica del emisor al receptor, pero la identidad puede ser delegada a otros objetos de manera que éstos puedan hacerse pasar por el usuario.

– CSI Nivel 3: Además de transferir la identidad, los atributos del elemento principal iniciador que pasan del cliente al objetivo pueden incluir otro tipo de información de autorización, tal como los miembros de los papeles o los grupos.

A los suministradores les interesa:

– Poder dialogar plenamente con las capacidades de seguridad de la tecnología ORB seleccionada.

– Asegurar que se atienda a los requisitos de seguridad descritos en esta Recomendación.

Como su nombre lo sugiere, CORBA trata de objetos. Por seguridad de los objetos se entiende impedir la utilización no autorizada de los mismos, exigiendo el cumplimiento de una serie de reglas de control de acceso. La seguridad de CORBA garantiza no sólo que los usuarios serán responsables de sus acciones sobre un objeto o con éste, sino también la disponibilidad de los objetos.

La seguridad de los objetos es algo que difiere de muchos otros aspectos de la seguridad. No suele ser necesario que el formulador conozca los detalles de seguridad, ya que la seguridad se aplica en una etapa posterior como si se tratara de una envoltura. Por consiguiente, ciertos aspectos son de vital importancia. En CORBA los nombres pueden haberse duplicado o no existir; lo que sí puede haber son los números de referencia y debería ser posible definir la política de un objeto sin conocer su nombre. Asimismo, debe ser posible definir la política de un objeto aun cuando se trate de objetos con muchos nombres y esta política debería aplicarse independientemente del nombre que se emplee para asegurar el objeto.

Los sistemas típicos orientados a objetos constan de decenas de miles de objetos y no resulta razonable esperar que la seguridad se defina para objetos individuales. Por consiguiente, debería ser posible agrupar objetos y definir una política para el grupo correspondiente cuyas necesidades de protección sean similares.

– *Autenticación extremo a extremo*: CORBA puede hacer pasar el contexto del usuario a otra aplicación. Cuando se haya establecido una sólida relación de confianza entre estos sistemas, cabría la posibilidad de aceptar esta información sin ninguna verificación adicional. Sin embargo, cuando no existan otros mecanismos, podría ser necesario, a efectos de la seguridad de otros sistemas, acoplarlos rigurosamente con la seguridad que ofrece CORBA. La autenticación extremo a extremo es muy importante, y es recomendable verificar si el proveedor la soporta.

– *Control de acceso:* CORBA soporta la idea de un acceso al sistema basado en papeles. En todo momento, los sistemas deberían desarrollarse utilizando esta característica ya que no solamente permite reducir los costos de administración sino que la simplifica, y reduce, por tanto, la probabilidad de errores en la configuración.

– *Criptación:* El empleo de criptación en CORBA debe cumplir con los requisitos establecidos en esta Recomendación. Es necesario que utilicen plenamente las características de CORBA, en lo que respecta a la integridad, confidencialidad y a la autenticación del origen, especialmente cuando una red de cualquier tipo establece una comunicación.

– *Administración de política:* La administración de la política de CORBA se encarga de establecer la información acerca de los dominios, usuarios, papeles, política de acceso a objetos, política de protección de mensajes y política de auditoría. Durante el diseño hay que lograr la transparencia de todos los aspectos de la denominación de dominios y objetos. Los papeles deben ser definidos con claridad para garantizar una adecuada separación de las tareas.

I.2.2 Seguridad SNMP

El protocolo SNMP es un método que se utiliza en gran medida para administrar una gama muy diversa de equipos basados en procesador y tiene la capacidad de:

– obtener los parámetros de configuración del dispositivo;

– establecer los parámetros de configuración del dispositivo;

– enviar mensajes de alerta del dispositivo gestionado a un sistema de análisis centralizado.

Muchas de las versiones de SNMP que se han desplegado presentan aspectos muy vulnerables en materia de seguridad. En las versiones 1 y 2, la contraseña (conocida como la cadena comunitaria) se transmite en texto normal. Además, aunque pueden efectuarse verificaciones para validar la dirección de protocolo Internet (IP, *Internet protocol*) del cliente, un atacante moderadamente determinado puede simular direcciones IP. Las versiones 1 y 2 de SNMP son objeto de riesgos de seguridad considerables en diversas redes. Por consiguiente, esas versiones deberían utilizarse únicamente como último recurso. La Comisión de Estudio 4 del UIT-T se encuentra considerando el establecimiento de dos nuevas pilas de protocolos:

– SNMPv3 o V2C con TLS en relación con el protocolo de control de transmisión (sin control de acceso), y
– SNMPv3 con modelo de seguridad de usuario en relación con el protocolo de datagrama de usuario (como una pila orientada hacia el futuro).

Cuando se despliega SNMP, la versión 3 es el nivel que se prefiere. La versión 3 de SNMP es la más segura y debe ser utilizada en todos los nuevos sistemas, ya que ofrece protección contra la modificación de los datos, la impostura, el reordenamiento de mensajes y la pérdida de confidencialidad. Habría que tener en cuenta las siguientes contramedidas para asegurar el acceso por SNMPv3 a los NE:

– Si un agente de SNMP recibe una instrucción de origen desconocido, debe enviar un mensaje de alerta a un gestor.
– Deben utilizarse controles de acceso que permitan únicamente la entrada de mensajes SNMP que provengan de un gestor autorizado. Los mensajes SNMP de las demás fuentes deben denegarse y tratarse con arreglo a las políticas de seguridad apropiadas. Tal vez convenga bloquear las peticiones no autorizadas en el dispositivo y en un perímetro de la red.
– No debe recurrirse a la cadena comunitaria por defecto.
– Deben registrarse cronológicamente las violaciones y los errores de acceso.
– SNMPv3 utiliza la criptación estándar de datos por defecto; no obstante, pueden aplicarse algoritmos más seguros.
– SNMPv3 debe utilizarse al menos con AuthNoPriv, que proporciona autenticación aunque no ofrece confidencialidad de las transacciones. De preferencia se utilizará AuthPriv.
– Es necesario habilitar el registro de agentes SNMP.
– Debe inhabilitarse cualquier servicio o capacidad no solicitado explícitamente, lo que incluye el SNMP cuando éste se encuentre habilitado.

I.2.3 XML

La norma XML proporciona el lenguaje necesario para definir la estructura de datos. La norma vigente es la 1.0. La versión 1.1 es una Recomendación postulante que se está examinando. El Comité técnico de los servicios de seguridad de la organización para de las normas estructuradas de información (OASIS, *organization for the advancement of structured information standards*) intenta ampliar la funcionalidad de seguridad, impulsando XML. OASIS se encuentra a punto de terminar el lenguaje de etiquetado de enunciados de seguridad (SAML, *security assertion markup language*). El SAML se basa en cuatro aserciones:

– *Autenticación* – el emisor ha autenticado el objeto.
– *Atributo* – identificador de recurso uniforme especifico o esquema de extensión que define el atributo.
– *Decisión* – notifica la validez de la autenticación.
– *Autorización* – el sujeto tiene autorización para acceder a los recursos.

Las aserciones XML deben incluir:

– *Información básica* – identificador o nombre único para la aserción que incluye por lo general la fecha y la hora de emisión y el intervalo temporal de validez.

– *Afirmación* – documento que describe la utilización de la aserción.

– *Condición* – la aserción puede estar sujeta a condiciones que la validan o la invalidan.

– *Aviso* – proporciona información adicional tal como las aserciones que se utilizan para tomar una decisión sobre política.

I.2.4 SOAP

SOAP 1.1 es la Recomendación actual del Consorcio WWW (W3C, *World Wide Web Consortium)*. Se trata de un formato de mensaje que no está orientado a ningún protocolo específico. SOAP utiliza por lo general el protocolo de transferencia de hipertexto (HTTP, *hypertext transfer protocol*), aunque puede aplicar otros protocolos, como el protocolo de transferencia de correo simple (SMTP, *single mail transfer protocol*) o el protocolo de transferencia de ficheros (FTP, *file transfer protocol*). Cuando SOAP se combina con HTTP, el cortafuegos ve a SOAP como HTTP y generalmente autoriza su paso. En principio, el cortafuegos puede filtrar el protocolo SOAP, aun cuando el cortafuegos no sea consciente de dicho protocolo. Sin embargo, ese filtrado no es una tarea fácil y por consecuencia está sujeto a errores. El filtrado es difícil, ya que la criptación puede ocultar el contenido y el contexto de los datos transportados (es decir, XML), y SOAP no tiene un esquema de direccionamiento o una estructura interna uniforme, lo que quiere decir que las cabeceras y los nombres de los métodos son facultativos.

I.3 Supervisión electrónica autorizada legalmente

Los operadores de telecomunicaciones habrán de tener en cuenta las siguientes consideraciones de seguridad en cuanto a la implementación de la supervisión electrónica autorizada legalmente (LAES, *lawfully authorized electronic surveillance*).

Las prácticas de seguridad de las actividades de LAES deben ser robustas e idénticas a las que se aplicarían a cualquier NE, sistema de soporte de operaciones (OSS, *operations support system*), o MS cruciales, salvo en ciertos casos, que se enumeran más adelante. Estas prácticas guardan relación con la necesidad de mantener la confidencialidad de las actividades de LAES.

– Únicamente los empleados autorizados podrán participar en las actividades de LAES.

– La información de LAES, incluida la que versa sobre la identidad del objetivo, los organismos de aplicación de la ley participantes, el contenido de la comunicación y la información relativa a la identificación de la llamada quedarán protegidos contra su divulgación a personal no autorizado.

– Únicamente el personal autorizado tendrá acceso a las instrucciones y los procesos de LAES.

– Es necesario mantener una relación actualizada del personal autorizado para acceder, mantener, administrar y gestionar las actividades, procesos y procedimientos de LAES.

– Las actividades, políticas y procedimientos de seguridad de LAES deberán documentarse adecuadamente y ponerse a la disposición del personal autorizado.

– Los registros cronológicos y los registros de las actividades de seguridad relacionadas con LAES deberán mantenerse almacenados en una instalación segura.

– Es necesario que se aplique un proceso de documentación riguroso que permita identificar y autenticar a los organismos de aplicación de la ley y procesar las peticiones de LAES.

