



UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

X.736

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

REDES DE COMUNICACIÓN DE DATOS

**TECNOLOGÍA DE LA INFORMACIÓN –
INTERCONEXIÓN DE SISTEMAS ABIERTOS –
GESTIÓN DE SISTEMAS:
FUNCIÓN SEÑALADORA DE ALARMAS
DE SEGURIDAD**

Recomendación X.736



Ginebra, 1992

Prefacio

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El CCITT (Comité Consultivo Internacional Telegráfico y Telefónico) es un órgano permanente de la UIT. En el CCITT, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 166 países miembros, 68 empresas de explotación de telecomunicaciones, 163 organizaciones científicas e industriales y 39 organizaciones internacionales.

Las Recomendaciones las aprueban los miembros del CCITT de acuerdo con el procedimiento establecido en la Resolución N.º 2 del CCITT (Melbourne, 1988). Además, la Asamblea Plenaria del CCITT, que se celebra cada cuatro años, aprueba las Recomendaciones que se le someten y establece el programa de estudios para el periodo siguiente.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del CCITT, las normas necesarias se preparan en colaboración con la ISO y la CEI. El texto de la Recomendación X.736 del CCITT se aprobó el 17 de enero de 1992. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10164-7

NOTA DEL CCITT

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

© UIT 1992

Es propiedad. Ninguna parte de esta publicación puede producirse o utilizarse, de ninguna forma o por ningún medio, sea éste electrónico o mecánico, de fotocopia o de microfilm, sin previa autorización escrita por parte de la UIT.

ÍNDICE

| | | <i>Página</i> |
|-----|--|---------------|
| 1 | Alcance..... | 1 |
| 2 | Referencias normativas | 2 |
| 2.1 | Pares Recomendación del CCITT Norma Internacional idénticas | 2 |
| 2.2 | Pares Recomendación del CCITT Norma Internacional equivalentes en su contenido técnico | 2 |
| 2.3 | Referencias adicionales..... | 3 |
| 3 | Definiciones | 3 |
| 3.1 | Definiciones del modelo de referencia básico | 3 |
| 3.2 | Definiciones de arquitectura de seguridad..... | 3 |
| 3.3 | Definiciones del marco de gestión..... | 4 |
| 3.4 | Definiciones de conjunto de la gestión de sistemas | 4 |
| 3.5 | Definiciones de la función de gestión de informes de eventos | 4 |
| 3.6 | Definiciones de convenios de servicio..... | 4 |
| 3.7 | Definiciones de pruebas de conformidad OSI | 4 |
| 3.8 | Definiciones adicionales | 4 |
| 4 | Abreviaturas | 4 |
| 5 | Convenios..... | 5 |
| 6 | Requisitos..... | 5 |
| 7 | Modelo | 5 |
| 8 | Definiciones genéricas | 6 |
| 8.1 | Notificaciones genéricas | 6 |
| 8.2 | Objeto gestionado | 9 |
| 8.3 | Definiciones genéricas importadas | 9 |
| 8.4 | Cumplimiento | 9 |
| 9 | Definición de servicio | 9 |
| 9.1 | Introducción..... | 9 |
| 9.2 | Servicio señalador de alarmas de seguridad | 9 |

| | | |
|------|---|----|
| 10 | Unidades funcionales | 10 |
| 11 | Protocolo | 11 |
| 11.1 | Elementos de procedimiento..... | 11 |
| 11.2 | Sintaxis abstracta | 11 |
| 11.3 | Negociación de la unidad funcional de señalación de alarmas de seguridad..... | 14 |
| 12 | Relaciones con otras funciones | 14 |
| 13 | Conformidad | 14 |
| 13.1 | Requisitos de la clase de conformidad general | 14 |
| 13.2 | Requisitos de la clase de conformidad dependiente | 15 |

NOTA DE INFORMACIÓN

El cuadro siguiente incluye una lista de las Recomendaciones de la serie X.700 elaboradas en colaboración con la ISO/CEI y que son idénticas a la Norma Internacional correspondiente. Se dan las referencias a los números de las Normas Internacionales ISO/CEI correspondientes, así como el título abreviado de la Recomendación | Norma Internacional.

| Recomendación del CCITT Norma Internacional ISO/CEI | Título abreviado |
|---|--|
| X.700 7498-4 (NOTA) | Management Framework |
| X.701 10040 | Visión general de la gestión de sistemas |
| X.710 9595 | Definición del servicio común de información de gestión |
| X.711 9596-1 | Especificación del protocolo común de información de gestión |
| X.712 9596-2 | CMIP PICS |
| X.720 10165-1 | Modelo de información de gestión |
| X.721 10165-2 | Definición de la información de gestión |
| X.722 10165-4 | Directrices para la definición de objetos gestionados |
| X.730 10164-1 | Función de gestión de objetos |
| X.731 10164-2 | Función de gestión de estados |
| X.732 10164-3 | Atributos para la representación de relaciones |
| X.733 10164-4 | Función señaladora de alarmas |
| X.734 10164-5 | Event Management Function |
| X.735 10164-6 | Log Control Function |
| X.736 10164-7 | Función señaladora de alarmas de seguridad |
| X.740 10164-8 | Security Audit Trail Function |
| <p>NOTA – Esta Recomendación y la Norma Internacional no son idénticas, pero están alineadas técnicamente. Se señala que los títulos abreviados que figuran en inglés corresponden a Recomendaciones del CCITT que no han sido aprobadas aún.</p> | |

