UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

CCITT

COMITÉ CONSULTIVO
INTERNACIONAL
TELEGRÁFICO Y TELEFÓNICO

X.740

(09/92)

REDES DE COMUNICACIÓN DE DATOS

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – GESTIÓN DE SISTEMAS: FUNCIÓN DE PISTA DE AUDITORÍA DE SEGURIDAD

Recomendación X.740

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.° 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.740 del CCITT se aprobó el 10 de septiembre de 1992. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10164-8.

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 de telecomunicaciones.

Índice

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)	Marco de gestión
X.701 | 10040	Visión general de la gestión de sistemas
X.710 | 9595 (Nota)	Definición del servicio común de información de gestión
X.711 | 9596-1 (Nota)	Especificación de 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	Función de gestión de informes de evento
X.735 | 10164-6	Función de control de ficheros registro cronológico
X.736 | 10164-7	Función señaladora de alarmas de seguridad
X.740 | 10164-8	Función de pista de auditoría de seguridad
NOTA – Esta Recomendación y la Norma Internacional no son idénticas, pero están alineadas técnicamente.	

NORMA INTERNACIONAL

RECOMENDACIÓN DEL CCITT

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – GESTIÓN DE SISTEMAS: FUNCIÓN DE PISTA DE AUDITORÍA DE SEGURIDAD

1 Alcance

Esta Recomendación | Norma Internacional define la función de pista de auditoría de seguridad. La función de pista de auditoría de seguridad es una función de gestión de sistemas que puede ser utilizada por un proceso de aplicación en un entorno de gestión centralizada o descentralizada para intercambiar información e instrucciones a efectos de gestión de sistemas, como se define en la Rec. X.700 del CCITT | ISO/CEI 7498-4. Esta Recomendación | Norma Internacional está posicionada en la capa de aplicación de la Rec. X.200 del CCITT | ISO 7498 y se define de acuerdo con el modelo proporcionado por ISO/CEI 9545. El rol de funciones de gestión de sistemas se describe en la Rec. X.701 del CCITT | ISO/CEI 10040.

Esta Recomendación | Norma Internacional

- establece las exigencias de usuario en cuanto a la definición de servicio que se necesita para soportar la función de señalación de pista de auditoría de seguridad;
- define el servicio proporcionado por la función de señalación de pista de auditoría de seguridad;
- especifica el protocolo necesario para proporcionar el servicio;
- define la relación entre las notificaciones de servicio y de gestión;
- define relaciones con otras funciones de gestión de sistemas;
- especifica requisitos de conformidad.

Esta Recomendación | Norma Internacional no define

- una auditoría de seguridad ni cómo efectuarla. Puede utilizarse una auditoría de seguridad para evaluar la eficacia de una política de seguridad. La política de seguridad identifica las categorías de eventos relacionados con la seguridad que requieren auditoría, y la ubicación del fichero registro cronológico de pistas de auditoría de seguridad en el que han de ser incluidos;
- la naturaleza de toda realización destinada a proporcionar la función de pista de auditoría de seguridad;
- las ocasiones en las que la utilización de la función de pista de auditoría de seguridad es apropiada;
- los servicios necesarios para el establecimiento y la liberación normal y anormal de una asociación de gestión;
- cualesquiera otras notificaciones definidas por otras Recomendaciones | Normas Internacionales que puedan 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 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 Recomendaciones | Normas Internacionales idénticas

- Recomendación X.701 del CCITT (1992) | ISO/CEI 10040-2:1992, *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 la 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.724[1)] del CCITT (1992) | ISO/CEI 10165-6[1)], *Tecnología de la información – Interconexión de sistemas abiertos – Estructura de la Información de Gestión: Requisitos y directrices para los formularios de enunciado de conformidad de realización asociadas con información de gestión*.
- 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.734 del CCITT (1992) | ISO/CEI 10164-5:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de gestión de informes de evento*.
- Recomendación X.735 del CCITT (1992) | ISO/CEI 10164-6:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de control de ficheros registro cronológico*.
- Recomendación X.736 del CCITT (1992) | ISO/CEI 10164-7:1992, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función señaladora de alarmas de seguridad*.

2.2 Pares de Recomendaciones del CCITT | Normas Internacionales de contenido técnico equivalente

- 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 (ASN.1)*.

  ISO/CEI 8824:1990, *Information processing systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)*.
- Recomendación X.209 del CCITT (1988) *Especificación de reglas básicas de codificación de la notación de sintaxis abstracta uno (ASN.1)*.

  ISO/CEI 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 para las Recomendaciones sobre protocolos para aplicaciones del CCITT – Conceptos generales*.

---

1) Actualmente en estado de proyecto.

ISO/CEI 9646-1:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts*.

– Recomendación X.291 del CCITT (1992), *Metodología y marco de las pruebas de conformancia de interconexión de sistemas abiertos de las Recomendaciones sobre protocolos para aplicaciones del CCITT – Especificación de sucesiones de pruebas abstractas*.

ISO/CEI 9646-2:1991, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification*.

– Recomendación X.700, *Marco de gestión para interconexión de sistemas abiertos para aplicaciones del CCITT*.

ISO/CEI 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework*.

– Recomendación X.710 del CCITT (1991), *Definición del servicio común de información de gestión para aplicaciones del CCITT*.

ISO/CEI 9595:1991, *Information technology – Open Systems Interconnection – Common management information service definition*.

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

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

2.3 Referencias adicionales

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

– ISO/CEI 10181-7[2)], *Information technology – Open Systems Interconnection – Security frameworks – Part 7: Security audit framework*.

3 Definiciones

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

3.1 Definiciones del modelo de referencia básico

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

sistema abierto.

3.2 Definiciones de la arquitectura de seguridad

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.800 del CCITT | ISO 7498-2:

a) pista de auditoría de seguridad;

b) política de seguridad.

3.3 Definiciones del marco de gestión

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

objeto gestionado.

---

2) Actualmente en estado de proyecto.

3.4 Definiciones de la visión de conjunto de la gestión de sistemas

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.701 del CCITT | ISO/CEI 10040:

a) cometido de agente;

b) conformidad dependiente;

c) conformidad general;

d) dominio de gestión;

e) cometido de gestor;

f) notificación;

g) unidad funcional de gestión de sistemas.

3.5 Definiciones de la gestión de informes de evento

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

discriminador.