I.4 Consideraciones de seguridad física

Habrán de tenerse en cuenta las siguientes consideraciones a los efectos de la seguridad física. Durante la preparación de los requisitos de seguridad, la seguridad física representa un componente importante. En la mayoría de las arquitecturas de seguridad se supone que el entorno físico dispone de protección. En una época, todos los NE estaban contenidos en los edificios de las centrales locales (CO, *central office*). En estos edificios trabajaban empleados ininterrumpidamente para manejar, aprovisionar, administrar y mantener los equipos. Los empleados se conocían mutuamente y las personas extrañas no podían acceder a estos sitios sin que alguien notara su presencia y las interrogase. No obstante, hoy en día el entorno es muy distinto. Existe la tendencia a instalar equipo inalámbrico en exteriores en un entorno inseguro. Asimismo, muchas, sino la mayoría, de las oficinas centrales funcionan sin personal y a oscuras la mayor parte del tiempo. Los grupos o miembros del personal itinerantes que son enviados desde un emplazamiento central realizan las tareas de actualización y mantenimiento programadas. Actualmente, las guardas de seguridad de 24 horas y los siete días de la semana son muy excepcionales. Las oficinas centrales son utilizadas también por el personal de planta exterior como lugares convenientes de reunión y almacenamiento de herramientas y equipos. A continuación se presentan las características de un emplazamiento seguro:

– Todas las entradas y salidas del personal son registradas cronológicamente.
– Los proveedores y el personal coubicado son sometidos a investigación y su entrada/salida es registrada cronológicamente.
– El acceso físico al NE de que se trate está limitado a los empleados autorizados.
– El personal coubicado tiene la obligación de respetar los mismos requisitos de acceso que se aplican al proveedor de servicio incumbente.
– Nadie que disponga de acceso físico legítimo al edificio tendrá acceso lógico a los NE, consolas, dispositivos de acceso de red y OSS sin autenticación protegida.
– El acceso no autorizado debe ser detectado y atendido de un modo oportuno.
– Debe disponer de servicios tales como agua, energía eléctrica y telecomunicaciones.
– Los emplazamientos deben ser vigilados por personal de seguridad itinerante, sistemas de alarmas que permitan supervisar y registrar las aperturas y cierres de puertas y ventanas, detectores de movimiento, detectores de presencia por infrarrojos y supervisión de ubicaciones cruciales mediante vídeo a distancia.
– El periodo de conservación de los medios de vigilancia y de los registros cronológicos habrá de documentarse. La longitud del periodo podrá variar en función del nivel de riesgo.

En las siguientes cláusulas se da información adicional sobre la seguridad física. En las *Public Switched Network Security Assessment Guidelines*, de septiembre de 2000, del Sistema de comunicación nacional puede verse una descripción pormenorizada de los aspectos de seguridad física.

I.4.1 Seguridad de los locales

Por lo general, las organizaciones aplican diferentes niveles de control de acceso a los edificios, de conformidad con la importancia de los activos que se encuentren en el complejo. A menudo, las corporaciones grandes construirán edificios de alta seguridad independientes para instalar los componentes de red cruciales, tales como las centrales o los centros de datos. La importancia de los activos que se conservan en esos sitios determina el nivel de la seguridad. Esta determinación surge durante una fase de inventario e inspección para evaluar los activos. En las siguientes cláusulas se abordan varias cuestiones de evaluación en relación con los edificios en los que se encuentren activos cruciales o de alto valor. En el caso de edificios menos críticos se realizan inspecciones menos rigurosas. La evaluación total de la seguridad física debe permitir que se determine el nivel de protección necesario y la calidad relativa de los mecanismos de protección instalados.

I.4.1.1 Seguridad del edificio en general

Aunque normalmente se considera que las puertas y las ventanas de un edificio son los principales puntos de acceso, también habrán de considerarse otros puntos (por ejemplo, los conductos de ventilación, los puntos de entrada de agua, gas, comunicaciones y electricidad, y los conductos de desagüe), en función de los tipos de amenaza que se suscite. Hay que considerar también otros puntos de entrada, por ejemplo, los sótanos de cables de la oficina central y lugares donde exista la posibilidad de que se puedan provocar daños. Además, deberá considerarse el espacio de contención entre el público y el propio edificio. El césped, los jardines, el alumbrado y las vallas pueden contribuir al primer nivel de protección del perímetro, ya que retardan o impiden los acercamientos encubiertos. Las barreras físicas como los postes de concreto o las grandes macetas de cemento en los jardines pueden servir para impedir que se aproximen autos, camiones u otros vehículos en un posible intento destructivo. Las cámaras y otros dispositivos de vigilancia exteriores pueden mejorar aún más o extender el espacio de contención.

I.4.1.2 Guardias, cerraduras e insignias de identificación

Los guardias protegen el perímetro externo del edificio y algunas veces también las zonas internas. Para algunos edificios de importancia fundamental, la inspección debe garantizar lo siguiente:

– Todas las puertas de acceso al edificio deben estar cerradas con llave o vigiladas en todo momento.

– Cualquier puerta que no se utilice normalmente, como es el caso de las salidas de emergencia, deben estar provistas de alarmas. La inspección debe garantizar que el funcionamiento de las alarmas es óptimo y que se dispone de procedimientos para dar respuesta a las alarmas.

– Las puertas deben instalarse adecuadamente de manera que no puedan ser desmontadas desde el exterior (por ejemplo, protegiendo las bisagras y los pernos contra maniobras desde el exterior).

– Durante los periodos cresta de ingreso y egreso, debe haber guardias presentes en las entradas y salidas. Durante el resto del tiempo, las puertas deberán supervisarse y será conveniente que se instale algún otro tipo de control de acceso (por ejemplo, paso de tarjetas, tarjetas de proximidad y claves).

– Para el acceso a través de puertas no vigiladas por guardias debe aplicarse un método que exija la identificación de la persona que desea acceder.

– Las puertas no vigiladas por guardias que brindan acceso mediante claves, llaves u otros medios habrán de disponer de mecanismos que impidan que alguien venga siguiendo de cerca a la persona que se dispone a acceder[5]. Podrán utilizarse trampas de personas, las puertas giratorias y detectores para evitar "entrar pegado a otro" y para enviar una alarma que notifique que se está produciendo una situación de este tipo.

– Las calificaciones profesionales, la contratación, la formación y los métodos de retención de los guardias deben ser los adecuados. Esto reviste particular importancia en el caso de los servicios de guardias contratados, contratación que es una práctica común.

– Los empleados, los vendedores internos, los contratistas y otras personas autorizadas deben disponer de una tarjeta de identificación y llevarla en todo momento mientras permanezcan en el edificio.

– Debe proporcionarse a los visitantes que no son empleados un identificador temporal, por ejemplo un pase de visitante y se exigirá a éstos que lo lleven visiblemente.

---

5 "Entrar pegado a otro" es el acto que realiza una persona no autorizada para pasar por una puerta abierta por una persona autorizada.

– Es necesario establecer procedimientos y condiciones para que los visitantes puedan acceder y desempeñar sus actividades sin acompañante. En este contexto, habrá que estipular también las condiciones en las cuales estas personas deberán ser acompañadas.
– Las tarjetas de identificación de un empleado deben incluir una fotografía en color y lo suficientemente grande para que el empleado no tenga necesidad de entregar su tarjeta a un guardia para que éste la inspeccione. La fabricación de la tarjeta debe ser tal que no pueda alterarse o sustituirse la fotografía. La fotografía habrá de ser lo suficientemente clara de modo que el guardia pueda compararla con el rostro de su portador.
– En la tarjeta constarán, escritos con claridad, el nombre del empleado y cualquier otra información que facilite su identificación (por ejemplo, número, código de barras).
– La tarjeta deberá contar con una marca o indicación que permita distinguir a los empleados de los visitantes que accedan a los edificios.
– La tarjeta debe ser duradera y lo más resistente al uso, daño o alteración posible.
– La tarjeta habrá de contener la información electrónica o magnética que requieran los lectores de tarjetas.
– La tarjeta podrá incluir un circuito integrado inteligente que contenga información adicional, tal como datos biométricos o certificados X.509.
– Los sistemas de autenticación y autorización de tarjetas deben estar comunicados a un directorio de seguridad centralizado que permita modificar o suprimir inmediatamente los privilegios de acceso.
– La tarjeta debe disponer de capacidad para limitar, en caso necesario, el acceso a determinadas zonas del complejo de la empresa.
– En la tarjeta debe figurar una dirección para que, en caso de pérdida y si la encuentra alguien no empleado en la empresa, pueda enviarla por correo sin necesidad de franqueo.
– Para garantizar la seguridad de la empresa o del edificio podrá inhabilitarse o invalidarse cualquier tarjeta perdida o cuyo portador no esté autorizado ya a acceder al edificio o al complejo de la empresa.
– Cuando el portador deje de ser empleado, alguien (gestor, guardia del edificio, seguridad corporativa) deberá retener o destruir su tarjeta para que no pueda ser utilizada ilícitamente.

Los guardias no son el único personal encargado de preservar la seguridad interna de un edificio, ya que, a menudo, los ocupantes autorizados acrecientan la seguridad de un edificio desempeñando actividades de vigilancia y supervisión pasiva. La evaluación debe permitir determinar si el personal ha sido autorizado a interrogar a una persona no autorizada en las zonas controladas. Una prueba de penetración puede ser útil para determinar el grado de formación que han recibido los guardias y los empleados respecto a la importancia de la seguridad física. Los inspectores pueden intentar colarse o pasar de rondón engañando a los guardias, o sonsacar a empleados a fin de entrar por una puerta no vigilada.

I.4.1.3 Administración de llaves físicas y claves lógicas

En edificios de importancia no es común utilizar las llaves físicas tradicionales ya que su inventario y recuperación es difícil y, además, no permiten efectuar un registro de auditoría del usuario. A menudo, el empleo de llaves físicas se limita al acceso a ciertas partes internas del edificio, tales como almacenes, salas custodiadas y armarios de cables. No obstante, aún es común encontrar empresas e instalaciones en que se emplean las cerraduras con llave como medio principal para ingresar a los edificios o acceder a zonas cruciales dentro de los mismos. Cuando éste sea el caso, habrá que considerar las siguientes medidas:

– Aplicar procedimientos para autorizar la distribución de las llaves a particulares, lo que incluye el control de las llaves y el registro del acceso y la distribución de llaves.

– Numerar cada llave.
– Mantener y auditar un inventario completo de las llaves y de sus propietarios.
– Establecer criterios para sustituir las cerraduras cuando se pierden las llaves.
– Exigir auditorías periódicas del inventario de llaves y establecer procedimientos para conciliar las discrepancias.
– Definir procedimientos para recuperar las llaves cuando ya no se justifique el acceso o cuando se modifiquen las autorizaciones.

Los procedimientos de clave lógica (por ejemplo, tarjetas de proximidad) deben ser evaluados conforme a los mismos criterios. Los procedimientos de recuperación de claves, registro de ingreso y salida y de autorización quedan simplificados si se utilizan claves lógicas debido a que estos sistemas disponen de facilidades centralizadas para supervisar su utilización, la asignación de autorización y la inhabilitación de claves. En todo caso, habrá que establecer procedimientos para garantizar que las personas encargadas de mantener el inventario de claves y la base de datos de las autorizaciones sean notificadas cuando salgan personas o se modifiquen sus requisitos de acceso. Las cerraduras de combinación son un caso especial de las cerraduras lógicas y deben evaluarse para garantizar que las combinaciones no puedan reconocerse recurriendo a patrones de uso o anotando combinaciones. Las combinaciones deben modificarse si cambian las autorizaciones de acceso.

