Unión Internacional de Telecomunicaciones

UIT-T M.3016.2

(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: Servicios de seguridad

Recomendación UIT-T M.3016.2

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.3016.2

Seguridad en el plano de gestión: Servicios de seguridad

Resumen

Esta Recomendación, en la que se determinan los servicios 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.3016.2 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 mundiales. En consecuencia, resulta esencial disponer de una seguridad apropiada para las funciones de gestión que permita controlar esa infraestructura. Ya existen muchas normas sobre seguridad aplicadas a la gestión de la red de telecomunicaciones. No obstante, se considera que la conformidad es reducida y que las aplicaciones de los diversos equipos de telecomunicaciones y componentes de soporte lógico son incompatibles. Esta Recomendación define los servicios de seguridad mediante los cuales los fabricantes, organismos y proveedores de servicio podrán implementar una infraestructura segura de gestión de las telecomunicaciones. Aunque el conjunto de servicios y mecanismos de seguridad que se propone en esta Recomendación representa la mejor interpretación de los últimos adelantos, las tecnologías seguirán avanzando y las condiciones cambiarán. Para obtener los resultados previstos, esta Recomendación deberá evolucionar si las condiciones lo justifican. El objetivo de esta Recomendación será sentar las bases correspondientes en la materia. Los proveedores de servicio podrán incluir otros servicios y mecanismos de seguridad para responder a sus necesidades concretas, aparte de los ya indicados en la presente Recomendación.

Esta Recomendación forma parte de las 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: Visión 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 de los perfiles*.

Recomendación UIT-T M.3016.2

Seguridad en el plano de gestión: Servicios de seguridad

1 Alcance

En las Recs. UIT-T M.3016.1, M.3016.2 y M.3016.3 se especifica un conjunto de requisitos, servicios y mecanismos para lograr la seguridad que exigen las funciones de gestión necesarias para soportar la infraestructura de telecomunicaciones. En las Recs. UIT-T M.3016.1-M.3016.3 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 los servicios 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 de 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).

En la presente Recomendación no se definen los requisitos de seguridad ni los mecanismos de seguridad necesarios para soportar los requisitos de los servicios de seguridad.

Esta Recomendación forma parte de las Recomendaciones de la serie M.3016.x. En otras Recomendaciones de la misma serie se especifican los requisitos y mecanismos de seguridad, así como los formularios de las características de seguridad.

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.

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 X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

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

3 Definiciones

La presente Recomendación utiliza los siguientes términos de la Rec. UIT-T X.800:

– control de acceso;

– autenticación;

– confidencialidad;

– integridad de los datos;

– no repudio.

4 Abreviaturas, siglas o acrónimos

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

MS Sistema de gestión (*management system*)

NE Elemento de red (*network elemen*t)

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

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

RGT Red de gestión de las telecomunicaciones

5 Convenios

En las Recs. UIT-T M.3016.1, M.3016.2 y M.3016.3, se utiliza un descriptor para identificar los diferentes requisitos, servicios y mecanismos. Este descriptor está compuesto por una de las siguientes etiquetas de tres letras, seguida por un número:

– REQ para indicar requisito;

– SER para indicar servicio;

– MEC para indicar mecanismo.

6 Servicios de seguridad

En la figura 1 se representan las relaciones entre los objetivos de seguridad, amenazas, riesgos, requisitos de seguridad y servicios. Se describe el proceso para deducir "los requisitos de seguridad" a partir de "las amenazas" y de "los objetivos de seguridad", los que a su vez serán tenidos en cuenta en un conjunto de servicios de seguridad. Estos "servicios", que contrarrestan a las amenazas, utilizarán los "mecanismos" los cuales harán a su vez uso de los "algoritmos de seguridad".