3.6 Definiciones de la señalación de alarmas de seguridad

Esta Recomendación | Norma Internacional utiliza el siguiente término definido en la Rec. X.736 del CCITT | ISO/CEI 10164-7:

evento relacionado con la seguridad.

3.7 Definiciones de control de fichero registro cronológico

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.735 del CCITT | ISO/CEI 10164-6:

a) fichero registro cronológico;

b) registro de fichero registro cronológico.

3.8 Definiciones de las pruebas de conformidad OSI

Esta Recomendación | Norma Internacional utiliza los siguientes términos definidos en la Rec. X.290 del CCITT | ISO/CEI 9646-1:

a) formulario PICS;

b) enunciado de conformidad de realización de protocolo (PICS);

c) enunciado de conformidad de sistema.

4 Abreviaturas

ASN.1	Notación de sintaxis abstracta uno (*abstract syntax notation one*)
CMIS	Servicio común de información de gestión (*common management information services*)
Conf	Confirmación
Ind	Indicación
MAPDU	Unidad de datos de protocolo de aplicación de gestión (*management application protocol data unit*)
MCS	Sumario de conformidad de gestión (*management conformance summary*)
MIDS	Enunciado de definición de información de gestión (*management information definition statement*)

MOCS Enunciado de conformidad de objeto gestionado (*managed object conformance statement*)

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

PICS Enunciado de conformidad de realización de protocolo (*protocol implementation conformance statement*)

Req Petición (*request*)

Rsp Respuesta (*response*)

SMAPM Máquina de protocolo de aplicación de gestión de sistemas (*systems management application protocol machine*)

5 Convenios

Esta Recomendación | Norma Internacional define los servicios para la función de pista de auditoría de seguridad utilizando 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 que contiene los parámetros de sus primitivas. Para una primitiva dada, la presencia de cada parámetro se describe por uno de los siguientes valores.

M El parámetro es obligatorio.

(=) 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 de servicio.

-- El parámetro no aparece en la interacción descrita por la primitiva correspondiente.

C El parámetro es condicional. La condición o condiciones se definen en el texto que describe el parámetro.

P El parámetro está sujeto a las constricciones impuestas por la Rec. X.710 | ISO/CEI 9595.

NOTA – Los parámetros marcados con una «P» en el cuadro 1 de esta Recomendación | Norma Internacional tienen una correspondencia directa con los parámetros correspondientes de la primitiva de servicio CMIS, sin cambiar la semántica ni la sintaxis de los parámetros. Los parámetros restantes se utilizan para construir una MAPDU.

6 Requisitos

El usuario de gestión de seguridad necesita poder incluir, en un fichero registro cronológico de pistas de auditoría de seguridad los eventos relacionados con la seguridad que ocurran en el dominio de gestión. La política de seguridad de un sistema abierto podría requerir que determinados eventos relacionados con la seguridad fuesen enviados a un fichero registro cronológico de pistas de auditoría de seguridad del mismo sistema abierto o de un sistema abierto diferente.

La siguiente es una lista, no exhaustiva, de tipos de eventos relacionados con la seguridad que pueden estar sujetos a una auditoría de seguridad:

– conexiones;

– desconexiones;

– utilización de mecanismos de seguridad;

– operaciones de gestión; y

– contabilización de la utilización.

El usuario de la gestión de seguridad necesita además poder controlar la operación de la función pista de auditoría de seguridad.

Esta Recomendación | Norma Internacional describe el empleo de servicios y técnicas que satisfacen estos requisitos.

7 Modelo

Esta Recomendación | Norma Internacional exige que los eventos relacionados con la seguridad sean incluidos en un fichero registro cronológico de acuerdo con los procedimientos definidos en la Rec. X.735 del CCITT | ISO/CEI 10164-6. El constructivo de discriminador dentro del fichero registro cronológico de pistas de auditoría de seguridad se especificará de tal modo que sea posible la captura de eventos entrantes cuya inclusión en fichero registro cronológico sea requerida por la política de seguridad. Si los informes de eventos han de enviarse a diferentes destinos, se crearán los discriminadores de envío de eventos definidos en la Rec. X.734 del CCITT | ISO/CEI 10164-5 y la dirección de destino se fijará de modo que los eventos se envíen al sistema en el que se halle el fichero registro cronológico de pistas de auditoría de seguridad seleccionado. El fichero registro cronológico de pistas de auditoría de seguridad es un fichero registro cronológico como los definidos en la Rec. X.735 del CCITT | ISO/CEI 10164-6.

El modelo para llevar informes de eventos al sistema en el que se halla el fichero registro cronológico de pistas de auditoría de seguridad se define en la Rec. X.734 del CCITT | ISO/CEI 10164-5. El modelo para la creación y recuperación de inscripciones (asientos) en el fichero registro cronológico de pistas de auditoría de seguridad se define en la Rec. X.735 del CCITT | ISO/CEI 10164-6.

8 Definiciones genéricas

8.1 Notificaciones genéricas

Esta Recomendación | Norma Internacional define un conjunto de notificaciones genéricas de pistas de auditoría de seguridad así como sus parámetros y semántica aplicables.

El conjunto de notificaciones genéricas, parámetros y semánticas definidos por esta Recomendación | Norma Internacional proporciona el detalle de los siguientes parámetros del servicio M-INFORME-EVENTO definido en la Rec. X.710 del CCITT | ISO/CEI 9595.

- tipo de evento;
- información de evento;
- respuesta a evento.

Todas las notificaciones son entradas potenciales en un fichero registro cronológico de gestión de sistemas. La Rec. X.721 del CCITT | ISO/CEI 10165-2 define una clase de objeto, registro de fichero registro cronológico de eventos, genérica, de la que se derivan todas las inscripciones, 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 de informe de pista de auditoría de seguridad. En esta Recomendación | Norma Internacional se definen los siguientes tipos de evento:

- Informe de servicio: una indicación de un evento relacionado con la prestación, denegación o recuperación de un servicio. En el 8.1.2 se describen causas específicas de la generación del evento;
- Informe de utilización: una indicación de un registro que contiene información de naturaleza estadística, de interés para la seguridad.

En el fichero registro cronológico de pistas de auditoría de seguridad pueden anotarse otras informaciones definidas en otras Recomendaciones | Normas Internacionales (por ejemplo, la Rec. X.736 del CCITT | ISO/CEI 10164-7). Los tipos de notificación (análogos a los tipos de informe de pista de auditoría de seguridad) y sus parámetros asociados se definen en las Recomendaciones | Normas Internacionales apropiadas.