I.4.1.4 Separación funcional de las instalaciones y control de acceso en múltiples niveles

La seguridad física se aplica no sólo a las partes internas de un edificio sino también al perímetro externo. El acceso a las zonas internas consideradas como sensibles o de funcionamiento crucial debe controlarse cuando el acceso a los contenidos esté limitado por cualquier motivo (por ejemplo, porque contienen datos sensibles, experimentos o equipos). En general:

– Las instalaciones de computadoras y las redes informáticas esenciales deben ubicarse en zonas que dispongan de mecanismos de control de acceso físico independientes. El acceso debe concederse únicamente a las personas que así lo requieren.
– Es necesario establecer procedimientos para garantizar que la información patentada se mantenga en lugares seguros cuando no está siendo utilizada. Las oficinas y los archivos donde se conserve dicho material rutinariamente debe cerrarse con llave, y otro tanto cabe decir de los gabinetes en los que se mantenga información patentada.
– Todos los posibles puntos de acceso a las instalaciones de computadoras y las redes informáticas cruciales (por ejemplo, consolas, centros de operación) habrán de controlarse de manera acorde con el control obligatorio de la propia instalación.
– Es necesario mantener un registro de acceso a todos los espacios controlados.
– Los medios de almacenamiento que contengan información crucial deben utilizar encriptación o mantenerse en zonas de acceso limitado cerradas con llave.
– La dirección física de un sistema de importancia fundamental no debe divulgarse a personas que no tengan necesidad de conocerla.

El control de las zonas internas de un edificio podrá mejorarse estableciendo papeles y responsabilidades separadas. Por ejemplo, el personal administrativo no necesita acceder a las salas de computadoras de la organización. Asimismo, por lo general los ingenieros no requieren acceder al cuarto de control de documentos. La inspección mencionada debe permitir evaluar si la separación de funciones existente es la apropiada. Además, pueden emplearse dobles llaves de entrada o cerraduras de combinación si el grado de riesgo así lo exige.

I.4.2 Servicios del edificio

Las operaciones de una organización dependen crucialmente de la disponibilidad de algunos servicios, tales como el agua, la energía eléctrica, las telecomunicaciones y el retiro de los desperdicios.

I.4.2.1 Servicios públicos (agua, energía eléctrica, telecomunicaciones y gestión de los desperdicios)

Una organización no podría funcionar de manera eficaz o en modo alguno sin los servicios de agua, energía eléctrica, telecomunicaciones y el retiro de los desperdicios. La dependencia respecto a estos servicios suele subestimarse. En la inspección mencionada hay que evaluar la reacción prevista por la organización ante la interrupción de dichos servicios. Por lo que se refiere a los servicios cruciales que permiten que una empresa siga funcionando, deben considerarse los siguientes puntos esenciales:

– Las líneas de alimentación de energía deben duplicarse y separarse geográficamente para evitar la pérdida accidental de la alimentación eléctrica.
– Hay que disponer de una fuente de suministro eléctrico de emergencia que permita seguir funcionando por mayor tiempo que la duración media de las interrupciones de suministro. Además, debe disponerse de capacidad para generar energía eléctrica antes de que se agote el suministro de emergencia. (Pueden arrendarse generadores móviles.)
– Es necesario disponer de suficiente capacidad *in situ* de almacenamiento de agua (o de servicios de suministro) para permitir que sigan funcionando los componentes cruciales de la instalación.
– Es necesario respaldar con recursos de reserva o activos las comunicaciones con el exterior. En caso contrario, los sistemas de comunicación deben ser lo suficientemente robustos como para funcionar en caso de crisis y otro tanto cabe decir de las comunicaciones internas. La capacidad debe ser suficiente para manejar el tráfico de nivel de crisis.
– Las instalaciones sanitarias y de tratamiento de aguas residuales deben funcionar bien en caso de crisis, o habrá que establecer instalaciones temporales (al menos contractualmente) que se puedan activar rápidamente.
– Los sistemas de aire acondicionado de las salas de cómputo y de otras zonas que requieran entornos controlados deben quedar respaldados para evitar los fallos de las máquinas o los daños provocados por sobrecalentamiento.
– Es necesario disponer fácilmente de contenedores cerrados con llave para destruir y deshacerse de información patentada, siempre que se maneje ese tipo de información. La inspección deberá permitir rastrear el trayecto seguido para deshacerse de dicho material a fin de garantizar que se cumplió con el cometido.

A los efectos de la evaluación conviene distribuir estos servicios dentro de los edificios. Esta actividad debe permitir evaluar la resistencia general de la instalación a las interrupciones del servicio desde su origen en las instalaciones del proveedor de servicio hasta los trayectos de distribución dentro del edificio.

I.4.2.2 Instalaciones de emergencia

La inspección debe permitir la evaluación de la idoneidad de las instalaciones de emergencia, tales como los sistemas de detección y supresión de incendios, de acondicionamiento de energía eléctrica, de aire acondicionado, de ventilación y de protección del medio ambiente, que requiere el funcionamiento continuo de los sistemas fundamentales. Estos sistemas deben reaccionar de tal modo que permitan que:

– El personal pueda evacuar las instalaciones.

– El equipo esté debidamente protegido (al menos el tiempo suficiente para que los bomberos u otros servicios de socorro puedan acudir).
– Las instalaciones mantengan su integridad estructural.
– Los contenidos del edificio queden protegidos en la medida de lo posible contra el entorno exterior.

Las instalaciones de emergencia revisten importancia tanto durante el periodo subsiguiente a la infracción de la seguridad como en los casos de accidentes y de catástrofes naturales, como se indicó en la cláusula anterior.

I.4.2.3 Redundancia del transporte de las comunicaciones y protección física de las instalaciones fundamentales

Las instalaciones de los sistemas de cómputo y de las comunicaciones fundamentales deberán distribuirse geográficamente en la medida de lo posible sin afectar demasiado los costos de operación, la calidad de funcionamiento y la seguridad. Además, el encaminamiento de los enlaces de comunicación esenciales (por ejemplo, importantes troncales entre las oficinas y enlaces de señalización) deberían duplicarse y distribuirse geográficamente dentro y fuera de las instalaciones, de modo que las comunicaciones puedan ser reencaminadas inmediatamente por distintas rutas físicas de respaldo cuando resulte necesario. Las redes de comunicaciones necesarias para mantener el servicio deben concebirse de tal forma que un solo punto de fallo no dé lugar a una interrupción grave o generalizada.

I.4.3 Amenazas geográficas y al entorno

Los sitios cruciales deben ser inspeccionados para identificar cualquier riesgo que resulte de su ubicación en zonas con probabilidad de que sobrevengan catástrofes naturales, accidentes graves (por ejemplo, derrames químicos y explosiones de las líneas de gas), interrupciones del suministro eléctrico y problemas conexos. En la inspección habrá que tener en cuenta los efectos de aspectos simples del entorno, como calor o frío extremos, daños producidos por sales y contaminantes, y condiciones climáticas adversas.

Las cuestiones geográficas incluyen las reacciones de los habitantes locales; entre otras, actos de hostilidad, capacidad de respuesta de los servicios de emergencia locales y nivel de seguridad previsto para el personal, tanto en su lugar de trabajo como en camino a las instalaciones. Dado que las actividades y las motivaciones humanas cambian con el tiempo como resultado del descontento, los problemas políticos, las opiniones religiosas y otros factores, las inspecciones deben repetirse periódicamente conforme a un programa predeterminado. Aunque a menudo es impráctico abandonar las instalaciones cuando existe este tipo de riesgos, puede convenir duplicar o reubicar los sistemas y los recursos cruciales alojados en instalaciones de alto riesgo.

Sería útil diseñar planes de continuidad comercial y de recuperación en casos de catástrofe en cuyo marco se aborden las actuaciones que puedan suscitar los eventos provocados por estas amenazas y problemas. Los planes deben incluir procedimientos de instrucciones, control y comunicaciones que habrá que probar regularmente. Los planes de restablecimiento de las actividades deben incluir también disposiciones y contratos que puedan ejecutarse rápidamente en respuesta a incidentes provocados por materiales peligrosos (HAZMAT, *hazardous material*). En los planes se tendrá en cuenta que el restablecimiento completo a un entorno seguro podría impedir el acceso normal a las instalaciones por un periodo prolongado. Los posibles remedios pueden exigir reubicar a una instalación de apoyo o la disponibilidad de personal formado y equipado para manejar materiales peligrosos a fin de hacer posible que entretanto funcionen las instalaciones.

I.4.4 Procedimientos de coubicación

La coubicación se remite a la situación que prevalece cuando las instalaciones de diferentes proveedores se encuentran en el mismo lugar. A los fines de las inspecciones de seguridad física

reviste particular importancia tomar en consideración que proporcionar acceso a múltiples proveedores a menudo significa que los competidores (algunas veces varios de ellos) tendrán que acceder a los componentes e instalaciones físicas del proveedor anfitrión. En la inspección debe considerarse que:

– Hay que aislar mediante barreras físicas el equipo indispensable; sin embargo, el personal coubicado debe quedar sujeto a los mismos requisitos de acceso que el personal del proveedor de servicio tradicional.
– Han de establecerse procedimientos para la distribución de claves o llaves, la contabilidad y la auditoría. Deben establecerse procesos para garantizar que los cambios del personal puedan ser supervisados en todas las empresas coubicadas.
– El equipo y las instalaciones cruciales no deben atraer la atención. El método tradicional de marcar claramente las instalaciones de equipos y de medios de transporte como cruciales (denominado "bloqueo de nivel rojo"[6]) en un entorno abierto es un peligro potencial que debe evitarse.

I.5 Proceso de desarrollo

I.5.1 Programa inicial, instalación y modos de fallo

Las siguientes consideraciones deben tenerse en cuenta tratándose de los procedimientos de seguridad referentes al programa inicial, la instalación y el modo de fallo.

Es indispensable desplegar distintos esfuerzos para garantizar la implementación desde una "nueva instalación" a lo largo de su vida útil. Para abordar estas cuestiones importa comenzar entendiendo las amenazas con que tropieza una implementación. Estas amenazas se señalan en la Norma ANSI T1.233-2004, *Operations, Administration, Maintenance, and Provisioning – Security framework for Telecommunications Management Network Interfaces*, y en la Norma ISO/CEI 10181, *Open Systems Interconnection – Security frameworks for open systems*. La conectividad generalizada a los sistemas abiertos hace aumentar las amenazas, por ejemplo:

– virus en las rutinas de inicialización;
– acceso no autorizado;
– impostura;
– amenazas a la integridad de los datos;
– amenazas a la confidencialidad;
– denegación de servicio (DoS, *denial of service*); y
– rechazo.