NORMA INTERNACIONAL

RECOMENDACIÓN DEL CCITT

**TECNOLOGÍA DE LA INFORMACIÓN –
INTERCONEXIÓN DE SISTEMAS ABIERTOS –
GESTIÓN DE SISTEMAS: FUNCIÓN SEÑALADORA
DE ALARMAS DE SEGURIDAD**

1 Alcance

Se define en esta Recomendación | Norma Internacional la función señaladora de alarmas de seguridad. La función señaladora de alarmas de seguridad es una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizado o descentralizado para intercambiar información con fines de gestión de sistemas, según se define en la Rec. X.700 del CCITT | ISO/CEI 7498-4. Esta Recomendación | Norma Internacional está situada en la capa de aplicación de CCITT, Rec. X.200 | ISO 7498, y está definida con arreglo al modelo proporcionado por ISO/CEI 9545. El cometido de las funciones de gestión de sistemas está descrito en la Rec. X.701 del CCITT | ISO/CEI 10040. Las notificaciones de alarma de seguridad definidas por esta función de gestión de sistemas proporcionan información sobre la condición operacional y la calidad de servicio, por lo que se refiere a la seguridad.

Los eventos relacionados con la seguridad atañen a la prestación de seguridad. La política de seguridad determina las acciones a emprender cada vez que se produce un evento relacionado con la seguridad. Así, por ejemplo, la política de seguridad puede especificar que se genere un informe de alarma de seguridad, que se registre el evento en un registro de auditoría de seguridad, que se incremente un contador de umbral, que se ignore el evento, o una combinación de estas acciones. Esta Recomendación | Norma Internacional versa únicamente sobre la señalación de alarmas de seguridad.

En esta Recomendación | Norma Internacional:

- se establecen requisitos de usuario para la definición del servicio necesaria para soportar la función de alarmas de seguridad;
- se define el servicio prestado por la función señaladora de alarmas de seguridad;
- se especifica el protocolo necesario para prestar el servicio;
- se define la relación entre las notificaciones de servicio y de gestión;
- se definen relaciones con otras funciones de gestión de sistemas;
- se especifican requisitos de conformidad.

En cambio, en esta Recomendación | Norma Internacional:

- no se define la naturaleza de realización alguna destinada a prestar la función señaladora de alarmas de seguridad;
- no se especifica la manera en que el usuario de la función señaladora de alarmas de seguridad efectúa la gestión;
- no se define la naturaleza de interacción alguna que dé como resultado la utilización de la función señaladora de alarmas de seguridad;
- no se especifican los servicios necesarios para el establecimiento, liberación normal y anormal de una asociación de gestión;
- no se definen notificaciones ya definidas en alguna otra Recomendación | Norma Internacional que pudieran ser de interés para un administrador de seguridad.

2 Referencias normativas

Las Recomendaciones del CCITT y las Normas Internacionales siguientes contienen disposiciones, que mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y las Normas Internacionales son objeto de revisiones, con lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas Internacionales citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Secretaría del CCITT mantiene una lista de las Recomendaciones del CCITT actualmente vigentes.

2.1 Pares Recomendación del CCITT | Norma Internacional idénticas

- Recomendación X.701 del CCITT (1992) | ISO/CEI 10040: 1992, *Tecnología de la información – Interconexión de sistemas abiertos – Visión general de la gestión de sistemas.*
- Recomendación X.721 del CCITT (1992) | ISO/CEI 10165-2: 1992, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: definición de información de gestión.*
- Recomendación X.722 del CCITT (1992) | ISO/CEI 10165-4: 1992, *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la información de gestión: directrices para la definición de objetos gestionados.*
- Recomendación X.733 del CCITT (1992) | ISO/CEI 10164-4: 1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: función señaladora de alarmas.*
- Recomendación X.734¹⁾ del CCITT | ISO/IEC 10164-5 : 1992, *Information technology – Open Systems Interconnection – Systems Management: Event report management function.*
- Recomendación X.735¹⁾ del CCITT | ISO/IEC 10164-6 : 1992, *Information technology – Open Systems Interconnection – Systems Management: Log control function.*

2.2 Pares Recomendación del CCITT | Norma Internacional equivalentes en su contenido técnico

- Recomendación X.200 del CCITT (1988), *Modelo de referencia de interconexión de sistemas abiertos para aplicaciones del CCITT.*
ISO 7498: 1984, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
- Recomendación X.208 del CCITT (1988), *Especificación de la notación de sintaxis abstracta uno (NSA.1).*
ISO/CEI 8824: 1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*

¹⁾ Actualmente en estado de proyecto de Recomendación.