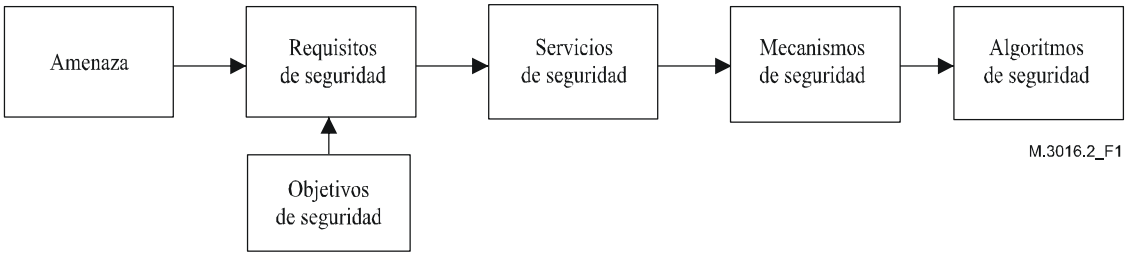

Figura 1/M.3016.2 – Marco de seguridad

El cuadro 1, a continuación, se extrae de la Rec. UIT-T M.3016.0 (cuadro 4 de dicha Recomendación). El cuadro, en el que se presenta una visión general de la relación entre los requisitos y los servicios de seguridad, se utiliza como base para organizar las demás Recomendaciones de la serie. Por ejemplo, en la Rec. UIT-T M.3016.1 se tratan los requisitos funcionales de seguridad, en la presente Recomendación (Rec. UIT-T M.3016.2) se tratan los servicios de seguridad y en la Rec. UIT-T M.3016.3 se tratan los mecanismos de seguridad específicos relacionados con los servicios de seguridad.

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

Cuadro 1/M.3016.2 – Correspondencia entre los requisitos de seguridad y los servicios de seguridad

Requisito funcional de seguridad	Servicio de seguridad
Verificación de identidades	Autenticación del usuario Autenticación de la entidad par Autenticación del origen de los datos
Acceso controlado y autorización	Control de acceso
Protección de la confidencialidad – datos almacenados	Control de acceso Confidencialidad
Protección de la confidencialidad – datos transferidos	Confidencialidad
Protección de la integridad de los datos – datos almacenados	Control de acceso
Protección de la integridad de los datos – datos transferidos	Integridad
Imputabilidad	No repudio
Registro de actividades	Registro de auditoría
Notificación de alarma de seguridad	Alarma de seguridad
Auditoría de seguridad	Registro de auditoría
Protección de la DCN	Inspección de paquetes

En el cuadro 2, se esboza la disposición de esta cláusula:

Cuadro 2/M.3016.2 – Organización de la cláusula 6

Cláusula	Contenido
6.1	Trata los servicios de seguridad, incluidas la autenticación del usuario, la autenticación de la entidad par y la autenticación del origen de los datos.
6.2	Trata el servicio de control de acceso.
6.3	Trata el servicio de confidencialidad de los datos.
6.4	Trata el servicio de integridad de los datos.
6.5	Trata el servicio de no repudio.
6.6	Trata el servicio de registro de auditoría
6.7	Trata el servicio de alarma de seguridad

6.1 Autenticación

Una RGT debe ofrecer las capacidades necesarias para establecer y verificar la identidad pretendida por cualquiera de los actores de la RGT.

Los actores pueden ser usuarios humanos o entidades que forman parte de la RGT. Una vez verificadas, las identidades constituyen la base para la imputabilidad y son fundamentales para el cumplimiento de la mayoría de los requisitos de seguridad que se indican en la presente cláusula.

El servicio de seguridad que da soporte a este requisito se denomina **autenticación**. Mediante el servicio de autenticación se comprueba que la identidad de un objeto o sujeto es en realidad la identidad que éste reclama tener. Dependiendo del tipo de actor y del propósito de la identificación, se podrían exigir los siguientes tipos de autenticación:

– autenticación del usuario, que comprueba la identidad del usuario humano o del proceso de aplicación;
– autenticación de la entidad par, que comprueba la identidad de la entidad par durante una relación de comunicación;
– autenticación del origen de los datos, que comprueba la identidad del responsable de una unidad específica de datos.

El servicio de autenticación que se utilice, hace la comprobación para un ejemplar particular de tiempo. Para garantizar una comprobación continua se debe realizar la autenticación de manera repetitiva o ligada a un servicio de integridad.

Algunos ejemplos de los mecanismos que se utilizan para la implementación del servicio de autenticación son las contraseñas y los números de identificación personal (PIN, *personal identification numbers*) (en el caso de una autenticación sencilla) y los métodos basados en criptografía (en el caso de una autenticación robusta).

La **autenticación** cumple dos propósitos en la salvaguarda del **plano de gestión**:

1) garantizar la identidad de las partes en comunicación, suministrando las bases para el establecimiento de comunicaciones privadas con plena integridad de datos y confidencialidad entre los dos sistemas; y
2) suministrar un mecanismo básico para el registro de sucesos en un sistema de gestión y/o la auditoría de las actividades de gestión de cualquier sistema.