I.5.2 Proceso de corrección de las rutinas

Los proveedores de servicio contratan vendedores que desarrollan y suministran una aplicación y una plataforma en la que se instala la aplicación, o únicamente el soporte lógico de la aplicación. En este último caso, los proveedores instalan el soporte lógico en una plataforma adquirida previamente.

Los vendedores desarrollan correcciones de las rutinas que permiten remediar o modificar sistemas operativos (OS, *operating system*) o soporte lógico de aplicación, o ambos, entre las versiones generales. Tras las pruebas apropiadas, la corrección se hace pública y se pone a disposición del proveedor de servicio. En algunos casos, un vendedor de soporte lógico de aplicación puede hacer

---

6 El bloqueo de nivel rojo permite poner sobre aviso al personal de apoyo de que el circuito es particularmente importante y hay que estar atento a no perturbarlo accidentalmente.

públicas las correcciones en "grupos", incluso con cierta regularidad contractual. Es bastante común publicar versiones semestrales.

Una corrección de OS por lo general no debe afectar el modo de funcionamiento de la aplicación; sin embargo, éste no es siempre el caso. Por consiguiente, cuando un vendedor de plataformas hace pública una corrección de OS, queda a cargo del proveedor verificar ante el vendedor de la aplicación que la corrección de OS liberada no afecte adversamente el funcionamiento de la aplicación.

En caso de que un vendedor de aplicaciones suministre tanto la aplicación como la plataforma de soporte físico, aunque no se trate de un vendedor de equipo original (OEM, *original equipment manufacturer*) para la plataforma, y el OEM de la plataforma haga pública una corrección de rutinas de seguridad de OS, el vendedor de la aplicación y el proveedor de servicio deben estar al tanto de que está disponible dicha corrección de rutinas de seguridad y adoptar las disposiciones necesarias para probarla oportunamente, a fin de verificar que dicha corrección no afecte adversamente la aplicación.

El vendedor de la aplicación debe asignar una prioridad para examinar la introducción de las correcciones de rutinas de seguridad (en cuestión de semanas y no de meses). Por consiguiente, habrá de establecerse un proceso ordinario de manera que cuando un proveedor notifique al vendedor de la aplicación un problema relativo a una corrección de rutinas de seguridad, el vendedor adoptará rápidamente la medida del caso. Además, el vendedor debe garantizar que la instalación de la corrección de rutinas no afecte las correcciones de rutinas de seguridad instaladas anteriormente.

Si la prueba de la corrección de rutinas de seguridad incide en una aplicación, habrán de tomarse oportunamente las medidas correctivas adecuadas para identificar el problema y formular planes para corregir la condición que provoca el fallo de la aplicación, y aplicar ulteriormente la corrección de las rutinas de seguridad.

Las siguientes consideraciones de seguridad han de tenerse en cuenta cuando se instalen correcciones de rutinas respecto al OS o al soporte lógico de la aplicación.

- Los vendedores de equipos o los integradores de sistemas deben suministrar manuales de referencia de seguridad y de formación para los administradores, que incluyan funciones y procedimientos detallados de seguridad del OS y de la aplicación y los procedimientos de acceso de usuario.
- Es necesario verificar que las correcciones de rutinas respecto a seguridad del OS y las demás correcciones de rutinas sean compatibles con las aplicaciones del NE y del MS.
- Soporte lógico del OS: sólo deben aplicarse correcciones de rutinas aprobadas por un OEM a un elemento de red operacional o a un sistema operativo de plataforma de gestión.
- Soporte lógico de aplicación de gestión: en una aplicación de gestión operacional sólo deben instalarse correcciones de rutinas aprobadas por un vendedor original de aplicaciones de gestión.
- Las correcciones de rutinas de gran repercusión deberán distribuirse oportunamente y no quedar limitadas por los procesos de divulgación periódica de las correcciones de rutinas.
- Todas las telecargas en sentido descendente o ascendente de cualquier soporte lógico o de datos de configuración deben quedar aseguradas mediante autenticación fuerte del origen de los datos y protección resistente de la integridad. Lo ideal sería que ambas medidas de seguridad fueran suministradas gracias a la firma digital del proveedor del soporte lógico. Además, el proveedor del soporte lógico puede elegir la utilización de criptación del soporte lógico o de los datos de configuración.
- En el momento de entrega debería proporcionarse una descripción del procedimiento o procedimientos para obtener e incorporar las correcciones de rutinas de seguridad más

recientes para el sistema y el soporte lógico de aplicación que se utiliza dentro de cada elemento.

– En el momento de entrega debe proporcionarse una descripción del proceso de prueba de cada corrección de rutinas de seguridad, antes de que se autorice su entrega al proveedor de servicio.
– En el momento de entrega debe especificarse el nivel de compatibilidad con versiones anteriores del soporte lógico del sistema y de las correcciones de las rutinas de mantenimiento de seguridad.
– El soporte lógico del sistema o un proceso deben permitir el rastreo de las correcciones de rutinas y de las actualizaciones aplicadas. El estado de las actualizaciones y las correcciones de rutinas deben ser objeto de auditoría.

I.5.3 Seguridad durante el ciclo de vida del desarrollo

La seguridad de un producto o servicio depende del proceso de todo su ciclo de vida. La seguridad es un factor importante durante el diseño conceptual y lo sigue siendo durante el diseño detallado, el desarrollo, la instalación y la supresión de un producto. En el caso de productos o servicios que tratan información sensible, puede ser necesario que la seguridad continúe más allá de la supresión del producto o servicio de que se trate. Realizar la prueba y los controles apropiados durante el ciclo completo de vida útil es indispensable si se desea proporcionar niveles aceptables de seguridad.

I.5.3.1 Gestión del personal

La honradez del personal es un factor fundamental de la seguridad que a menudo se pasa por alto. Todo personal que tenga acceso al diseño, desarrollo y prueba debe ser honrado.

– Deben verificarse los antecedentes del personal, los contratistas, los subcontratistas, los consultores y los empleados que participan en el desarrollo y la prueba de componentes de soporte lógico cruciales.

I.5.3.2 Formación y sensibilización sobre la seguridad

El personal debe ser sensibilizado respecto a las políticas y los procedimientos de seguridad y la necesidad de proteger los recursos de información. El eslabón más frágil de la seguridad es a menudo el personal que interviene. La sensibilización y la formación sobre la seguridad fortalecen en grado sumamente apreciable el eslabón más débil. La sensibilización reduce el número de acciones no autorizadas por parte del personal, aumenta la eficacia de los controles de protección, y ayuda a evitar el fraude, el despilfarro y el abuso de los recursos de computación.

– Debe impartirse formación y sensibilización en materia de seguridad a todo el personal, incluidos los contratistas, subcontratistas, consultores y empleados.

I.5.3.3 Gestión de riesgo

La gestión de riesgo es un factor esencial de la seguridad de la información y está integrada por la identificación, análisis, control y reducción al mínimo de la pérdida asociada con un "evento". Las principales etapas en la identificación de un riesgo son, entre otras, la identificación de las auténticas amenazas, las consecuencias de una amenaza cumplida, la posible frecuencia de la ocurrencia de una amenaza y la posibilidad de una amenaza cumplida. La gestión del riesgo no sólo entraña un análisis del riesgo y un análisis de costo-beneficio de las protecciones, sino también la aplicación, la inspección y el mantenimiento de la protección.

Un análisis de riesgo permite identificar los riesgos y justifica el costo-beneficio de las medidas de reacción necesarias. Esta información puede emplearse para contribuir al proceso de toma de decisión en todas las fases del ciclo de vida útil, incluyendo la selección del sitio, el diseño del edificio y las decisiones de construcción. Para determinar si se ha garantizado una salvaguarda, se determina la pérdida anualizada prevista (ALE, *annualized loss expectancy*). La (ALE antes de la

implementación de la salvaguarda) – (la ALE tras la implementación de la salvaguarda) = valor de salvaguarda. Obsérvese que la implementación de la salvaguarda debería incluir el costo anual de explotación y mantenimiento.

– Para cada nuevo producto o servicio debería llevarse a cabo un análisis de riesgo. Este análisis habría de incluir la preparación de documento oficial en el que se describa el método utilizado y los resultados del análisis. Como mínimo, el informe debería permitir identificar todos los datos accesibles y del propietario de los datos (es decir, corporación, proveedor de servicios de Internet), cuantificar o calificar el valor de los datos o del servicio en riesgo y determinar las posibles repercusiones de las amenazas en sentido ascendente y descendente para los NE o los OSS.

I.5.3.4 Requisitos

– Durante la fase de recopilación de requisitos del producto o servicio deben documentarse los requisitos de seguridad.

I.5.3.5 Diseño

– Durante la fase de diseño deben abordarse los requisitos de seguridad y no añadirse una vez iniciado el desarrollo.

– Para localizar las imperfecciones del diseño que pueden afectar la seguridad debe inspeccionarse el diseño de seguridad.

– Todos los puntos de acceso al sistema habrán de documentarse apropiadamente y soportar la identificación y la autenticación.

– NO deberán autorizarse las puertas traseras o las trampas de mantenimiento que violen la política de seguridad.

I.5.3.6 Separación de tareas

Las funciones inofensivas en un entorno de confianza pueden suscitar una vulnerabilidad en cuanto a la seguridad si se desempeñan en entornos no fiables. Así, aunque se ha diseñado un interpretador del lenguaje de descripción de página para ver documentos, un documento que no inspire confianza podría utilizar las funciones que contiene ese interpretador de forma malintencionada, para realizar copias o suprimir ficheros.

– El sistema debería soportar como mínimo tres niveles de usuario: usuario, administrador/operador de sistema y administrador de seguridad.

– Cada función debería tener el nivel mínimo de privilegios necesarios para desarrollar su función de trabajo.

I.5.3.7 Implementación

– Los recursos reutilizados deben purgarse de toda información (es decir, ficheros, memoria y almacenamiento temporal) antes de ser aplicados nuevamente.

– Los conceptores han de seguir las mejores prácticas para asegurar los programas (es decir, gestionar las memorias intermedias para que no puedan saturarse).

– Conviene realizar auditorías periódicas de seguridad en los entornos de desarrollo, prueba y soporte.

– Los entornos de desarrollo no deben utilizarse para realizar actividades comerciales que no pertenezcan a la empresa considerada.

– El soporte lógico de dominio público no debe importarse, utilizarse o distribuirse para ser empleado en sistemas de desarrollo, de prueba o de soporte, a menos de que esté disponible en código fuente inspeccionado para detectar si el código es malicioso.

I.5.3.8 Documentación

– La documentación ha de incluir marcas patentadas, cuando proceda.