- Recomendación X.209 del CCITT (1988), *Especificación de las reglas básicas de codificación de la notación de sintaxis abstracta uno (NSA.1)*.
ISO/IEC 8825 : 1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
- Recomendación X.210 del CCITT (1988), *Convenios relativos a la definición del servicio de capa en la interconexión de sistemas abiertos*.
ISO/TR 8509: 1987, *Information processing systems – Open Systems Interconnection – Service conventions*.
- Recomendación X.290 del CCITT (1992), *Metodología y marco de las pruebas de conformidad de interconexión de sistemas abiertos de las Recomendaciones sobre los protocolos para aplicaciones del CCITT – Conceptos generales*.
ISO/CEI 9646-1 : 1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework - Part 1: General concepts*.
- Recomendación X.800 del CCITT (1991), *Arquitectura de seguridad de interconexión de sistemas abiertos para aplicaciones del CCITT*.
ISO 7498-2 : 1988, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.
- Recomendación X.700¹⁾ del CCITT, *Management framework definition for Open Systems Interconnection for CCITT applications*.
ISO/CEI 7498-4 : 1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework*.
- CCITT Recomendación X.710 del CCITT (1991), *Definición de servicio de información de gestión común para aplicaciones del CCITT*.
ISO/CEI 9595 : 1991, *Information technology – Open Systems Interconnection – Common management information service definition*.

2.3 Referencias adicionales

- ISO/CEI 9545: 1989, *Information technology – Open Systems Interconnection – Application Layer structure*.

3 Definiciones

A los efectos de la presente Recomendación | Norma Internacional son aplicables las definiciones siguientes:

3.1 Definiciones del modelo de referencia básico

En esta Recomendación | Norma Internacional se utiliza el término siguiente, definido en la Rec. X.200 del CCITT | ISO 7498:

- sistema abierto.

3.2 Definiciones de arquitectura de seguridad

En esta Recomendación | Norma Internacional se utilizan los términos siguientes definidos en la Rec. X.800 del CCITT | ISO 7498-2:

- a) autenticación;
- b) confidencialidad;
- c) integridad;

¹⁾ Actualmente en estado de proyecto de Recomendación.

ISO/CEI 10164-7 : 1992

- d) no repudio;
- e) política de seguridad;
- f) servicio de seguridad.

3.3 Definiciones del marco de gestión

En esta Recomendación | Norma Internacional se utiliza el término siguiente definido en la Rec. X.700 del CCITT | ISO/CEI 7498-4:

- objeto gestionado.

3.4 Definiciones de conjunto de la gestión de sistemas

En esta Recomendación | Norma Internacional se utilizan los términos siguientes definidos en la Rec. X.701 del CCITT | ISO/CEI 10040:

- a) cometido de agente;
- b) conformidad dependiente;
- c) conformidad general;
- d) cometido de gestor;
- e) notificación;
- f) unidad funcional de gestión de sistemas.

3.5 Definiciones de la función de gestión de informes de eventos

En esta Recomendación | Norma Internacional se utiliza el término siguiente definido en la Rec. X.734 del CCITT | ISO/CEI 10164-5:

- discriminador.

3.6 Definiciones de convenios de servicio

En esta Recomendación | Norma Internacional se utilizan los términos siguientes definidos en la Rec. X.210 del CCITT | ISO/TR 8509:

- a) usuario del servicio;
- b) proveedor del servicio.

3.7 Definiciones de pruebas de conformidad OSI

En esta Recomendación | Norma Internacional se utiliza el término siguiente definido en la Rec. X.290 del CCITT | ISO/CEI 9646-1:

- declaración de conformidad del sistema.

3.8 Definiciones adicionales

3.8.1 alarma de seguridad: Evento relacionado con la seguridad que ha sido identificado por una política de seguridad como una posible brecha en la seguridad.

3.8.2 evento relacionado con la seguridad: Evento considerado de incumbencia en relación con la seguridad.