8.1.2 Información de evento

El parámetro causa de informe de servicio constituye la información de evento específica de la notificación.

Este parámetro se suministrará cuando el tipo de evento especifica un informe de servicio, y define una mayor cualificación en lo tocante a la causa probable del informe de servicio. El valor de este parámetro en combinación con el valor del tipo de evento, determina qué parámetros constituyen el balance del informe de servicio y cuáles son los valores posibles que esos parámetros pueden adoptar.

Los valores de la causa de informe de servicio para las notificaciones se indicarán en la cláusula de comportamiento de la definición de la clase de objeto. Esta Recomendación | Norma Internacional define, para su utilización dentro del contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040, causas de informe de servicio que tienen una gran aplicabilidad en clases de objeto gestionado. Estos valores se indican en el anexo A a la presente Recomendación | Norma Internacional. La sintaxis de las causas de informe de servicio será el identificador de objeto de tipo ASN.1. Pueden añadirse a esta Recomendación | Norma Internacional otras causas de informe de servicio, para uso en el contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040, y registrarse utilizando los procedimientos de registro definidos en la Rec. X.208 del CCITT | ISO/CEI 8824 para valores de identificador de objeto ASN.1.

Otras causas de informe de servicio, para uso dentro del contexto de aplicación de gestión de sistemas definido en la Rec. X.701 del CCITT | ISO/CEI 10040, pueden ser definidas fuera de esta Recomendación | Norma Internacional y registradas utilizando los procedimientos de registro definidos en la Rec. X.208 | ISO/CEI 8824 para valores de identificador de objeto ASN.1.

Se han definido los siguientes valores de causa de informe de servicio:

- Petición de servicio: este valor especifica que la notificación ha sido generada debido a una petición de prestación de un servicio.
- Denegación de servicio: este valor especifica que la notificación ha sido generada porque una petición de servicio ha sido denegada.
- Respuesta de servicio: este valor especifica que la notificación ha sido generada porque una petición de servicio ha sido satisfecha.
- Fallo de servicio: este valor especifica que la notificación ha sido generada porque durante la prestación de un servicio se detectó una condición anormal que provocó el fallo del servicio.
- Recuperación de servicio: este valor especifica que la notificación ha sido generada porque un servicio se ha recuperado de una condición anormal.
- Otro motivo (o razón): este valor especifica que la notificación ha sido generada por motivos (razones) distintos a los arriba indicados. La causa efectiva y otra información pertinente se especifican en otros parámetros del informe.

8.1.3 Réplica a evento

Esta Recomendación | Norma Internacional no especifica la información de gestión que se utiliza en el parámetro réplica a evento.

8.2 Objeto gestionado

Un registro de pista de auditoría de seguridad es una clase de objeto gestionado derivada de la clase de objeto registro de fichero registro cronológico definida en la Rec. X.721 del CCITT | ISO/CEI 10165-2. La clase de objeto récord de pista de auditoría de seguridad representa información almacenada en ficheros registro cronológico resultantes de notificaciones de pistas de auditoría de seguridad.

8.3 Definiciones genéricas importadas

También se utilizan los parámetros que a continuación se indican. Estos parámetros se definen 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 la referencia a las plantillas de notificación definidas en el anexo A. El mecanismo de referencia se define en la Rec. X.722 del CCITT | ISO/CEI 10165-4.

Se requiere una definición de clase de objeto gestionado que importa una o más de las notificaciones de pista de auditoría de seguridad, definidas en esta Recomendación | Norma Internacional, para cada ejemplar de un informe de pista de auditoría de seguridad para seleccionar el tipo de informe de pista de auditoría de seguridad que refleja más fielmente el evento real que conduce a que el objeto gestionado que emite la notificación. La definición de la clase de objeto gestionado deberá especificar, para cada notificación importada, en la cláusula de comportamiento, qué parámetros opcionales y condicionales deben utilizarse, las condiciones para su uso y sus valores. Es admisible enunciar que el uso de un parámetro sigue siendo opcional.

9 Definición de servicio

9.1 Introducción

Las notificaciones de pista de auditoría de seguridad permiten señalar eventos relacionados con la seguridad, detectados por un objeto gestionado. Los parámetros llevan la información pertinente a la pista de auditoría de seguridad.

9.2 Servicio de señalación de pista de auditoría de seguridad

El servicio de señalación de pista de auditoría 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 1 figura la lista de parámetros del servicio de señalación de pista de auditoría de seguridad.

Cuadro 1 – Parámetros de señalación de pista de auditoría de seguridad

Parámetro	Pet/Ind	Rsp/Conf
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 informe del servicio	C	–
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 pista de auditoría de seguridad constituye una unidad funcional simple 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 pista de auditoría de seguridad son iniciados por la primitiva petición de señalación de pista de auditoría de seguridad. Al recibirse una primitiva petición de señalación de pista de auditoría de seguridad, la SMAPM construye una MAPDU y emite una primitiva de servicio CMIS petición M-INFORME-EVENTO, con parámetros derivados de la primitiva petición de señalación de pista de auditoría de seguridad. En el modo no confirmado no es aplicable el procedimiento de 11.1.1.2.

11.1.1.2 Recepción de respuesta

Al recibirse una primitiva de servicio CMIS confirmación M-INFORME-EVENTO que contiene una MAPDU que responde a una notificación de señalación de pista de auditoría de seguridad, la SMAPM emitirá una primitiva confirmación de señalación de pista de auditoría de seguridad al usuario del servicio de señalación de pista de auditoría de seguridad, con parámetros derivados de la primitiva de servicio CMIS confirmación M-INFORME-EVENTO, completando así el procedimiento de señalación de pista de auditoría de seguridad.

NOTA – La SMAPM ignorará todos los errores de la MAPDU recibida. El usuario del servicio de señalación de pista de auditoría de seguridad puede ignorar tales errores, o abortar la asociación a consecuencia de los mismos.

11.1.2 Cometido de gestor

11.1.2.1 Recepción de petición

Al recibirse una primitiva de servicio CMIS indicación M-INFORME-EVENTO que contiene una MAPDU en la que se pide el servicio de señalación de pista de auditoría de seguridad, la SMAPM emite, si la MAPDU está bien formada, una primitiva indicación de señalación de pista de auditoría de seguridad al usuario del servicio de señalación de pista de auditoría de seguridad con parámetros derivados de la primitiva de servicio CMIS indicación M-INFORME-EVENTO. En otro caso, la SMAPM deberá construir, en el modo confirmado, una MAPDU que contenga una notificación del error y emitir una primitiva de servicio CMIS respuesta M-INFORME-EVENTO con un parámetro de error presente. En el modo no confirmado no es aplicable el procedimiento de 11.1.2.2.