– En la documentación de usuario final deberá describirse la funcionalidad de seguridad que no sea transparente para el usuario, explicando su función e incluyendo las directrices de utilización.

– El manual del administrador del sistema incluirá lo siguiente:

  • Advertencias sobre las funciones y privilegios que deben controlarse durante el funcionamiento en modo seguro.

  • Documentación de la utilización de las funciones de auditoría.

  • Procedimientos para examinar y mantener los registros cronológicos de auditoría.

  • Estructuras pormenorizadas de los registros cronológicos de auditoría.

  • Procedimientos para el respaldo y la supresión de registros cronológicos de auditoría.

  • Procedimientos para verificar la cantidad de espacio disponible para los registros cronológicos de auditoría.

I.5.3.9 Sistema operativo

El OS debe estar en condiciones de controlar de manera eficaz el soporte físico y el soporte lógico a fin de proteger adecuadamente el valor de los datos y los recursos que se están gestionando. Por lo que hace a la arquitectura de seguridad propuesta, se supone que el OS proporcionará el nivel de seguridad necesario para los datos y recursos que se están gestionando. Esta suposición debe examinarse en función de las necesidades específicas del proveedor de servicio. Si el OS no puede satisfacer las necesidades de seguridad del proveedor de servicio, el soporte lógico tendrá que ser trasladado a otro OS que soporte altos niveles de seguridad.

– El OS debe contar con las correspondientes correcciones de rutinas de seguridad.

– El OS habrá de configurarse de modo seguro y entregarse con una configuración de privilegios restringidos de acceso de seguridad. Existen varios documentos y sitios web en los que se examina la seguridad del OS. Aunque queda fuera del alcance de esta Recomendación enumerar todos los posibles ejemplos, algunos incluyen los criterios comunes y los perfiles de protección del OS. [7, 8, 9]

– Para el funcionamiento por defecto sólo se habilitará el mínimo de servicios necesario.

I.5.3.10 Ingeniería del soporte lógico

La seguridad forma parte integral de la ingeniería del soporte lógico. Para desarrollar un producto de seguridad, deben utilizarse técnicas de programación y protocolos seguros. Las técnicas de programación que no son seguras pueden contrarrestar los mejores mecanismos y protocolos de seguridad. Por ejemplo, si un programador no gestiona las memorias intermedias adecuadamente, podría saturarse una de ellas y otorgar a un usuario más privilegios de los que correspondan.

– Los vendedores deberían seguir los procesos formales de desarrollo documentado, tales como el modelo de madurez de capacidades concebido por el Instituto de Ingeniería de

---

[7] El criterio común se está convirtiendo en una norma reconocida internacionalmente para la evaluación formal de la seguridad (http://www.commoncriteria.org/).

[8] Perfiles de protección del sistema operativo del Foro Marco técnico de la seguridad de la información, http://www.iatf.net/protection_profiles/operating_systems.cfm

[9] Centro de recursos de seguridad informática, Instituto Nacional de Normas y Tecnología, http://csrc.nist.gov/

soporte lógico. Durante las etapas de diseño, desarrollo, prueba y distribución del soporte lógico habrán de seguirse las mejores prácticas de programación segura.

I.5.3.11 Disponibilidad y calidad de funcionamiento

La disponibilidad y la calidad de funcionamiento forman parte integral de los sistemas seguros. La calidad de funcionamiento puede degradarse hasta un punto en el que ya resulte imposible utilizar el sistema.

– El diseño, el desarrollo y la aplicación deberían contribuir a disminuir al mínimo los efectos de un ataque tipo DoS.
– El diseño, el desarrollo y la aplicación deberían garantizar una gran disponibilidad.
– La arquitectura y la aplicación de la red no deberían tener un solo punto de fallo.

I.5.3.12 Soporte lógico del sistema

El soporte lógico utilizado para hacer funcionar y mantener los sistemas informáticos (OS, utilidades y MS) deberá poder ser configurado y mantenido de forma segura. Es necesario realizar las pruebas que permitan garantizar que los componentes y las características de seguridad se han aplicado de manera robusta y configurado correctamente.

– El soporte lógico del sistema y los productos de soporte físico intermedios deben instalarse y configurarse de forma segura, lo que incluye la instalación de las correcciones de rutinas de seguridad. El soporte lógico debe entregarse con una configuración de privilegios restringidos de acceso de seguridad.

I.5.3.13 Transmisión

– A criterio del proveedor de servicio, podrá ser utilizada la opción de transmisiones seguras de datos. Las opciones de transmisión segura deben estar disponibles para las modalidades de cliente a servidor y de sistema a sistema.

I.5.3.14 Almacenamiento seguro

– Conviene que se ofrezcan opciones que serán configuradas por el proveedor de servicio para el almacenamiento seguro de los datos. Es necesario que el proveedor de servicio pueda especificar qué campos se almacenan de forma segura.

I.5.3.15 Seguridad del soporte lógico

La seguridad del soporte lógico deberá abordarse desde dos perspectivas: prueba de las características de seguridad y prueba de las posibles violaciones a la política de seguridad.

– Las tareas habrán de dividirse entre los grupos de desarrollo del soporte lógico y los de prueba del soporte lógico.
– Deben documentarse un plan de prueba de seguridad, los procedimientos de prueba y los resultados correspondientes.
– Todas las características de seguridad deben comprobarse.
– Las pruebas deben incluir los intentos para localizar las violaciones de la política de seguridad (es decir, vulnerabilidades tales como el control de acceso).
– Como parte de la prueba, las verificaciones han de realizarse de forma tal que el sistema o aplicación recientemente desarrollados no vulnere las estructuras, redes comunes y sistemas existentes.
– Hay que verificar las técnicas de programación segura. La verificación puede realizarse a través de inspecciones del código o de herramientas de soporte lógico.
– Todas las imperfecciones de seguridad deben ser corregidas, suprimidas o neutralizadas, tras lo cual habrá que probar una vez más el sistema.

I.5.3.16 Empaque y entrega

A lo largo de la vida útil de un producto, debe utilizarse un sistema de gestión de configuración de soporte lógico que permita mantener el control de las modificaciones al código fuente y a la documentación.

- Los conceptores no deben encargarse de mantener el sistema de gestión de configuración del soporte lógico.
- Los conceptores no deben tener acceso a los sistemas de producción, salvo cuando se adopten disposiciones de emergencia controladas, debidamente aprobadas y registradas cronológicamente.
- Debe añadirse únicamente código y modificaciones de código autorizados a la línea básica de productos fuente que pueden suministrarse.
- Todas las modificaciones deben documentarse y examinarse.
- Es necesario disponer de herramientas y procedimientos para generar una nueva versión del sistema a partir del código fuente.
- Es preciso que existan herramientas y procedimientos para proteger el código fuente contra modificaciones no autorizadas.
- Es necesario que existan herramientas y procedimientos para verificar las apropiadas versiones y niveles de los módulos fuente de los componentes, si los hubiere.
- El producto debe incorporar mecanismos que posibiliten verificar la compatibilidad entre el soporte lógico instalado y el soporte lógico entregado (es decir, verificar que no se hayan realizado modificaciones no autorizadas).
- Cuando se disponga de una herramienta de exploración mecanizada, deberá realizarse una exploración de vulnerabilidad tras las actualizaciones u otras modificaciones significativas al OS o al soporte lógico de la aplicación.
- La reparación de imperfecciones de seguridad o "arreglos" debe aplicarse oportunamente acorde y a la vista de cuál sea la amenaza.
- Deberá disponerse de una base de datos maestra que contenga copias de todo el soporte lógico entregado. El soporte lógico dispondrá de un número de versión y de las especificaciones correspondientes al OS y soporte físico apropiados.

I.5.3.17 Instalación, configuración y funcionamiento de la seguridad

- Deben definirse parámetros de configuración de seguridad para el soporte lógico.
- Deben definirse y documentarse los procedimientos de las operaciones de seguridad en relación con el soporte lógico.
- Todas las intervenciones de soporte a distancia para el soporte lógico deben llevarse a cabo en forma segura.
- Todos los ID de usuario por defecto que se entreguen con el sistema deben encontrarse en un estado inactivo y que exija una medida explícita del administrador/instalador del soporte lógico, para que dichos ID puedan ser utilizados.
- Todos los procesos de instalación deben ser seguros y no depender de relaciones de confianza (es decir, unidades de disco compartidas).

Apéndice II

Marco y directrices de diseño

II.1 Marco y modelo

En el contexto de esta Recomendación, asegurar algo significa protegerlo (es decir, se trate de computadoras, redes, datos u otros recursos) contra el acceso, el uso o las actividades no autorizados. La pérdida de datos, denegación de servicio (DoS) y el hurto del servicio son ejemplos de los resultados de incidentes de seguridad. Los administradores del sistema y de la red tienen obligación de proteger los sistemas y sus elementos componentes contra usuarios internos y externos y contra los atacantes. Pese a que la seguridad es multifacética (abarca las operaciones, los equipos, las comunicaciones, el tratamiento de datos y el personal), lo que preocupa en este caso son los problemas de seguridad provocados por la debilidad inherente a las configuraciones y la tecnología comúnmente empleadas. Entre las amenazas cabe citar la divulgación, la utilización no autorizada, las modificaciones de elementos de información y la negación del servicio. En el cuadro II.1 se enumeran algunas de las amenazas contra la seguridad.

Cuadro II.1/M.3016.1 – Amenazas

Categoría de las amenazas (nota)	Ejemplos de amenazas
Acceso no autorizado	Introducción indebida Acceso a sistema no autorizado para realizar ataques Hurto de servicio
Impostura	Reproducción de sesión Secuestro de sesión Ataques mediante intermediario
Amenazas contra la integridad del sistema	Manipulación no autorizada de ficheros de configuración del sistema Manipulación no autorizada de datos del sistema
Amenazas contra la integridad de la comunicación	Manipulación no autorizada de los datos en tránsito
Amenazas contra la confidencialidad	Escucha clandestina Grabación y divulgación de la sesión Violaciones de la privacidad
Denegación de servicio	Inundación SYN del protocolo de control de transmisión Ataques mediante paquetes deformes DoS distribuida
NOTA – Categorías derivadas de la Norma T1.233-1993 (R1999) del Instituto Nacional de Normas de los Estados Unidos, sobre *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces* y de la Norma 7498-2: 1989 de la Organización Internacional de Normalización (ISO) sobre *Sistemas de Tratamiento de Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.	

Estas amenazas contra la seguridad pueden reducirse a un mínimo o mitigarse dentro de un sistema de red, una plataforma de NE o una aplicación, si se incluyen servicios de seguridad (como los definidos en la Norma ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.) para exigir el cumplimiento de:

– Identificación y **autenticación**.
– Autorización y nivel de **control de acceso**.
– Integridad de los datos.
– Privacidad y confidencialidad.
– No rechazo.