4 Abreviaturas

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

CMIS Servicios comunes de información de gestión (*common management information services*)

| | |
|-------|--|
| Conf | Confirmación |
| Ind | Indicación |
| MAPDU | Unidad de datos de protocolo de aplicación de gestión (<i>management application protocol data unit</i>) |
| OSI | Interconexión de sistemas abiertos (<i>open systems interconnection</i>) |
| Req | Petición (<i>request</i>) |
| Rsp | Respuesta (<i>response</i>) |
| SMAPM | Máquina de protocolo de aplicación de gestión de sistemas (<i>systems management application protocol machine</i>) |

5 Convenios

En esta Recomendación | Norma Internacional se definen servicios para la función señaladora de alarmas de seguridad, utilizando para ello los convenios descriptivos definidos en la Rec. X.210 del CCITT | ISO/TR 8509. En la cláusula 9, la definición de cada servicio incluye un cuadro en el que se indican los parámetros de sus primitivas. Para una primitiva dada, la presencia de cada parámetro está descrita por uno de los valores siguientes:

- M El parámetro es obligatorio (*mandatory*).
- (=) El valor del parámetro es igual al valor del parámetro de la columna de la izquierda.
- U La utilización del parámetro es una opción del usuario del servicio.
 - El parámetro no está presente en la interacción descrita por la primitiva en cuestión.
- C El parámetro es condicional. La (o las) condiciones están definidas en el texto que describe el parámetro.
- P Sujeto a las constricciones impuestas al parámetro por CCITT, Rec. X.710 | ISO/CEI, 9595.

NOTA – A los parámetros marcados con una «P» en el cuadro 2 de esta Recomendación | Norma Internacional se les establece una correspondencia directa con los parámetros correspondientes de la primitiva de servicio CMIS, sin cambiar la semántica o sintaxis de los parámetros. Los parámetros restantes son utilizados para construir una MAPDU.

6 Requisitos

El usuario de la gestión de seguridad necesita ser avisado siempre que se detecte un evento indicador de un ataque o de un ataque potencial contra la seguridad del sistema. Un ataque contra la seguridad puede ser detectado por un servicio de seguridad, por un mecanismo de seguridad, o por otro proceso.

Una notificación de alarma de seguridad puede ser generada por uno de los usuarios finales comunicantes o por cualquier sistema o proceso intermedio situado entre los usuarios finales. El informe de alarma de seguridad identificará la causa de la alarma de seguridad, la fuente de la detección del evento relacionado con la seguridad, los usuarios finales apropiados y la gravedad apreciada en toda operación incertada, ataque contra la seguridad o brecha en la misma, según especifique la política de seguridad.

En esta Recomendación | Norma Internacional se describe la utilización de servicios y técnicas para satisfacer estos requisitos.

7 Modelo

El modelo para la señalación de alarmas de seguridad está definido en la Rec. X.734 del CCITT | ISO/CEI 10164-5. La información puede ser registrada de acuerdo con la Rec. X.735 del CCITT | ISO/CEI 10164-6.

8 Definiciones genéricas

8.1 Notificaciones genéricas

En esta Recomendación | Norma Internacional se define un conjunto de notificaciones de alarma de seguridad genéricas junto con sus parámetros y semántica aplicables.

El conjunto de notificaciones genéricas, parámetros y semántica definidos en esta Recomendación | Norma Internacional permite pormenorizar los parámetros siguientes del servicio M-INFORME-EVENTO, según se define en la Rec. X.710 del CCITT | ISO/CEI 9595:

- tipo de evento;
- información de evento;
- réplica de evento.

Todas las notificaciones son asientos potenciales de un registro cronológico de gestión de sistemas, y en esta Recomendación | Norma Internacional se define una clase de objeto gestionado que responde a tal fin. En la Rec. X.721 del CCITT | ISO/CEI 10165-2 se define una clase de objeto registro de fichero registro cronológico genérico de la que se obtienen todos los asientos, estando especificada la información adicional por los parámetros información de evento y réplica a evento.

8.1.1 Tipo de evento

Este parámetro define el tipo del informe de alarma de seguridad. En esta Recomendación | Norma Internacional se definen los tipos de evento siguientes:

- violación de la integridad: indicación de que puede haber sido modificada, insertada o suprimida información ilegalmente;
- violación operacional: indicación de que la prestación del servicio solicitado no ha sido posible por indisponibilidad, mal funcionamiento o invocación incorrecta del servicio;
- violación física: indicación de que un recurso físico ha sido violado de un modo que sugiere un ataque contra la seguridad;
- violación de servicio o mecanismo de seguridad: indicación de que un servicio o mecanismo de seguridad ha detectado un ataque a la seguridad;
- violación del dominio temporal: indicación de que se ha producido un evento en un momento no esperado o prohibido.

8.1.2 Información de evento

La información de evento específica de notificación está constituida por los parámetros siguientes.

8.1.2.1 Causa de alarma de seguridad

Este parámetro define variantes adicionales como causas probables de la alarma de seguridad. El valor de este parámetro, en combinación con el valor de tipo de evento, determina cuáles son los parámetros que constituyen el balance del informe de evento de alarma de seguridad y cuáles pueden ser los valores de dichos parámetros.