Las siguientes capas pueden suministrar este servicio (de acuerdo con la Rec. UIT-T X.800):

– capa de red (confirmación de la identidad de los pares de la capa de transporte);
– capa de transporte (confirmación de la identidad de los pares de la capa de sesión);
– capa de aplicación (confirmación de la identidad de los procesos de aplicación);
– externo a OSI: en el propio proceso de aplicación.

Teniendo en cuenta que el requisito para la RGT será identificar y autenticar los gestores y agentes, así como el enlace de autenticación con control de acceso, las ubicaciones recomendadas con respecto a la pila OSI son la capa de aplicación y el proceso de aplicación.

6.1.1 Autenticación del usuario

La **autenticación del usuario** se refiere a la **autenticación** de los clientes relacionados con la gestión de la red. En este caso, la **autenticación** comprueba la identidad del usuario legítimo y evita los ataques de impostura efectuados por usuarios ilegítimos. Con una **autenticación** adecuada, es posible registrar las actividades y limitar a los usuarios a unas actividades o cometidos previamente autorizados.

SER 1: Todo NE/MS que cuente con acceso de usuario debe soportar un servicio de autenticación robusto que compruebe la identidad.

Cabe señalar que aunque en esta Recomendación no se exige un servicio de inicio de sesión único, este servicio se podrá tratar en una Recomendación posterior. Sin embargo, si se establece este servicio, el protocolo deberá también solicitar las credenciales de la entidad o entidades. Es posible que un usuario no tenga que volver a introducir sus credenciales si éstas han sido almacenadas de alguna manera segura (por ejemplo, mediante un mecanismo Kerberos).

6.1.2 Autenticación de la entidad par

La autenticación de la entidad par se refiere a la **autenticación** de la entidad par durante la comunicación entre entidades, como aplicaciones, sistemas o dispositivos. La **autenticación** comprueba la identidad del par y evita los ataques de impostura por parte de dispositivos ilegítimos.

La **autenticación** de la entidad par proporciona la **autenticación** durante la comunicación de datos entre sistemas (por ejemplo de sistema a sistema, de aplicación a aplicación) y es la base para el establecimiento de las comunicaciones privadas con integridad plena de datos. Durante la comunicación de datos, la **autenticación** de la entidad transmisora le permite al receptor de un mensaje tener seguridad acerca del origen del mismo. En un canal de comunicaciones seguro, se debe aplicar **autenticación** criptográfica a cada mensaje con el fin de vincular al mensaje la identidad de la entidad transmisora. El receptor deberá revisar la información criptográfica que se suministra con el mensaje con el fin de verificar la verdadera identidad de la entidad transmisora.

SER 2: Todo NE/MS que cuente con comunicación de datos entre sistemas debe soportar **autenticación** de entidad par para sus comunicaciones y debe utilizar sistemas basados en el certificado X.509 para la **autenticación** o **autenticación protegida**.

6.1.3 Autenticación del origen de los datos

La **autenticación** del origen de los datos se refiere a la comprobación de la identidad de la entidad de sistema que es supuestamente la fuente original de los datos recibidos. Esta **autenticación** corrobora que el origen de los datos es el que se supone. Este servicio por lo general se presta conjuntamente con un servicio de integridad de datos. El servicio es independiente de cualquier relación que haya entre el remitente y el destinatario, y los datos en cuestión pueden haberse originado en cualquier momento pasado.

SER 3: Todo NE/MS que suministre la identidad de una entidad de sistema con corroboración del origen de los datos debe soportar el servicio de **autenticación** del origen de los datos.

6.2 Control de acceso

Una RGT debe ofrecer las capacidades que aseguren que los actores de la red no pueden acceder a la información o a los recursos para los que no tienen autorizado el acceso.

El servicio de seguridad que cumple con este requisito se denomina **control de acceso**. El servicio de control de acceso ofrece la forma de garantizar que los sujetos tienen acceso a los recursos únicamente de la manera autorizada. Puede que sea necesario volver a llevar a cabo la autenticación debido a caducidad de los temporizadores de espera o a requisitos de cambio de contraseña. Los recursos implicados pueden ser el sistema físico, el software de sistema, las aplicaciones y los datos. El servicio de control de acceso se puede definir e implementar con diversos niveles de detalle en la RGT: a nivel de agente, de objeto o de atributo.