En la presente Recomendación se aborda la seguridad en el plano de gestión, es decir, las características de seguridad que permiten garantizar que la red podrá ser administrada y gestionada de una forma segura. Con todo, pese a haber seguido las recomendaciones de esta Recomendación, aún puede subsistir cierta vulnerabilidad. Los riesgos que se señalan a continuación figuran entre los que pueden poner en peligro el plano de gestión:

– Acciones improcedentes iniciadas por usuarios no autorizados o atacantes. Estas acciones pueden ser malevolentes o accidentales.
– Puenteo de la seguridad del plano de control (por ejemplo, protocolos de señalización, encaminamiento, denominación y descubrimiento).
– Los efectos de las vulnerabilidades en protocolos específicos.
– Soporte lógico maligno (por ejemplo, virus, caballos de Troya, gusanos y otros tipos de código incorporado). Cuando el soporte lógico maligno logra poner en riesgo cualquier NE/MS, podrá utilizar los enlaces de comunicación por la red segura para llevar a cabo ataques a otros componentes NE/MS. Estos ataques continuarán hasta que los gestores de la red los detecten y adopten las medidas necesarias para eliminarlos.

Esta Recomendación trata de la seguridad del tráfico de gestión, especialmente cuando dicho tráfico atraviesa redes en las que se mezcla con el tráfico de usuario de extremo. En la figura II.1 se ilustra un modelo de referencia que puede aprovecharse para especificar soluciones de seguridad de la gestión de la red. Este modelo sirve para examinar trayectos de comunicación lógica en toda la red y cuantificar los protocolos que se emplean para comunicaciones en cada trayecto. Al utilizar este modelo, cabe examinar en cada trayecto, las amenazas y vulnerabilidades, y podrán aplicarse los mecanismos de seguridad que correspondan.

Los NE de diversos vendedores se indican en la parte inferior del modelo representado en la figura II.1. Los sistemas de gestión de elementos (EMS, *element management system*) que proporcionan funciones de gestión específicas para el NE particular se ilustran encima del NE. El sistema de gestión de red (NMS, *network management system*) se representa en la parte superior del modelo. El NMS se encarga de la gestión general del NE y del EMS, y contiene las aplicaciones específicas de gestión de servicio y de gestión comercial, como los sistemas de configuración y de facturación. En el modelo también se indican los operadores distantes y locales, y los trayectos de comunicación se señalan junto con los elementos del sistema restantes.

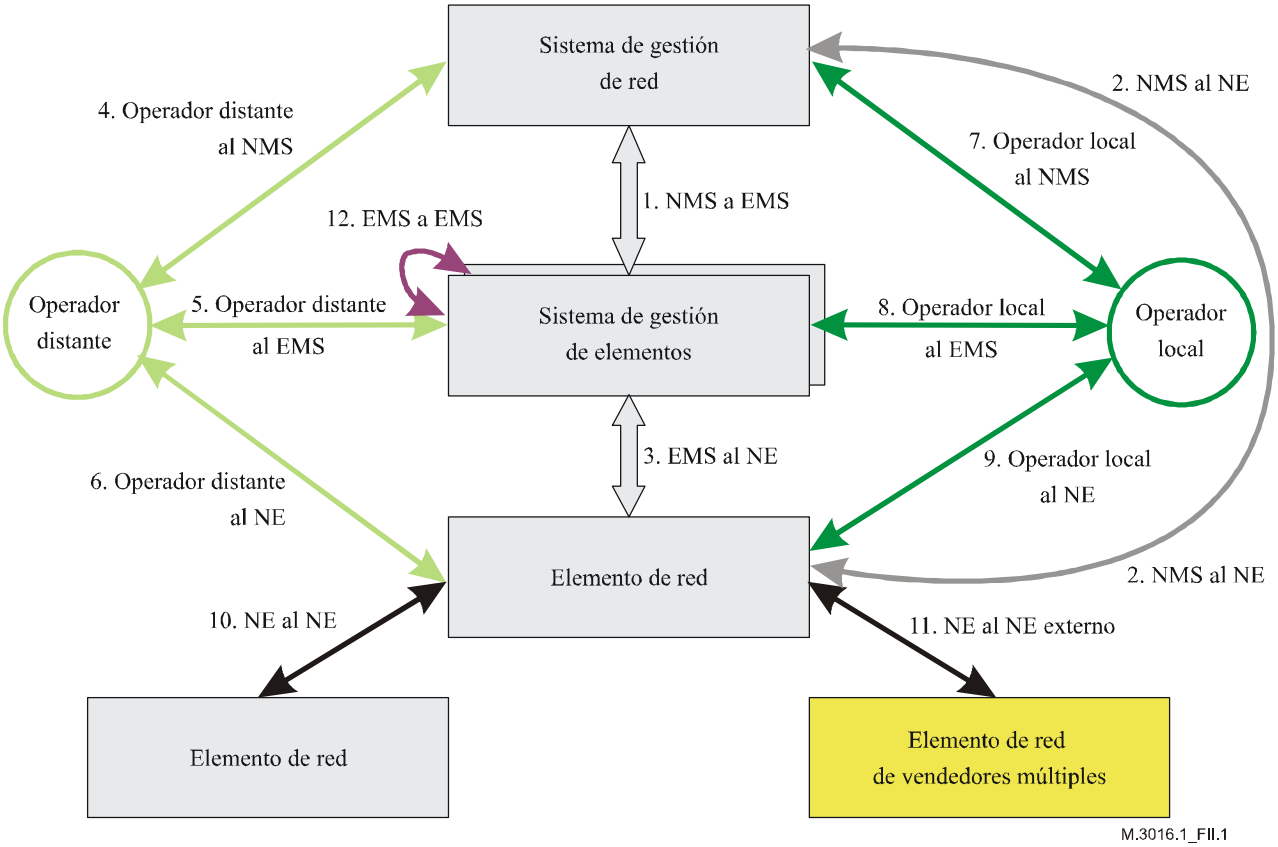

Figura II.1/M.3016.1 – Modelo de referencia de seguridad de gestión de red

El modelo de referencia de seguridad (figura II.1) también puede utilizarse para establecer una correlación entre las interfaces definidas en la red de gestión de las telecomunicaciones (RGT) y el modelo de seguridad. La RGT se define en la Rec. UIT-T M.3010, *Principios para una red de gestión de las telecomunicaciones*. La RGT se define como una arquitectura de gestión que incluye la planificación, aprovisionamiento, instalación, mantenimiento, operaciones y administración de los equipos, redes y servicios de telecomunicaciones.

II.2 Directrices de diseño

En el cuadro II.2 se presentan los objetivos de diseño que pretenden satisfacer los requisitos de la cláusula 6 para mitigar las amenazas mencionadas en el cuadro II.1.

Cuadro II.2/M.3016.1 – Consideración de las directrices de diseño

Directriz	Descripción
Aislamiento	Aislamiento entre el tráfico de gestión y el tráfico de los clientes.
Políticas de seguridad eficaces	Los requisitos y las arquitecturas de soporte deben permitir la aplicación de políticas definibles, flexibles, exigibles, auditables, verificables, fiables y útiles.
Autenticación, autorización y contabilidad (AAA) fuertes	Contabilidad fiable de las sesiones de autorización apropiadas entre entidades autenticadas.
Mayor beneficio para un determinado costo	Al acrecentar la seguridad mediante la utilización de mecanismos de seguridad normalizados, se logran implementaciones con una disponibilidad más amplia y un despliegue generalizado, de forma tal que dichos mecanismos pueden ser evaluados a partir de las experiencias de utilización.
Trayecto para lograr una mejora	Deben considerarse las siguientes etapas, si se desea reforzar y mejorar la seguridad de gestión de la red a fin de satisfacer en mayor grado los requisitos dados mediante tecnologías y mecanismos en evolución o para satisfacer requisitos de seguridad recién definidos.
Viabilidad técnica	Los requisitos deben ser atendidos por los productos, soluciones y/o tecnologías disponibles actualmente.
Control interno	Los requisitos deberían ser compatibles con los procedimientos de funcionamiento normalizados que se aplican en la gestión de red bien administrada.
Normas abiertas	Conviene utilizar ideas y conceptos que ya estén normalizados o que estén en curso de ser normalizados por los organismos de normalización (por ejemplo, seguridad IP (IPsec), firmas digitales). Habrán de considerarse todos los aspectos de las normas abiertas, incluyendo el sistema, los protocolos, los modos, los algoritmos, las opciones, el tamaño de las claves y la codificación.

Apéndice III

Semántica de los términos utilizados en la serie M.3016.x

Los siguientes términos aparecen en **negritas** cuando se utilizan en una declaración de requisito.

III.1 control de acceso: Se destina a impedir el uso no autorizado de un recurso, lo que incluye impedir el uso de un recurso de forma no autorizada.[10]

III.2 servidor de control de acceso (**ACS,** ***access control server***): Elemento de red auxiliar que se despliega para imponer el acceso autenticado a un MS basándose en **contraseñas complejas**, si un NE no puede exigir directamente el cumplimiento de esta funcionalidad.

III.3 administrador de aplicación: Papel que corresponde a la activación, mantenimiento y utilización apropiados de una aplicación de NE/MS. Las tareas de administración de la aplicación incluyen la actualización del soporte lógico de la aplicación.[11]

III.4 administrador de la seguridad de la aplicación: Papel que corresponde a la activación, mantenimiento y utilización apropiados de las características de seguridad de la capa de aplicación de un NE/MS. Representa el nivel más alto de autoridad de seguridad para un ejemplar de aplicación de NE/MS. Las tareas pueden incluir:

– definir y asignar los privilegios de un nuevo usuario y de un grupo en el nivel de aplicación;
– mantener un registro de todas la peticiones de ID de acceso a la aplicación;
– añadir y suprimir usuarios en el nivel de aplicación;
– supervisar todos los registros cronológicos de seguridad de la aplicación;
– configurar los registros y las alarmas de seguridad de la aplicación;
– gestionar los procesos de registro de seguridad de la aplicación;
– terminar la sesión de aplicación del usuario.

III.5 autenticación: **Autenticación** es el acto de verificar una identidad pretendida.

III.6 contraseñas complejas: Una contraseña puede caracterizarse como "compleja" si tiene alguna combinación de caracteres alfabéticos, numéricos y especiales, lo que dificultará o hará poco probable que se pueda deducir la contraseña a través de ingeniería social o por medios automatizados.