11.1.2.2 Respuesta

En el modo confirmado, la SMAPM aceptará una primitiva respuesta de señalación de pista de auditoría de seguridad y construirá una MAPDU confirmando la notificación y emitirá una primitiva de servicio CMIS respuesta M-INFORME-EVENTO con los parámetros derivados de la primitiva respuesta de señalación de pista de auditoría de seguridad.

11.2 Sintaxis abstracta

11.2.1 Objetos gestionados

Esta Recomendación | Norma Internacional define el siguiente objeto de soporte, cuya sintaxis abstracta se especifica en el anexo A.

securityAuditTrailRecord (registro de pista de auditoría de seguridad).

11.2.2 Atributos

El cuadro 2 identifica la relación entre el parámetro definido en 8.1.2 y la especificación de tipo de atributo del anexo A.

Cuadro 2 – Atributos

Parámetro	Nombre de atributo
Causa de informe de servicio	serviceReportCause

11.2.3 Grupos de atributos

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

11.2.4 Acciones

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

11.2.5 Notificaciones

El cuadro 3 identifica la relación entre las notificaciones definidas en 8.1.1 y las especificaciones de tipo de notificación del anexo A.

Cuadro 3 – Notificaciones

Tipo de pista de auditoría de seguridad	Tipo de notificación
Informe de servicio	serviceReport
Informe de utilización	usageReport

La sintaxis abstracta referenciada por las especificaciones de tipo de notificación se transporta en la MAPDU.

11.2.6 Causas de informe de servicio

El cuadro 4 identifica la relación entre las causas de informe de servicio definidas en 8.1.2 y las referencias de valor ASN.1 definidas en el anexo A.

Cuadro 4 – Causas de informe de servicio

Causa de informe de servicio	Referencia de valor ASN.1
Petición de servicio	serviceRequest
Denegación de servicio	serviceDenial
Respuesta del servicio	serviceResponse
Fallo de servicio	serviceFailure
Recuperación del servicio	serviceRecovery
Otro motivo (u otra razón)	otherReason

11.3 Negociación de unidad funcional de señalación de pista de auditoría de seguridad

Esta Recomendación | Norma Internacional asigna el identificador de objeto

{joint-iso-ccitt ms(9)function(2)part8(8)functionalUnitPackage(1)}

como un valor del tipo ASN.1 FunctionalUnitPackageId (identificador de lote de unidades funcionales) definido en la Rec. X.701 del CCITT | ISO/CEI 10040 que ha de utilizarse para negociar la siguiente unidad funcional:

0 unidad funcional de señalación de pista de auditoría de seguridad

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

Dentro del contexto de aplicación de gestión de sistemas, el mecanismo para negociar la unidad funcional de señalación de pista de auditoría de seguridad se describe en la Rec. X.701 del CCITT | ISO/CEI 10040.

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

12 Relaciones con otras funciones

El control del servicio de señalación de pista de auditoría de seguridad lo proporcionan los mecanismos especificados en la Rec. X.734 del CCITT | ISO/CEI 10164-5. La modificación de los atributos de registro fichero cronológico de pistas de auditoría de seguridad está prevista en la Rec. X.735 del CCITT | ISO/CEI 10164-6.

El servicio de notificación de pista de auditoría de seguridad puede existir independientemente de los servicios de control de la Rec. X.734 del CCITT | ISO/CEI 10164-5, y de la Rec. X.735 del CCITT | ISO/CEI 10164-6.

13 Conformidad

Hay dos clases de conformidad: la clase de conformidad general y la clase de conformidad dependiente. Un sistema que alega la realización de los elementos de procedimiento para la unidad funcional de señalación de pista de auditoría de seguridad definida en esta Recomendación | Norma Internacional debe satisfacer los requisitos de la clase de conformidad general y de la clase de conformidad dependiente, definidos en las cláusulas siguientes. El suministrador de la realización deberá enunciar la clase para la que alega la conformidad.

NOTA – Se está reexaminando la utilización de los dos términos «clase de conformidad general» y «clase de conformidad dependiente». No obstante, esta norma continúa utilizando estos términos a fin de mantener la armonía con la Rec. X.701 del CCITT | ISO/CEI 10040 y otras normas bajo el título general *Tecnología de la Información* – Interconexión de sistemas abiertos – gestión de sistemas. Una vez que se haya aprobado lo reexaminado se tiene el propósito de aclarar y/o corregir esta cláusula de conformidad, así como las cláusulas conexas de otras normas.

13.1 Requisitos de la clase de conformidad general

Un sistema que alegue la conformidad general con esta Recomendación | Norma Internacional deberá soportar esta función de gestión de sistemas para todas las clases de objeto gestionado que importan información de gestión definida por esta Recomendación | Norma Internacional.

13.1.1 Conformidad estática

El sistema:

a) soportará el cometido de gestor o el cometido de agente o ambos, con respecto a la unidad funcional de señalación de pista de auditoría de seguridad;

b) soportará la sintaxis de transferencia derivada de las reglas de codificación especificadas en la Rec. X.209 del CCITT | ISO/CEI 8825 y denominada

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

para generar e interpretar las MAPDU, definida por los tipos de datos abstractos referenciados en 11.2.5.

13.1.2 Conformidad dinámica

El sistema soportará los elementos de los procedimientos definidos en esta Recomendación | Norma Internacional para el servicio de señalación de pista de auditoría de seguridad en el (o en los) cometidos para los que se alega la conformidad.

13.2 Requisitos de la clase de conformidad dependiente

13.2.1 Conformidad estática

El sistema soportará la sintaxis de transferencia derivada de las reglas de codificación especificadas en la Rec. X.209 del CCITT | ISO/CEI 8825 y denominada

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

para generar e interpretar las MAPDU, definida por los tipos de datos abstractos referenciados en 11.2.5 de esta Recomendación | Norma Internacional, según lo requiera una especificación referenciante.

13.2.2 Conformidad dinámica

El sistema soportará los elementos de procedimiento definidos en esta Recomendación | Norma Internacional, según lo requiera una especificación referenciante.