En la cláusula de comportamiento de la definición de clase de objeto serán indicados valores de causa de alarma de seguridad correspondientes a notificaciones. En esta Recomendación | Norma Internacional se definen, para su utilización en el contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040, causas de alarma de seguridad aplicables a muy diversas clases de objetos gestionados. Estos valores están registrados en la Rec. X.721 del CCITT | ISO/CEI 10165-2. La sintaxis de las causas de alarma de seguridad será el tipo de identificador de objeto ASN.1. Cabe la posibilidad de añadir a esta Recomendación | Norma Internacional, y de registrar mediante los procedimientos de registro definidos para los valores de identificador de objeto ASN.1 de la Rec. X.208 del CCITT | ISO/CEI 8824, causas de alarmas de seguridad adicionales a utilizar en el contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040.

Es posible definir fuera del contexto de esta Recomendación | Norma Internacional, y registrar mediante los procedimientos de registro definidos para los valores de identificador de objeto ASN.1 de la Rec. X.208 del CCITT | ISO/CEI 8824, otras causas de alarma de seguridad a utilizar en el contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040.

En el cuadro 1 se indican las causas de alarma de seguridad correspondientes a los tipos de evento especificados en esta Recomendación | Norma Internacional.

Cuadro 1 – Causas de alarma de seguridad

| Tipo de evento | Causas de alarma de seguridad |
|---|--|
| Violación de la integridad | Información duplicada Información faltante Detección de modificación de información Información fuera de secuencia Información no esperada |
| Violación operacional | Denegación de servicio Fuera de servicio Error de procedimiento Razón no especificada |
| Violación física | Manipulación de cable Detección de intrusión Razón no especificada |
| Violación de servicio o de mecanismo de seguridad | Fallo de autenticación Brecha en la confidencialidad Fallo de no repudio Intento de acceso no autorizado Razón no especificada |
| Violación del dominio temporal | Información retardada Clave caducada Actividad a deshora |

En esta Recomendación | Norma Internacional se definen las causas de alarma de seguridad siguientes:

- Fallo de autenticación: indicación de que un intento de autenticación de un usuario ha sido infructuosa.
- Brecha en la confidencialidad: indicación de que puede haber sido leída información por un usuario no autorizado.
- Manipulación de cable: indicación de que ha acaecido una violación física de un medio físico de comunicaciones.
- Información retardada: indicación de que ha sido recibida información más tarde de lo esperado.
- Denegación de servicio: indicación de que ha sido impedida o desautorizada una petición de servicio válida.
- Información duplicada: indicación de haber sido recibida más de una vez un determinado elemento información, lo que podría revelar un ataque de representación.
- Información faltante: indicación de no haber sido recibida información esperada.
- Detección de modificación de información: indicación por ejemplo, de un mecanismo de integridad de datos, de haber sido modificada información.

- Información fuera de secuencia: indicación de haber sido recibida información en una secuencia incorrecta.
- Detección de intrusión: indicación de que, o bien puede haberse entrado ilegalmente en la ubicación del equipo identificado, o bien el equipo mismo ha sido violado.
- Clave caducada: indicación de haber sido presentada o utilizada una clave de cifrado caducada.
- Fallo de no repudio: indicación de haber sido impedida o detenida una comunicación por fallo o indisponibilidad de un servicio de no repudio.
- Actividad a deshora: indicación de que ha habido utilización de recursos en un momento inesperado.
- Fuera de servicio: indicación de que una petición de servicio válida no ha podido ser atendida por indisponibilidad del proveedor de servicio.
- Error de procedimiento: indicación de haber sido utilizado un procedimiento incorrecto en la invocación de un servicio.
- Intento de acceso no autorizado: indicación de que un mecanismo de control de acceso ha detectado un intento ilegal de acceso a un recurso.
- Información inesperada: indicación de haber sido recibida información que no se esperaba.
- Razón no especificada: indicación de que se ha producido un evento no especificado relacionado con la seguridad.

El definidor de clase de objeto gestionado debería elegir la causa de alarma de seguridad más específica aplicable.

8.1.2.2 Gravedad de una alarma de seguridad

Este parámetro define el grado de importancia de la alarma de seguridad recibida por el objeto gestionado. Se definen los niveles de gravedad siguientes:

- Indeterminado: ha sido detectado un ataque contra la seguridad. La integridad del sistema es desconocida.
- Crítico: se ha producido una brecha en la seguridad que ha puesto en peligro el sistema. No es posible seguir suponiendo que el sistema opera correctamente como soporte de la política de seguridad. La gravedad crítica puede implicar a la modificación de información de seguridad sin autorización correcta, la fuga de información vital para la seguridad del sistema (por ejemplo, contraseñas, claves de cifrado privadas, etc.) o brechas en la seguridad física.
- Mayor: ha sido detectada una brecha en la seguridad y han quedado en peligro información o mecanismos importantes.
- Menor: ha sido detectada una brecha en la seguridad y han quedado en peligro información o mecanismos menos importantes.
- Aviso: ha sido detectado un ataque contra la seguridad. No se considera que la seguridad del sistema esté en peligro.