III.7 plano de control: El **plano de control** realiza las funciones de control de la llamada y de la conexión. El **plano de control** establece y libera conexiones, mediante señalización, y puede restablecer una conexión en caso de una avería.[12]

III.8 medidas de administración de seguridad fundamental: Un **administrador de seguridad del sistema** se encarga de las **medidas de administración de seguridad fundamentales**, las cuales permiten la activación, mantenimiento y utilización apropiados de las características de seguridad

---

[10] Tomado de la cláusula 3.1 de la Norma ANSI T1.233-1993 (R1999), *Operations, Administration, Maintenance, and Provisioning – Security Framework for Telecommunications Management Network Interfaces*.

[11] Esta tarea puede ser una función del **administrador del sistema**, si se requiere la autoridad del **superusuario** para completarla. Podrían desarrollarse procesos para controlar el acceso a la cuenta del **superusuario**.

[12] Rec. UIT-T G.8080/Y.1304, *Arquitectura de la red óptica con conmutación automática,* noviembre de 2001, (disponible en la libreria electrónica de la UIT).

de un sistema (NE/MS). Las **medidas de administración de seguridad fundamentales** incluyen, aunque no sean las únicas:

– definir y asignar privilegios de usuario;
– añadir y suprimir ID de usuario;
– inhabilitar la utilización de ID de usuario específicos como ID de acceso a la aplicación;
– inicializar y reactivar contraseñas de acceso a la aplicación;
– inicializar y modificar las claves criptográficas;
– fijar el umbral de prescripción del sistema por lo que se refiere a las contraseñas de acceso a la aplicación;
– fijar el límite del sistema en relación con el número de intentos fallidos de acceso a la aplicación por cada ID de acceso a la aplicación;
– suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema;
– fijar el valor del temporizador de inactividad del sistema;
– establecer el registro de seguridad del sistema y la configuración de las alarmas;
– gestionar los procesos de registro de seguridad;
– actualizar el soporte lógico de seguridad;
– terminar cualquier sesión de usuario o de sistema.

III.9 inhabilitar/inhabilitado: Estas condiciones se utilizan cuando se hace referencia a un ID de usuario, es decir, un estado en el que el ID de usuario no puede ser utilizado para acceder al sistema o aplicación hasta que haya sido habilitado mediante una acción específica de otro ID de usuario que disponga de los adecuados privilegios de autorización (por ejemplo, **administrador de seguridad del sistema** o **administrador de seguridad de la aplicación**).

III.10 sistema de gestión de elementos (EMS, *element management system*): Sistema que realiza la función OS en la capa de gestión de elementos.

III.11 fortaleza de las claves: Los diferentes algoritmos criptográficos disponen de varios grados de seguridad dependiendo del nivel de dificultad para descriptarlos. Un algoritmo criptográfico es considerado resistente si resulta muy poco probable que pueda descifrarse mediante instrumentos informáticos, es decir, que dispone de suficiente complejidad para que no pueda ser manipulado dentro de un periodo "razonable" utilizando los recursos disponibles tanto actualmente como en un futuro previsible. La complejidad informática equivale, la mayoría de las veces, a la complejidad del procesamiento de los datos o el tiempo y el espacio de memoria necesarios para realizar un ataque. Pese a que la complejidad de un ataque no varía para un determinado algoritmo y tamaño de la clave, la potencia de computación aumenta constantemente. Se han venido diseñando buenos criptosistemas cuya posibilidad de violación será prácticamente nula, a la vista de la potencia de computación que se prevé en los próximos años. Como resultado del rápido desarrollo de nuevas tecnología y métodos criptoanalíticos, cambia continuamente el tamaño correcto de la clave para una aplicación particular.

III.12 bloqueo/bloqueado: Tratándose de un ID de usuario, se trata de un estado en el que el ID de usuario no puede ser utilizado para acceder al sistema hasta que el estado de bloqueo se haya suprimido mediante una o varias acciones apropiadas. Entre estas acciones, cabe citar, entre otras:

– reactivación automática, una vez transcurrido un periodo umbral (por ejemplo, 60 minutos),
– reactivación automática, tras la compleción satisfactoria de un proceso de reactivación predefinido (por ejemplo, una vez que el propietario responde correctamente a un conjunto de preguntas predeterminadas),

– reactivación mediante una acción específica de otro ID de usuario que dispone de los privilegios de autorización del caso (por ejemplo, **administrador de seguridad del sistema** o **administrador de seguridad de la aplicación**).

III.13 acción de gestión: Acciones iniciadas por el **administrador del sistema**, o en representación suya.

III.14 comunicación de gestión: Cualquier comunicación que resulte de una **acción de gestión**.

III.15 plano de gestión: El **plano de gestión** ejecuta las funciones de gestión del **plano de transporte**, del **plano de control**, y del sistema considerado en su totalidad. Además, se encarga de la coordinación entre todos los planos. En el **plano de gestión**[13] se realizan las funciones identificadas en la Rec. UIT-T M.3010, *Principios de una red de gestión de telecomunicaciones*, en los ámbitos siguientes: calidad de funcionamiento, averías, configuración, contabilidad y gestión de la seguridad.

III.16 elemento de red (NE, *network element*): Véase la Rec. UIT-T M.3010.

III.17 sistema de gestión de red (NMS, *network management system*): Sistema que realiza la función OS en la capa de gestión de red.

III.18 elemento de red/sistema de gestión (NE/MS, *network element/management system*): Grupo de términos que permiten describir todos los elementos de una red de telecomunicaciones incluyendo los NE, EMS, NMS y OSS.

III.19 autenticación protegida: Incluye la **autenticación fuerte**, **autenticación de dos factores**, **autenticación de trayecto de confianza**, autenticación criptográfica por un tercero (por ejemplo, Kerberos) o autenticación mediante contraseña de un solo uso.

III.20 sesión: Secuencia de operaciones, ya sea entre máquinas o humano a máquina, y que está asociada con un proceso o ID de usuario único.

III.21 autenticación fuerte: La **autenticación fuerte** es aquella que utiliza técnicas criptográficas (por ejemplo, criptación de clave pública, criptación de clave simétrica, firmas digitales y técnicas de troceo digital). La **autenticación fuerte** debería incluir la autenticación bidireccional, la cual es útil para impedir ataques activos.

III.22 criptación resistente: Un ataque basado en la fuerza bruta es aquel que se produce cuando un atacante prueba todas las combinaciones de claves posibles utilizando los recursos informáticos disponibles con el objetivo de descifrar un mensaje criptado. De esta manera, en promedio podrá encontrarse la clave correcta después de haber probado la mitad de todas las combinaciones de claves posibles. El tiempo previsto para probar la mitad de las combinaciones de claves es una medida de la resistencia de la criptación. Por consiguiente, en cualquier momento dado los mecanismos de **criptación resistente** utilizan algoritmos y claves tales que cualquier atacante tendría que dedicar más de dos años para oponerse con éxito a la tecnología vigente.

III.23 administrador del sistema: Papel que se asigna al encargado de los procesos y procedimientos de nivel de OS referentes a la instalación, operación, mantenimiento de la plataforma de operación, instalación del soporte lógico en la plataforma y control de la autoridad del **superusuario**. Las tareas pueden incluir:

– coordinar la instalación de una nueva plataforma;

– definir y asignar nuevos privilegios de usuario y de grupo en el nivel OS;

---

[13] La arquitectura de la RGT se describe en la Rec. UIT-T M.3010, *Principios de una red de gestión de las telecomunicaciones* y los detalles adicionales referentes al PLANO DE GESTIÓN se presentan en las Recomendaciones de la serie M. La Rec. UIT-T G.8080/Y.1304, *Arquitectura de la red óptica con conmutación automática*, de noviembre de 2001 (disponible en la librería electrónica de la UIT).

– mantener un registro de todas las peticiones de ID de acceso al OS;
– añadir y suprimir usuarios en el nivel OS;
– inhabilitar la utilización de ID específicos como ID de acceso al sistema (bin, sys, uucp);
– instalar actualizaciones y correcciones de rutinas del OS;
– instalar soporte lógico de aplicación y de base de datos en el OS;
– supervisar todos los registros cronológicos del sistema;
– mantener y supervisar el acceso a la contraseña del **superusuario** y las modificaciones correspondientes;
– controlar el acceso a la cuenta del **superusuario**, facilitando el acceso adecuado conforme lo exija la actividad comercial;
– gestionar los procesos de registro de sistema;
– delegar autorizaciones de administración a personas específicas que tienen otras funciones, incluyendo los **administradores de aplicación**;
– terminar cualquier sesión de usuario o sistema.

III.24 administrador de seguridad del sistema: Papel que se asigna al encargado de la activación, mantenimiento y utilización adecuados de las características de seguridad del sistema de un NE/MS. Representa el nivel más alto de autoridad en materia de seguridad de un ejemplar de sistema/aplicación. Las tareas pueden incluir:

– definir y asignar nuevos privilegios de usuario y de grupo en el nivel OS;
– mantener un registro de todas las peticiones de ID de acceso al OS;
– añadir y suprimir usuarios en el nivel OS;
– inhabilitar la utilización de ID específicos como ID de acceso al sistema (bin, sys, uucp);
– supervisar todos los registros cronológicos de seguridad del sistema;
– inicializar y modificar las claves criptográficas;
– establecer el umbral de obsolescencia del sistema por lo que se refiere a las contraseñas de acceso al sistema;
– establecer el límite del sistema en cuanto al número de intentos fallidos de acceso por cada ID de acceso al sistema;
– suprimir un bloqueo o modificar el valor del temporizador de bloqueo del sistema;
– establecer el valor del temporizador de inactividad del sistema;
– configurar las alarmas y los registros del sistema;
– gestionar los procesos de registros de seguridad del sistema;
– delegar autorizaciones de seguridad a personas específicas que tienen otras funciones, incluyendo los **administradores de seguridad de la aplicación**;
– terminar cualquier sesión de usuario o de sistema.

III.25 plano de transporte: El **plano de transporte** se encarga de la transferencia bidireccional o unidireccional de la información del usuario entre elementos de red. Además, puede proporcionar la transferencia de alguna información de control y de gestión de red. El **plano de transporte** está estructurado por capas y es equivalente a la red de transporte que se define en la Rec. UIT-T G.8080/Y.1304, *Arquitectura de la red óptica con conmutación automática*.[12]

III.26 trayecto de confianza: Mecanismo mediante el cual puede asegurarse cualquier interacción usuario/operador a sistema, o sistema a sistema. Este mecanismo podrá ser activado únicamente por el usuario/operador o por el sistema y no puede ser imitado. Un **trayecto de confianza** puede ser un trayecto físico dedicado (es decir, un terminal conectado directamente al sistema) o un trayecto criptado, que incluye protección de integridad y contra la reproducción (por ejemplo, red privada virtual "asegurada", túnel por capa de zócalo segura [SSL], estructura segura [SSH]).[14]

III.27 autenticación de dos factores: Se trata de un término comúnmente utilizado para describir un proceso de a**utenticación** que requiere la posesión de una entidad física (por ejemplo, testigo o tarjeta) y el conocimiento de un secreto (por ejemplo, contraseña o secreto de usuario).