13.3 Requisitos de conformidad de información de gestión

Un formulario MCS que sea conforme a esta Recomendación | Norma Internacional será textualmente idéntico al anexo B, del que sólo se diferenciará en la paginación y los encabezamientos de página. Un formulario MOCS de la clase de objeto registro de señalación de pista de auditoría de seguridad que sea conforme a esta Recomendación | Norma Internacional deberá ser textualmente idéntico al formulario MOCS especificado en el anexo C, del que sólo diferirá en la paginación y en los encabezamientos de página. Un formulario MIDS de notificación de pista de auditoría de seguridad que sea conforme a esta Recomendación | Norma Internacional será textualmente idéntico al formulario MIDS especificado en el anexo D, del que sólo diferirá en la paginación y en los encabezamientos de página. Un sistema que sea conforme a esta Recomendación | Norma Internacional:

- describirá una realización que sea conforme a esta Recomendación | Norma Internacional;
- será un formulario MCS, MOCS o MIDS conforme que ha sido completado de acuerdo con las instrucciones para compleción dadas en la Rec. X.724 | ISO/CEI 10165-6;
- incluirá la información necesaria para identificar de manera unívoca tanto al suministrador como a la realización.

El suministrador de una realización que se pretenda conforme con esta Recomendación | Norma Internacional completará una copia del formulario de conformidad de información de gestión que figura en el anexo B, como parte de los requisitos de conformidad, y proporcionará la información necesaria para identificar al suministrador y a la realización.

13.4 Requisitos del PICS

Un formulario PICS que sea conforme a esta Recomendación | Norma Internacional será textualmente idéntico al anexo E, del que sólo se diferenciará en la paginación y los encabezamientos de página. Un PICS que sea conforme a esta Recomendación | Norma Internacional deberá:

- ser conforme con un formulario PICS que haya sido completado de acuerdo con las instrucciones para compleción que figuran en E.1;
- incluir la información necesaria para identificar unívocamente tanto el suministrador como la realización.

El suministrador de una realización de protocolo para la que pretenda la conformidad con esta Recomendación | Norma Internacional completará una copia del formulario PICS proporcionado en el anexo E como parte de los requisitos de conformidad, y proporcionará la información necesaria para identificar el suministrador y la realización.

Anexo A
Definición de información de gestión

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

A.1 Adjudicación de identificadores de objeto

Esta Recomendación | Norma Internacional adjudica los siguientes identificadores de objeto:

SecurityAuditTrailDefinitions {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 1}
DEFINITIONS ::= BEGIN

securityAuditTrail-Object OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3)}
securityAuditTrail-Package OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) package(4)}
securityAuditTrail-Attribute OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)}
securityAuditTrail-Notification OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) notification(10)}

serviceReportCause OBJECT IDENTIFIER ::= {joint-iso-ccitt ms(9) function(2) part8(8) standardSpecificExtension(0) 1}

-- Los siguientes valores OBJECT IDENTIFIER pueden utilizarse como valores del parámetro de causa de informe de -- servicio en A.5.

serviceRequest ServiceReportCause ::= {serviceReportCause 1}
serviceDenial ServiceReportCause ::= {serviceReportCause 2}
serviceResponse ServiceReportCause ::= {serviceReportCause 3}
serviceFailure ServiceReportCause ::= {serviceReportCause 4}
serviceRecovery ServiceReportCause ::= {serviceReportCause 5}
otherReason ServiceReportCause ::= {serviceReportCause 6}

END

A.2 Definición de clases de objeto gestionado

La clase de objeto securityAuditTrailRecord (registro de pista de auditoría de seguridad) se utiliza para definir la información almacenada en un fichero registro cronológico como resultado de notificaciones de pista de auditoría de seguridad o informes de evento.

securityAuditTrailRecord MANAGED OBJECT CLASS
    DERIVED FROM "CCITT Rec. X.721 | ISO/IEC 10165-2 : 1992":eventLogRecord;
    CONDITIONAL PACKAGES
        serviceReportCausePackage PACKAGE
        BEHAVIOUR
            serviceReportCausePackageBehaviour BEHAVIOUR
                DEFINED AS "This package provides further qualification as to the probable cause of a service report.";
            ;
        ATTRIBUTES serviceReportCause GET;
        REGISTERED AS {securityAuditTrail-Package 1};
        PRESENT IF "This package shall be present if the notification concerns a service report.";

REGISTERED AS {securityAuditTrail-Object 1};

A.3 Definición de atributos

serviceReportCause ATTRIBUTE
    WITH ATTRIBUTE SYNTAX SecurityAuditTrail-ASN1Module.ServiceReportCause;
    MATCHES FOR EQUALITY;
    BEHAVIOUR
    serviceReportCauseBehaviour BEHAVIOUR
        DEFINED AS "This attribute is used to provide the reason for the service report. The value of this attribute is an OBJECT IDENTIFIER that has been registered by a registration authority. Some of the possible values of this attribute are specified by, and registered in this Recommendation | International Standard.";
    ;
REGISTERED AS {securityAuditTrail-Attribute 1};

A.4 Definición de tipos de notificación

A.4.1 Informe de servicio

serviceReport NOTIFICATION

BEHAVIOUR serviceReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

serviceReportCause serviceReportCause,

notificationIdentifier notificationIdentifier,

correlatedNotifications correlatedNotifications,

additionalText additionalText,

additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 1};

serviceReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information about a service request, denial, response, recovery or other information which is relevant to the security administrator.";

A.4.2 Informe de utilización

usageReport NOTIFICATION

BEHAVIOUR usageReportBehaviour;

WITH INFORMATION SYNTAX SecurityAuditTrail-ASN1Module.SecurityAuditInfo

AND ATTRIBUTE IDS

notificationIdentifier notificationIdentifier,

correlatedNotifications correlatedNotifications,

additionalText additionalText,

additionalInformation additionalInformation;

REGISTERED AS {securityAuditTrail-Notification 2};

usageReportBehaviour BEHAVIOUR

DEFINED AS "This notification type is used to report information of a statistical nature which is relevant to the security administrator.";