8.1.2.3 Detector de alarmas de seguridad

Este parámetro identifica el detector de la alarma de seguridad.

8.1.2.4 Usuario del servicio

Este parámetro identifica al usuario del servicio cuya petición de servicio ha ocasionado la generación de la alarma de seguridad.

8.1.2.5 Proveedor del servicio

Este parámetro identifica al proveedor del servicio para el que se ha generado alarma de seguridad.

8.1.3 Réplica a evento

En esta Recomendación | Norma Internacional se especifica información de gestión a utilizar en el parámetro de réplica a evento.

8.2 Objeto gestionado

Un registro de alarma de seguridad es una clase de objeto gestionado obtenida de la clase de objeto registro de fichero registro cronológico de eventos definida en la Rec. X.721 del CCITT | ISO/CEI 10165-2. La clase de objeto registro de alarma de seguridad representa información almacenada en ficheros registro cronológico resultante de notificaciones de alarma de seguridad.

8.3 Definiciones genéricas importadas

Se utilizan también los parámetros siguientes, definidos en la Rec. X.733 del CCITT | ISO/CEI 10164-4:

- información adicional;
- texto adicional;
- notificaciones correlacionadas;
- identificador de notificación.

8.4 Cumplimiento

Las definiciones de clase de objeto gestionado soportan las funciones definidas en esta Recomendación | Norma Internacional incorporando la especificación de las notificaciones mediante referencias a las plantillas de notificación definidas en la Rec. X.721 del CCITT | ISO/CEI 10165-2. El mecanismo de referencia está definido en la Rec. X.722 del CCITT | ISO/CEI 10165-4.

Para que cada ejemplar de un informe de alarma de seguridad seleccione el tipo de alarma de seguridad y la causa de alarma de seguridad que refleje más aproximadamente el evento real que origina la emisión de la notificación por el objeto gestionado, se requiere una definición de clase de objeto gestionado que importe una o más notificaciones de alarma de seguridad definidas en esta Recomendación | Norma Internacional.

Para cada notificación importada, la definición de la clase de objeto gestionado especificará, en la cláusula de comportamiento, cuáles de los parámetros optativos y condicionales deben ser utilizados, así como las condiciones para su utilización y los valores de los mismos. Es permisible declarar que el uso de un parámetro sigue siendo optativo.

9 Definición de servicio

9.1 Introducción

En esta Recomendación | Norma Internacional se define un servicio. Las notificaciones de alarma de seguridad hacen posible señalar ataques contra la seguridad, malas operaciones de servicios o mecanismos de seguridad u otros eventos relacionados con la seguridad. Los parámetros transportan la información incumbente a la alarma de seguridad.

9.2 Servicio señalador de alarmas de seguridad

El servicio señalador de alarmas de seguridad utiliza los parámetros definidos en la cláusula 8 de esta Recomendación | Norma Internacional, además de los parámetros generales del servicio M-INFORME-EVENTO definidos en la Rec. X.710 del CCITT | ISO/CEI 9595.

En el cuadro 2 se indican los parámetros correspondientes al servicio señalador de alarmas de seguridad.

Cuadro 2 – Parámetros de señalación de alarmas de seguridad

| Nombre de parámetro | Petición/ indicación | Respuesta/ confirmación |
|--|-------------------------|----------------------------|
| Identificador de invocación | P | P |
| Modo | P | – |
| Clase de objeto gestionado | P | P |
| Ejemplar de objeto gestionado | P | P |
| Tipo de evento | M | C(=) |
| Tiempo de evento | P | – |
| Información de evento Causa de la alarma de seguridad | M | – |
| Gravedad de la alarma de seguridad | M | – |
| Detector de alarmas de seguridad | M | – |
| Usuario del servicio | M | – |
| Proveedor del servicio | M | – |
| Identificador de notificación | U | – |
| Notificaciones correlacionadas | U | – |
| Texto adicional | U | – |
| Información adicional | U | – |
| Tiempo actual | – | P |
| Réplica a evento | – | – |
| Errores | – | P |

Los parámetros tiempo de evento, notificaciones correlacionadas e identificador de notificación pueden ser asignados por el objeto gestionado que emite la notificación, o por el sistema gestionado.

10 Unidades funcionales

La función señaladora de alarmas de seguridad constituye una única unidad funcional de gestión de sistemas.

11 Protocolo

11.1 Elementos de procedimiento

11.1.1 Cometido de agente

11.1.1.1 Invocación

Los procedimientos de señalación de alarmas de seguridad son iniciados por la primitiva petición de señalación de alarmas de seguridad. A la recepción de una primitiva petición de señalación de alarmas de seguridad, la SMAPM construirá una MAPDU y emitirá una primitiva de servicio CMIS petición M-INFORME-EVENTO con parámetros obtenidos de la primitiva petición de señalación de alarmas de seguridad. En modo no confirmado, el procedimiento de 11.1.1.2 no es aplicable.