Los límites de acceso se basan en la información de control de acceso, la cual especifica:

- los medios para determinar las entidades con acceso autorizado;
- el tipo de acceso permitido (lectura, escritura, modificación, creación, supresión);
- los medios para relacionar la dimensión del tiempo con las entidades autenticadas y los testigos que éstas utilizan para la autenticación.

Se puede clasificar de manera más específica el control de acceso de la RGT en los siguientes tres tipos:

– *Control de acceso a la asociación de gestión*

  Este servicio permite el control de acceso a nivel de la asociación de gestión, lo que significa que los derechos de acceso se relacionan con la asociación misma, es decir con el derecho a crear la asociación.

– *Control de acceso de la notificación de gestión*

  Este servicio permite el control de acceso con respecto a las notificaciones, es decir con el fin de garantizar que las notificaciones sólo se difunden a las entidades autorizadas para recibirlas.

– *Control de acceso del recurso gestionado*

  Este servicio permite el control de acceso con respecto a los propios recursos.

Antes de que se otorgue acceso a un recurso, es necesario verificar la identidad de la entidad que pretende tener acceso a éste. Ello significa que la utilización del control de acceso está siempre vinculada con la utilización de un servicio de autenticación.

SER 4: Todo NE/MS debe soportar servicios de control de acceso para la asociación de gestión, notificación de gestión y control de acceso a los recursos de gestión.

6.3 Confidencialidad de los datos

La RGT debe ofrecer las capacidades necesarias para garantizar la confidencialidad de los datos almacenados y cursados.

Los servicios de seguridad que soportan este requisito son: **control de acceso**, en el caso de los datos almacenados, y **confidencialidad de los datos**, en el caso de los datos cursados.

El servicio de confidencialidad ofrece protección contra la revelación no autorizada de los datos intercambiados. Se distinguen los siguientes tipos de servicios de confidencialidad:

– *Confidencialidad de campos seleccionados*

  Este servicio se puede utilizar en la capa de aplicación o en el propio proceso de aplicación, dado que es este proceso el que puede distinguir los campos.

– *Confidencialidad con conexión y sin conexión*

  Teniendo en cuenta que se necesita confidencialidad de extremo a extremo, que excluye la capa física y la capa de enlace de datos, puede ofrecerse confidencialidad en la capa de red, en la capa de transporte, en la capa de presentación, en la capa de aplicación o en el proceso de aplicación.

SER 5: Todo NE/MS debe soportar un servicio de confidencialidad de datos con el fin de ofrecer protección contra la divulgación no autorizada de los intercambios de datos orientados a la conexión o sin conexión, y proporcionar la confidencialidad de campos seleccionados.

6.4 Integridad de los datos

La RGT debe poder garantizar la integridad de los datos almacenados y cursados.

Los servicios de seguridad que soportan este requisito son: **control de acceso**, para el caso de los datos almacenados, e **integridad de los datos**, para el caso de los datos cursados.

El servicio de integridad ofrece los medios para garantizar la conformidad de los datos intercambiados, la protección contra la modificación, la supresión, la creación (inserción) y la reproducción de los datos intercambiados. Se distinguen los siguientes tipos de servicios de integridad:

– integridad con selección del campo;
– integridad de la conexión sin recuperación;
– integridad de la conexión con recuperación.

El servicio de integridad de datos requiere que se utilice un valor secreto conocido únicamente por las partes que se comunican. Diversos protocolos utilizan el valor secreto para crear un compendio HMAC-MD5 y ese compendio se añade a cada mensaje.

SER 6: Todo NE/MS debe soportar un servicio de integridad de datos con el fin de ofrecer protección contra la modificación, borrado, inserción y reproducción de los datos que se intercambian.

6.5 No repudio

La RGT debe ofrecer la capacidad de evitar que una entidad niegue la responsabilidad de las acciones que lleva a cabo o de sus efectos.

El servicio de **no repudio** soporta este requisito que vincula al individuo (o a la entidad) con la operación que se lleva a cabo. Los servicios de no repudio proporcionan los medios para comprobar que en realidad se llevó a cabo el intercambio de datos. Puede ser de dos formas:

– no repudio: comprobación del origen;
– no repudio: comprobación de entrega.

Con el fin de lograr un servicio de no repudio más general, se pueden utilizar combinaciones adecuadas de los servicios de autenticación, control de acceso y registro de auditoría.