A.5 Definiciones de sintaxis abstracta

```
SecurityAuditTrail-ASN1Module {joint-iso-ccitt ms(9) function(2) part8(8) asn1Module(2) 2}
DEFINITIONS ::= BEGIN
IMPORTS
AdditionalText, AdditionalInformation, CorrelatedNotifications, NotificationIdentifier
FROM Attribute-ASN1Module {joint-iso-ccitt ms(9) smi(3) part2(2) asn1Module(2) 1}

SecurityAuditInfo ::= SEQUENCE {  serviceReportCause      IMPLICIT ServiceReportCause OPTIONAL,
                                  notificationIdentifier  IMPLICIT NotificationIdentifier OPTIONAL,
                                  correlatedNotifications [1] IMPLICIT CorrelatedNotifications OPTIONAL,
                                  additionalText          IMPLICIT AdditionalText OPTIONAL,
                                  additionalInformation   [2] IMPLICIT AdditionalInformation OPTIONAL }

ServiceReportCause ::= OBJECT IDENTIFIER

END
```

Anexo B
Formulario MCS[3)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

B.1 Introduction

B.1.1 Symbols, abbreviations and terms

The following abbreviations are used throughout the proformas:

o.N	(N is an INTEGER) support of at least one of the choices is required
dmi-att	**joint-iso-ccitt ms(9) smi(3) part2(2) attribute(7)**
dmi-nb	**joint-iso-ccitt ms(9) smi(3) part2(2) nameBinding(6)**
dmi-pkg	**joint-iso-ccitt ms(9) smi(3) part2(2) package(4)**
satf-att	**joint-iso-ccitt ms(9) function(2) part8(8) attribute(7)**
satf-not	**joint-iso-ccitt ms(9) function(2) part8(8) notification(10)**

B.1.2 Table format

Some of the tables in Annexes C and D have been split because the information is too wide to fit on the page. Where this occurs, the index number of the first block of columns has a lower case “a” appended, and index number of the second block of columns has a lower case “b” appended. A complete table reconstructed from the constituent parts should have the following layout.

Index	Columns associated with “a”	Columns associated with “b”

B.2 Identification of the implementation

B.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

B.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

3) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MCS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MCS cumplimentado. En la Rec. X.724 del CCITT | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MCS.

B.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the MCS, in the box below.

B.3 Identification of the Recommendation | International Standard in which the management information is defined

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard which specifies the management information to which conformance is claimed, in the box below.

Recommendation | International Standard to which conformance is claimed

B.3.1 Technical corrigenda implemented

The supplier of the implementation shall enter the reference numbers of implemented technical corrigenda which modify the identified Recommendation | International Standard, in the box below.

B.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to the identified Recommendation | International Standard, in the box below.

B.4 Management conformance summary

The supplier of the implementation shall provide information on whether the implementation claims conformance to any of the set of Recommendations | International Standards globally representing the implementation under claim. For each Recommendation | International Standard the supplier of the implementation claims conformance to, the corresponding conformance statement(s) shall be completed, or referenced, by the MCS. The supplier of the implementation shall complete the Support and Additional information columns.

Identification of the Recommendation | International Standard that includes the proforma	Reference of MOCS proforma	Managed object class template label	Status	Support	Additional information
CCITT Rec. X.740 | ISO/IEC 10164-8	Annex C	securityAuditTrailRecord	m		

Anexo C
Formulario MOCS[4)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

C.1 Statement of conformance to the managed object class

Managed object class template label	Value of OBJECT IDENTIFIER for the class
securityAuditTrailRecord	**{joint-iso-ccitt ms(9) function(2) part8(8) managedObjectClass(3) 1}**

The supplier of the implementation shall state whether or not all mandatory features of the security audit trail record are supported, in Table C.1.

Table C.1 – Feature support

Index		Support
C.1.1	Are all mandatory features of the managed object class supported?	
C.1.2	Do instances of the managed object class support allomorphism?	

C.2 Name bindings

The supplier of the implementation shall state which name bindings in which instances of the managed object class can be subordinate are supported, in the Support and Additional information columns of Table C.2.

Table C.2 – Name binding support

Index	Name binding template label	Value of OBJECT IDENTIFIER for name binding	Superior object class template label	Status	Support
C.2.1a	logRecord-log	**{dmi-nb 3}**	"CCITT Rec. X.721 | ISO/IEC 10165-2 : 1992":log AND SUBCLASSES	o	

Table C.2 (concluded) – Name binding support

	Status		Support		
Index	Object creation	Object deletion	Object creation	Object deletion	Additional information
C.2.1b	x	m			

4) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MOCS de este anexo a fin de que pueda ser utilizado para los fines previstos, y pueden además publicar el MOCS cumplimentado. En la Rec. X.724 del CCITT | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MOCS.

C.3 Packages

The supplier of the implementation shall state whether or not the packages specified by this managed object of this class are supported, in Table C.3.

Table C.3 – Package support

Index	Package label	Value of OBJECT IDENTIFIER	Status	Support
C.3.1	eventTimePackage	**{dmi-pkg 11}**	o	
C.3.2	notificationIdentifierPackage	**{dmi-pkg 24}**	o	
C.3.3	correlatedNotificationsPackage	**{dmi-pkg 23}**	o	
C.3.4	additionalTextPackage	**{dmi-pkg 19}**	o	
C.3.5	additionalInformationPackage	**{dmi-pkg 18}**	o	

C.4 Attributes

The supplier of the implementation shall state whether or not the attributes specified by all of the packages instantiated in a managed object of this class are supported, in the Support and Additional information columns of Table C.4. The supplier of the implementation shall indicate support for each of the operations for each attribute supported.

Table C.4 – Attribute support

			Status					
Index	Attribute template label	Value of OBJECT IDENTIFIER	SetByCreate	Get	Replace	Add	Remove	SetToDefault
C.4.1a	objectClass	**{dmi-att 65}**	x	m	x	x	x	x
C.4.2a	nameBinding	**{dmi-att 63}**	x	m	x	x	x	x
C.4.3a	packages	**{dmi-att 66}**	x	c1	x	x	x	x
C.4.4a	allomorphs	**{dmi-att 50}**	x	c2	x	x	x	x
C.4.5a	logRecordId	**{dmi-att 3}**	x	m	x	x	x	x
C.4.6a	loggingTime	**{dmi-att 59}**	x	m	x	x	x	x
C.4.7a	managedObjectClass	**{dmi-att 60}**	x	m	x	x	x	x
C.4.8a	managedObjectInstance	**{dmi-att 61}**	x	m	x	x	x	x
C.4.9a	eventType	**{dmi-att 14}**	x	m	x	x	x	x
C.4.10a	eventTime	**{dmi-att 13}**	x	c3	x	x	x	x
C.4.11a	notificationIdentifier	**{dmi-att 16}**	x	c4	x	x	x	x
C.4.12a	correlatedNotifications	**{dmi-att 12}**	x	c5	x	x	x	x
C.4.13a	additionalText	**{dmi-att 7}**	x	c6	x	x	x	x
C.4.14a	additionalInformation	**{dmi-att 6}**	x	c7	x	x	x	x
C.4.15a	serviceReportCause	**{satf-att 1}**	x	m	x	x	x	x

c1: if C.3.1 or C.3.2 or C.3.3 or C.3.4 or C.3.5 then m else –
c2: if C.1.2 then m else –
c3: if C.3.1 then m else –
c4: if C.3.2 then m else –
c5: if C.3.3 then m else –
c6: if C.3.4 then m else –
c7: if C.3.5 then m else –