11.1.1.2 Recepción de una respuesta

A la recepción de una primitiva de servicio CMIS confirmación M-INFORME-EVENTO que contenga una MAPDU que responda a una notificación de señalación de alarma de seguridad, la SMAPM emitirá una primitiva confirmación de señalación de alarma de seguridad destinada al usuario de servicio señalador de alarma de seguridad, con parámetros obtenidos de la primitiva de servicio CMIS confirmación M-INFORME-EVENTO, completando así el procedimiento de señalación de alarma de seguridad.

NOTA – La SMAPM ignorará todos los errores en la MAPDU recibida. El usuario del servicio señalador de alarmas de seguridad puede ignorar dichos errores, o abortar la asociación como consecuencia de ellos.

11.1.2 Cometido de gestor

11.1.2.1 Recepción de una petición

A la recepción de una primitiva de servicio CMIS indicación M-INFORME-EVENTO que contenga una MAPDU que pida el servicio señalador de alarmas de seguridad, la SMAPM emitirá, si la MAPDU está bien formada, una primitiva indicación de señalación de alarma de seguridad con destino al usuario del servicio señalador de alarmas de seguridad, con parámetros obtenidos de la primitiva de servicio CMIS indicación M-INFORME-EVENTO. De no ser así, la SMAPM construirá, en modo confirmado, una MAPDU que contenga notificación del error, y emitirá una primitiva de servicio CMIS respuesta M-INFORME-EVENTO con un parámetro de error presente. En modo no confirmado, el procedimiento de 11.1.2.2 no es aplicable.

11.1.2.2 Respuesta

En modo confirmado, la SMAPM aceptará una primitiva respuesta de señalación de alarma de seguridad y construirá una MAPDU que confirme la notificación y emita una primitiva de servicio CMIS respuesta M-INFORME-EVENTO con los parámetros obtenidos de la primitiva respuesta de señalación de alarma de seguridad.

11.2 Sintaxis abstracta

11.2.1 Objetos gestionados

Esta Recomendación | Norma Internacional hace referencia al objeto de soporte siguiente, cuya sintaxis abstracta está especificada en la Rec. X.721 del CCITT | ISO/CEI 10165-2:

- securityAlarmReportRecord (registro de informe de alarma de seguridad).

11.2.2 Atributos

En el cuadro 3 se identifican las relaciones existentes entre los parámetros definidos en 8.1.2 de esta Recomendación | Norma Internacional y las especificaciones de tipo de atributo de la Rec. X.721 del CCITT | ISO/CEI 10165-2.

Cuadro 3 – Atributos

| Parámetro | Nombre de atributo |
|------------------------------------|-----------------------|
| Causa de la alarma de seguridad | securityAlarmCause |
| Gravedad de la alarma de seguridad | securityAlarmSeverity |
| Detector de alarmas de seguridad | securityAlarmDetector |
| Usuario del servicio | serviceUser |
| Proveedor del servicio | serviceProvider |

11.2.3 Grupos de atributos

No existen grupos de atributos definidos por esta función de gestión de sistemas.

11.2.4 Acciones

No existen acciones específicas definidas por esta función de gestión de sistemas.

11.2.5 Notificaciones

En el cuadro 4 se identifican las relaciones existentes entre las notificaciones definidas en 8.1.1 de esta Recomendación | Norma Internacional y las especificaciones de tipo de notificación de la Rec. X.721 del CCITT | ISO/CEI 10165-2.

Cuadro 4 – Notificaciones

| Tipo de alarma de seguridad | Tipo de notificación |
|--|-------------------------------------|
| Violación de la integridad | integrityViolation |
| Violación operacional | operationalViolation |
| Violación física | physicalViolation |
| Violación de servicio o mecanismo de seguridad | securityServiceOrMechanismViolation |
| Violación del dominio temporal | timeDomainViolation |

La sintaxis abstracta referenciada por las especificaciones de tipo de notificación es transportada en la MAPDU.

11.2.6 Causas de alarma de seguridad

En el cuadro 5 se identifican las relaciones entre las causas de alarma de seguridad definidas en el 8.1.2.1 de esta Recomendación | Norma Internacional y las referencias de valores ASN.1 definidas en la Rec. X.721 del CCITT | ISO/CEI 10165-2.