[14] Adaptado del Centro Nacional de Seguridad Informática NCSC-TG-004-88, *Glosario de términos de seguridad de los ordenadores*, octubre de 1998 (disponible en la dirección web http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

BIBLIOGRAFÍA

Los incisos en esta bibliografía aportan información adicional referente a muchos de los tópicos abordados en los apéndices I y II.

– ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance.*

– ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation,* (disponible en la tienda electrónica de Normas ANSI X9, Electronic Standards Store, http://webstore.ansi.org/ansidocstore/ dept.asp?dept_id=80).

– ANSI X9.62-1998, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* (disponible en la tienda electrónica de Normas ANSI X9 Electronic Standards Store, http://webstore. ansi.org/ansidocstore/dept.asp?dept_id=80).

– ANSI T1.210-2004, *OAM&P – Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces.*

– ANSI T1.233-2004, *OAM&P – Security Framework for Telecommunications Management Network (TMN) Interfaces*.

– ANSI T1.252-1996 (R2002), *Operations, Administration, Maintenance and Provisioning OAM&P – Security for the Telecommunications Management Network (TMN) Directory.*

– ANSI T1.261-1998 (R2004), *OAM&P – Security for TMN Management Transactions over the TMN Q3 Interface.*

– ANSI T1.268-2000, *TMN – PKI – Digital Certificates and Certificate Revocation Lists Profile*.

– ANSI X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*.

– ATM Forum. AF-SEC-0179.000 (April 2002), *Methods of Securely Managing ATM Network Elements – Implementation Agreements Version 1.1,* (available at ftp://ftp.atmforum.com/pub/approved-specs/af-sec-0179.000.pdf).

– BARRETT (D.), SILVERMAN (R.): SSH, The Secure Shell: The Definitive Guide, *O'Reilly*, enero de 2001.

– BELLOVIN (S.): An Issue With DES-CBC When Used Without Strong Integrity, *Proceedings of the 32nd Internet Engineering Task Force*, Danvers, MA, April 1995.

– BLEICHENBACHER (D.): Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1, *Advances in Cryptology-Crypto '98*, Springer LNCS Vol. 1462, pp. 1-12, 1998.

– BONEH (D.): Twenty Years of Attacks on the RSA Cryptosystem, *Notices of the American Mathematical Society (AMS)*, Vol. 46, No. 2, pp. 203-213, febrero de 1999, (disponible en http://www.ams.org/notices/199902/boneh.pdf).

– BONEH (D.), JOUX (A.), NGUYEN (P.): Why Textbook RSA and ElGamal Encryption Are Insecure, *Advances in Cryptology-Asiacrypt 2000*, Springer LNCS Vol. 1976, pp. 30-43, 2000.

– Federal Communications Commission Docket Number 97-213 *Implementation of the Communications Assistance for Law Enforcement Act*, septiembre de 1999.

– General Requirements (GR)-815, *Generic Requirements for Network Element/Network System Security*, marzo de 2002 (disponible en la supertienda de información Telcordia, Information SuperStore, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GR-1194, *Bellcore Operations Systems Security Requirements*, diciembre de 1998, (disponible en la supertienda de información Telcordia, http://telecom-info.telcordia.com/site-cgi/ido/index.html).

– GUTMANN (P.): Software Generation of Practically Strong Random Numbers, *Seventh USENIX Security Symposium Proceedings*, The USENIX Association, pp. 243-257, 1998, (disponible en http://www.usenix.org/publications/library/proceedings/sec98/full_papers/gutmann/gutmann.pdf).

– Information Assurance Technical Framework Forum (IATF), http://www.commoncriteria.org/ and http://www.iatf.net/protection_profiles/profiles.cfm.

– IEEE 1363-2000, *IEEE Standard Specifications for Public Key Cryptography*, (disponible en el sitio en línea de normas del IEEE Standards Online, http://standards.ieee.org/catalog/olis/ busarch.html).

– IETF RFC 768, *User Datagram Protocol*, J. Postel, agosto de 1980 (disponible en http://www.ietf.org/rfc/rfc0768.txt?number=768).

– IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*, (disponible en http://www.ietf.org/rfc/ rfc0791.txt?number=791).

– IETF RFC 792 (1981), *Internet Control Message Protocol – DARPA Internet Program Protocol Specification*, (disponible en http://www.ietf.org/rfc/rfc0792.txt?number=792).

– IETF RFC 793 (1981), *Transmission Control Protocol – DARPA Internet Program Protocol Specification*, (disponible en http://www.ietf.org/rfc/rfc0793.txt?number=793).

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol – or – Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware*, (disponible en http://www.ietf.org/rfc/rfc0826.txt?number=826).

– IETF RFC 859 (1983), *Telnet Status Option,* (disponible en http://www.ietf.org/rfc/rfc0859.txt?number=859).

– IETF RFC 959 (1985), *File Transfer Protocol (FTP),* (disponible en http://www.ietf.org/rfc/rfc0959.txt?number=959).

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP),* (disponible en http://www.ietf.org/rfc/rfc1157.txt?number=1157).

– IETF RFC 1288 (1991), *The Finger User Information Protocol,* (disponible en http://www.ietf.org/rfc/rfc1288.txt?number=1288).

– IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2),* (disponible en http://www.ietf.org/rfc/rfc1905.txt?number=1905).

– IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,* (disponible en http://www.ietf.org/rfc/rfc2045.txt?number=2045).

– IETF RFC 2202 (1997), *Test Cases for HMAC-MD5 and HMAC-SHA-1,* (disponible en http://www.ietf.org/rfc/rfc2202.txt?number=2202).

– IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL),* (disponible en http://www.ietf.org/rfc/rfc2222.txt?number=2222).

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0,* (disponible en http://www.ietf.org/rfc/rfc2246.txt?number=2246).

– IETF RFC 2271 (1998), *An Architecture for Describing SNMP Management Frameworks,* (disponible en http://www.ietf.org/rfc/rfc2271.txt?number=2271).

– IETF RFC 2272 (1998), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP),* (disponible en http://www.ietf.org/rfc/rfc2272.txt?number=2272).

– IETF RFC 2273 (1998), *SNMPv3 Applications,* (disponible en http://www.ietf.org/rfc/rfc2273.txt?number=2273).

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, (disponible en http://www.ietf.org/rfc/rfc3414.txt?number=3414).

– IETF RFC 2275 (1998), *View-based Access Control Model for the Simple Network Management Protocol* (*SNMP)*, (disponible en http://www.ietf.org/rfc/rfc2275.txt?number=2275).

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

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

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

– IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms,* (disponible en http://www.ietf.org/rfc/rfc2451.txt?number=2451).

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol (HTTP) – HTTP/1.1,* (disponible en http://www.ietf.org/rfc/rfc2616.txt?number=2616).

– IETF RFC 2631 (1999), *Diffie-Hellman Key Agreement Method,* (disponible en http://www.ietf.org/rfc/rfc2631.txt?number=2631).

– IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core,* (disponible en http://www.ietf.org/rfc/rfc3080.txt?number=3080).

– IETF RFC 3081 (2001), *Mapping the BEEP Core onto TCP,* (disponible en http://www.ietf.org/rfc/rfc3081.txt?number=3081).

– ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture,* (disponible en la tienda en línea de ISO, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=14256&ICS1 =35&ICS2=100&ICS3=1).

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

– Recomendación UIT-T M.3013 (2000), *Consideraciones sobre una red de gestión de las telecomunicaciones*, (disponible en la librería electrónica de la UIT).

– JANSEN (W.A.): A Revised Model for Role Based Access Control, *NIST-IR 6192*, julio de 1998, (disponible en http://csrc.nist.gov/rbac/jansen-ir-rbac.pdf).

– JONSSON (J.), KALISKI (B.): On the Security of RSA Encryption in TLS, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 127-142, agosto de 2002.

– KELSEY (J.), SCHNEIER (B.), FERGUSON (N.): Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator, *Sixth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, agosto de 1999, (disponible en http://www.counterpane.com/yarrow-notes.html).

– KRAWCZYK (H.): Security Analysis of the Internet Key Exchange's Signature-Based Key Exchange Protocol, *Advances in Cryptology-Crypto 2002*, Springer LNCS Vol. 2442, pp. 143-161, agosto de 2002.

– LENSTRA (A.), VERHEUL (E.): Selecting Cryptographic Key Sizes, *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.

– National Computer Security Center, NCSC-TG-004-88, *Glossary of Computer Security Terms.* octubre de 1988, (disponible en http://csrc.nist.gov/SBC/PDF/NCSC-TG-004_COMPUSEC_Glossary.pdf).

– National Communications System, *Public Switched Network Security Assessment Guidelines*, septiembre de 2000, (disponible en http://www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification*, *Version 1.8*, marzo de 2002, (disponible en http://cgi.omg.org/docs/formal/02-03-11.pdf).

– Object Management Group, *Common Object Request Broker Architecture Security Service Specification, Version 1.7,* marzo de 2001, (disponible en http://cgi.omg.org/docs/formal/01-03-08.pdf).

– Partnership for Critical Infrastructure Security, *Partnership for Critical Infrastructure Security Common Reference Glossary of Terms, Version 2001-09*, septiembre de 2001, (disponible en http://www.pcis.org/library.cfm?urlSection=WG).

– RESCORLA (E.): SSL and TLS, Addison-Wesley, 2001.

– SCHNEIER (Bruce.): Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

– SILVERMAN (R.): The Mythical MIPS Year, *IEEE Computer*, agosto de 1999.

– SILVERMAN (R.): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, *RSA Laboratories Bulletin*, No. 13, abril de 2000.

– VAUDENAY (S.): Security Flaws Induced by CBC Padding – Applications to SSL, IPsec, WTLS, *Advances in Cryptology-Eurocrypt 2002*, Springer LNCS Vol. 2332, pp. 534-545, abril-mayo de 2002.

– World Wide Web Consortium, *Extensible Markup Language (XML) 1.0*, febrero de 1998, (disponible en http://www.w3.org/TR/1998/REC-xml-19980210).

– World Wide Web Consortium, *Simple Object Access Protocol 1.1*, D. Box et al, mayo de 2000, (disponible en http://www.w3.org/TR/SOAP/).

– WU (T.): The Secure Remote Password Protocol, *Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security*, San Diego, California, pp. 97-111, marzo de 1998, (disponible en http://www.isoc.org/isoc/conferences/ndss/98/wu.pdf)

– YLÖNEN, T.: SSH – Secure Login Connections Over the Internet, *Sixth USENIX Security Symposium Proceedings*, pp. 37-42, julio de 1996, (disponible en http://www.usenix.org/publications/library/proceedings/sec96/full_papers/ylonen/index.html).

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