SER 7: Todo NE/MS debe soportar un servicio de no repudio que garantice que ninguna entidad pueda negar responsabilidad sobre sus acciones o sobre los efectos de esas acciones.

6.6 Registro de auditoría

La RGT debe ofrecer la capacidad de almacenar información acerca de las actividades en el sistema, con la posibilidad de que se pueda seguir el rastro de esta información hasta individuos o entidades. La RGT debe también proporcionar la capacidad de analizar los datos registrados acerca de eventos relacionados con la seguridad, con el fin de detectar violaciones a la política de seguridad.

Un registro cronológico es una recopilación de registros. Es la abstracción OSI de los recursos de registro en sistemas abiertos reales. Los registros son los asientos de la información que se registra.

Muchas funciones de gestión requieren la capacidad de preservar la información acerca de eventos que han ocurrido o de operaciones que han sido ejecutadas o se han tratado de ejecutar sobre diversos recursos o por parte de los mismos.

Además, una vez recuperada la información desde un registro cronológico, el gestor debe poder determinar si se han perdido asientos del registro o si las características de los asientos almacenados en el mismo fueron modificadas en cualquier momento.

Una auditoría debe considerarse como una revisión y examen independiente de los registros y actividades del sistema que tiene como fin comprobar la aptitud de los controles del sistema, garantizar el cumplimiento de la política de seguridad establecida y de los procedimientos operativos y para detectar violaciones de la seguridad. Los resultados de la auditoría podrían llevar a identificar cambios en los controles, políticas y procedimientos.

Es importante que cada NE/MS ofrezca las capacidades adecuadas que permitan la investigación, auditoría y actividades de análisis y detección en tiempo real, de manera que se puedan tomar las medidas correctoras pertinentes. En la presente cláusula se tienen en cuenta los registros de

auditoría de seguridad, sin embargo, los detalles específicos del contenido y el formato de los registros de auditoría de seguridad no se tratan en esta Recomendación.

Cabe observar que las actividades de análisis forense e investigación pueden incluir la verificación de mensajes OAM&P que no están relacionados con la seguridad, así como de la información almacenada en los registros de auditoría de seguridad que se describen en esta cláusula. Se requiere, por lo tanto, que a los fines de las acciones sujetas a auditoría, se lleve un registro de los mensajes OAM&P que no están relacionados con la seguridad y que a veces se denominan mensajes "de cambios recientes".

SER 8: Los NE/MS deben poder llevar el registro de cualquier acción que modifique los servicios y atributos de seguridad, los controles de acceso, los parámetros de configuración de los dispositivos y de todo intento de registro en el sistema que dé lugar a la invocación del temporizador de inactividad del sistema, así como de toda acción que requiera auditoría. Todo NE/MS debe soportar la capacidad de auditar esos registros.

Se recomienda que una vez etiquetadas con un número de secuencia y autenticadas de manera criptográfica (firmadas), el NE/MS envíe las entradas del registro de auditoría a un servidor de auditoría inmodificable.

6.7 Informe de alarmas

La RGT debe ofrecer la capacidad de generar notificaciones de alarma de sucesos seleccionados. El usuario debe poder definir los criterios de selección.

La función de control de auditoría de seguridad es una función de gestión del sistema que describe la notificación de un conjunto de sucesos de seguridad. La notificación de alarma de seguridad definida por esta función de gestión de los sistemas presenta información relativa a la condición operativa relacionada con la seguridad.

SER 9: Todo NE/MS debe soportar un servicio de notificación de alarmas que alerte a los administradores de seguridad acerca de las condiciones operativas relacionadas con la seguridad.

6.8 Inspección de paquetes

La RGT debe ofrecer la capacidad de inspección de paquetes en el caso de tráfico basado en paquetes con destino al plano de gestión de cualquier dispositivo de la RGT. El usuario debe poder definir el filtrado basándose en las direcciones de red de origen y de destino, en el protocolo y en los puertos de origen y de destino de los paquetes.

La inspección de paquetes es el proceso mediante el cual se examinan los valores del encabezamiento de cada paquete que atraviesa los elementos de red, teniendo en cuenta determinados criterios de coincidencia. Se podrían llevar a cabo acciones con base en los resultados de la inspección del paquete.

SER 10: Todo NE/MS debe soportar un servicio de inspección de paquetes que proteja al plano de gestión de la RGT del tráfico que no cumple con las políticas de seguridad.

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