Cuadro 5 – Causas de alarma de seguridad

| Causa de alarma de seguridad | Referencia de valor ASN.1 |
|--|---------------------------------|
| Fallo de autenticación | authenticationFailure |
| Brecha en la confidencialidad | breachOfConfidentiality |
| Manipulación de cable | cableTamper |
| Información retardada | delayedInformation |
| Denegación de servicio | denialOfService |
| Información duplicada | duplicateInformation |
| Información faltante | informationMissing |
| Detección de modificación de información | informationModificationDetected |
| Información fuera de secuencia | informationOutOfSequence |
| Detección de intrusión | intrusionDetection |
| Clave caducada | keyExpired |
| Fallo de no repudio | nonRepudiationFailure |
| Actividad a deshora | outOfHoursActivity |
| Fuera de servicio | outOfService |
| Error de procedimiento | proceduralError |
| Intento de acceso no autorizado | unauthorizedAccessAttempt |
| Información inesperada | unexpectedInformation |
| Razón no especificada | unspecifiedReason |

11.2.7 Valores de gravedad de alarma de seguridad

En el cuadro 6 se identifican las relaciones entre los valores definidos para el parámetro gravedad de alarma de seguridad de 8.1.2.2 de esta Recomendación | Norma Internacional y las referencias de valores ASN.1 definidos en la Rec. X.721 del CCITT | ISO/CEI 10165-2.

Cuadro 6 – Valores de gravedad de alarma de seguridad

| Gravedad de alarma de seguridad | Referencia de valor ASN.1 |
|---------------------------------|---------------------------|
| Indeterminada | indeterminate |
| Crítica | critical |
| Mayor | major |
| Menor | minor |
| Aviso | warning |

11.3 Negociación de la unidad funcional de señalación de alarmas de seguridad

En esta Recomendación | Norma Internacional se asigna el identificador de objeto

{joint-iso-ccitt ms(9) function(2) part7(7) functionalUnitPackage(1)}

como un valor del tipo ASN.1 FunctionalUnitPackageId definido en la Rec. X.701 del CCITT | ISO/CEI 10040 para su utilización con objeto de negociar la unidad funcional siguiente:

0 unidad funcional de señalación de alarmas de seguridad,

donde el número identifica la posición de bit asignada a la unidad funcional, y el nombre hace referencia a la unidad funcional definida en la cláusula 10.

En el contexto de aplicación de gestión de sistemas, el mecanismo de negociación de la unidad funcional de señalación de alarmas de seguridad está descrito en la Rec. X.701 del CCITT | ISO/CEI 10040.

NOTA – El requisito de negociar unidades funcionales está especificado por el contexto de aplicación.

12 Relaciones con otras funciones

El control del servicio de señalación de alarmas de seguridad se presta mediante mecanismos especificados en la Rec. X.734 del CCITT | ISO/CEI 10164-5. El servicio señalador de alarmas de seguridad puede existir con independencia de los mecanismos de control de la Rec. X.734 del CCITT | ISO/CEI 10164-5.

13 Conformidad

Existen dos clases de conformidad: clase de conformidad general y clase de conformidad dependiente. Para poder decir que un sistema realiza los elementos de procedimiento correspondientes a los servicios de gestión de sistemas definidos en esta Recomendación | Norma Internacional el sistema deberá cumplir los requisitos de la clase de conformidad general o dependiente, según se define en las cláusulas siguientes. El realizador deberá declarar la clase de conformidad que se desea alegar para la realización.

13.1 Requisitos de la clase de conformidad general

Todo sistema que alegue conformidad general con respecto a esta Recomendación | Norma Internacional deberá soportar esta función de gestión de sistemas para todas las clases de objeto gestionado que importen información de gestión definida en esta Recomendación | Norma Internacional.

13.1.1 Conformidad estática

El sistema deberá:

- a) soportar el cometido de gestor o de agente, o ambos, con respecto a la unidad funcional de señalación de alarmas de seguridad;
- b) soportar la sintaxis de transferencia obtenida de las reglas de codificación especificadas en la Rec. X.209 del CCITT | ISO/CEI 8825 y denominadas

{joint-iso-ccitt asn1(1) basic encoding(1)}

con objeto de generar e interpretar las MAPDU, según definen los tipos de datos abstractos referenciados en 11.2.5.

13.1.2 Conformidad dinámica

En el cometido o los cometidos para los que se alega conformidad, el sistema deberá soportar los elementos de procedimiento definidos en esta Recomendación | Norma Internacional correspondientes al servicio señalador de alarmas de seguridad.

13.2 Requisitos de la clase de conformidad dependiente**13.2.1 Conformidad estática**

El sistema deberá:

- a) proporcionar una declaración de conformidad de sistema que identifique el uso normalizado de esta función de gestión de sistemas;
- b) soportar la sintaxis de transferencia obtenida de las reglas de codificación especificadas en la Rec. X.209 del CCITT | ISO/CEI 8825 y denominadas

{joint-iso-ccitt asn1(1) basic encoding(1)}

con objeto de generar e interpretar las MAPDU, según definen los tipos de datos abstractos referenciados en 11.2.5, conforme requiera una utilización normalizada de esta función de gestión de sistemas.

13.2.2 Conformidad dinámica

El sistema deberá soportar los elementos de procedimiento definidos en esta Recomendación | Norma Internacional, conforme requiera una utilización normalizada de esta función de gestión de sistemas.