Table C.4 (concluded) – Attribute support

	Support						
Index	SetByCreate	Get	Replace	Add	Remove	SetToDefault	Additional information
C.4.1b							
C.4.2b							
C.4.3b							
C.4.4b							
C.4.5b							
C.4.6b							
C.4.7b							
C.4.8b							
C.4.9b							
C.4.10b							
C.4.11b							
C.4.12b							
C.4.13b							
C.4.14b							
C.4.15b							

C.5 Attribute groups

There are no attribute groups specified for this managed object class.

C.6 Actions

There are no actions specified for this managed object class.

C.7 Notifications

There are no notifications specified for this managed object class.

C.8 Parameters

There are no parameters specified for this managed object class.

Anexo D
Formulario MIDS (notificación)[5)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

The specifier of a managed object class that claims to support the notifications specified by CCITT Rec. X.740 | ISO/IEC 10164-8 shall import a copy of this annex and complete it according to the instructions specified in CCITT Rec. X.724 | ISO/IEC 10165-6.

Table D.1 – Notification support

			Support			
Index	Notification template label	Value of OBJECT IDENTIFIER	Status	Confirmed	Non-confirmed	Additional information
D.1.1a	serviceReport	**{satf-not 1}**				
D.1.1.1a	–	–	–	–	–	–
D.1.1.2a	–	–	–	–	–	–
D.1.1.3a	–	–	–	–	–	–
D.1.1.4a	–	–	–	–	–	–
D.1.1.5a	–	–	–	–	–	–
D.1.2a	usageReport	**{satf-not 2}**				
D.1.2.1a	–	–	–	–	–	–
D.1.2.2a	–	–	–	–	–	–
D.1.2.3a	–	–	–	–	–	–
D.1.2.4a	–	–	–	–	–	–
D.1.2.5a	–	–	–	–	–	–

Table D.1 (concluded) – Notification support

Index	Notification field name label	OBJECT IDENTIFIER value of attribute type associated with the field	Status	Support	Additional information
D.1.1b	–	–	–	–	–
D.1.1.1b	ServiceReportCause	**{satf-att 1}**	m		
D.1.1.2b	NotificationIdentifier	**{dmi-att 16}**	o		
D.1.1.3b	CorrelatedNotifications	**{dmi-att 12}**	o		
D.1.1.4b	AdditionalText	**{dmi-att 7}**	o		
D.1.1.5b	AdditionalInformation	**{dmi-att 6}**	o		
D.1.2b	–	–	–	–	–
D.1.2.2a	ServiceReportCause	**{satf-att 1}**	–	–	–
D.1.2.2b	NotificationIdentifier	**{dmi-att 16}**	o		
D.1.2.3b	CorrelatedNotifications	**{dmi-att 12}**	o		
D.1.2.4b	AdditionalText	**{dmi-att 7}**	o		
D.1.2.5b	AdditionalInformation	**{dmi-att 6}**	o		

5) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de MIDS de este anexo a fin de que pueda ser utilizado para los fines previstos. En la Rec. X.724 del CCITT | ISO/CEI 10165-6 se especifican las instrucciones para rellenar el formulario de MIDS.

Anexo E
Formulario PICS[6)]

(Este anexo es parte integrante de esta Recomendación | Norma Internacional)

E.1 Instructions for completing the PICS proforma

E.1.1 Purpose and structure

The purpose of this PICS proforma is to provide a mechanism whereby a supplier of an implementation of CCITT Rec. X.740 | ISO/IEC 10164-8 may provide information in a standard form. The PICS proforma is subdivided into clauses for the following categories of information:

– implementation details;

– protocol details;

– overall conformance claim;

– implementation capabilities.

E.1.2 Symbols, abbreviations and terms

The PICS proforma contained in this annex is comprised of information in a tabular form in accordance with the guidelines presented in CCITT Rec. X.291 | ISO/IEC 9646-2. The following abbreviations are used:

Spt	Support
Sts	Status
TVR	Type(s), value(s) and range(s)

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the status (Sts) column:

m	mandatory
o	optional
o.N	(N is an integer) support of at least one of the choices is required
x	prohibited
–	not applicable

The following requirements are commonly used throughout the PICS proforma:

c1	if E.5.1 then m else –
c2	if E.5.2 or E.5.3 then m else –

The following common notations, defined in CCITT Rec. X.291 | ISO/IEC 9646-2, are used for the support (Spt) column:

N	not implemented
Y	implemented
–	not applicable

Within this PICS proforma, space has been provided for the supplier of the implementation to specify types, values and ranges of all parameters supported. It is recommended that references to additional specifications are included where appropriate (for example, to list the OBJECT IDENTIFIER values and/or ranges supported), and that these additional specifications be appended to the completed PICS proforma.

E.1.3 Scoping rules

In the Status column of the tables in this Recommendation | International Standard, a mandatory element contained within an optional or conditional constructor parameter is mandatory only if the option or condition is taken.

---

6) Los usuarios de esta Recomendación | Norma Internacional pueden reproducir libremente el formulario de PICS de este anexo a fin de que pueda ser utilizado para los fines previstos y pueden además publicar el PICS cumplimentado.

E.1.4 Instructions for completing the PICS

The supplier of the implementation shall enter an explicit statement in each of the boxes provided using the notation described in E.1.2. Specific instruction is provided in the text which preceeds each table.

E.2 Identification of the implementation

E.2.1 Date of statement

The supplier of the implementation shall enter the date of this statement in the box below. Use the format DD-MM-YYYY.

Date of statement

E.2.2 Identification of the implementation

The supplier of the implementation shall enter information necessary to uniquely identify the implementation and the system(s) in which it may reside, in the box below.

E.2.3 Contact

The supplier of the implementation shall provide information on whom to contact if there are any queries concerning the content of the PICS, in the box below.

E.2.4 Relationship with the system conformance statement

The supplier of the implementation shall provide information which describes the relationship between the PICS and the system conformance statement for the system, in the box below.

E.3 Identification of the protocol

The supplier of the implementation shall enter the title, reference number and date of the publication of the Recommendation | International Standard to which conformance is claimed, in the box below.

Recommendation | International Standard to which conformance is claimed

E.3.1 Defect reports implemented

The supplier of the implementation shall enter the reference numbers of implemented defect reports which modify the specification to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

E.3.2 Amendments implemented

The supplier of the implementation shall state the titles and reference numbers of implemented amendments to CCITT Rec. X.740 | ISO/IEC 10164-8, in the box below.

E.4 Global statement of conformance

The supplier of the implementation shall state whether or not all mandatory capabilities are implemented for CCITT Rec. X.740 | ISO/IEC 10164-8, in Table E.1.

Table E.1 – Capabilities

Index		Support
E.1.1	Are all mandatory capabilities implemented?	

NOTE – Answering NO to this question indicates non-conformance to the protocol standard. Non-supported mandatory capabilities are listed in the PICS below, explaining why the status of the implementation is abnormal.

Capability not implemented	Reason

E.5 Capabilities

E.5.1 Systems management functional unit support

The supplier of the implementation shall state the capability for supporting the security audit trail reporting functional unit, in Table E.2.

Table E.2 – SMFU support

Index	Functional unit name	Status	MAPDU support	CMIS support	Support
E.2.1	Security audit trail reporting functional unit	m	serviceReport usageReport	M-EVENT-REPORT	

E.5.2 Systems management functional unit negotiation support

The supplier of the implementation shall state the capability for negotiating the use of the security audit trail reporting functional unit, in Table E.3.

Table E.3 – SMFU negotiation support

Index	Negotiation capability	Status	Support
E.3.1	Does the implementation support the negotiation of the systems management functional unit?	o	

E.5.3 Management roles

The supplier of the implementation shall state the management role for which conformance is claimed, in Table E.4.

Table E.4 – Management role support

		Status		Support	
Index	Functional unit name	Manager	Agent	Manager	Agent
E.4.1	Security audit trail reporting functional unit	o.1	o.1		

E.5.4 Parameter support

The supplier of the implementation shall state support for sending the identified parameters, in Table E.5.

Table E.5 – Parameter support

Index	Parameter name	Status	Support
E.5.1	CorrelatedNotifications	o	
E.5.2	AdditionalText	o	
E.5.3	AdditionalInformation	o	

E.5.5 MAPDU support

The supplier of the implementation shall state support for the MAPDUs in the management role(s) for which conformance is claimed, in Table E.6.

Table E.6 – MAPDU support

		Status		Support	
Index	MAPDU name	Manager	Agent	Manager	Agent
E.6.1	serviceReport	o.2	o.2		
E.6.2	usageReport	o.3	o.3		

If support for the serviceReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.7. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.7 – Service report MAPDU (sending)

Index	Parameter name	Sts	Value	Spt	TVR
E.7.1	SecurityAuditInfo	–	–	–	–
E.7.1.1	serviceReportCause	m			
E.7.1.2	notificationIdentifier	c1			
E.7.1.3	correlatedNotifications	o			
E.7.1.3.1	correlatedNotifications	m			
E.7.1.3.2	sourceObjectInst	o			
E.7.1.3.2.1	distinguishedName	o.4			
E.7.1.3.2.2	nonSpecificForm	o.4			
E.7.1.3.2.3	localDistinguishedName	o.4			
E.7.1.4	additionalText	c2			
E.7.1.5	additionalInformation	c2			
E.7.1.5.1	identifier	m			
E.7.1.5.2	significance	m			
E.7.1.5.3	information	m			

If support for the serviceReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.8. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.8 – Service report MAPDU (receiving)

Index	Parameter name	Sts	Value	Spt	TVR
E.8.1	SecurityAuditInfo	–	–	–	–
E.8.1.1	serviceReportCause	m			
E.8.1.2	notificationIdentifier	m			
E.8.1.3	correlatedNotifications	m			
E.8.1.3.1	correlatedNotifications	m			
E.8.1.3.2	sourceObjectInst	m			
E.8.1.3.2.1	distinguishedName	m			
E.8.1.3.2.2	nonSpecificForm	m			
E.8.1.3.2.3	localDistinguishedName	m			
E.8.1.4	additionalText	m			
E.8.1.5	additionalInformation	m			
E.8.1.5.1	identifier	m			
E.8.1.5.2	significance	m			
E.8.1.5.3	information	m			

If support for the usageReport MAPDU in the agent role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.9. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.9 – Usage report MAPDU (sending)

Index	Parameter name	Sts	Value	Spt	TVR
E.9.1	SecurityAuditInfo	–	–	–	–
E.9.1.1	serviceReportCause	–	–	–	–
E.9.1.2	notificationIdentifier	c1			
E.9.1.3	correlatedNotifications	o			
E.9.1.3.1	correlatedNotifications	m			
E.9.1.3.2	sourceObjectInst	o			
E.9.1.3.2.1	distinguishedName	o.5			
E.9.1.3.2.2	nonSpecificForm	o.5			
E.9.1.3.2.3	localDistinguishedName	o.5			
E.9.1.4	additionalText	c2			
E.9.1.5	additionalInformation	c2			
E.9.1.5.1	identifier	m			
E.9.1.5.2	significance	m			
E.9.1.5.3	information	m			

If support for the usageReport MAPDU in the manager role is claimed, then the supplier of the implementation shall state whether or not each parameter of the MAPDU is supported in Table E.10. The supplier of the implementation shall indicate the type, value(s) and range(s) of each parameter.

Table E.10 – Usage report MAPDU (receiving)

Index	Parameter name	Sts	Value	Spt	TVR
E.10.1	SecurityAuditInfo	–	–	–	–
E.10.1.1	serviceReportCause	–	–	–	–
E.10.1.2	notificationIdentifier	m			
E.10.1.3	correlatedNotifications	m			
E.10.1.3.1	correlatedNotifications	m			
E.10.1.3.2	sourceObjectInst	m			
E.10.1.3.2.1	distinguishedName	m			
E.10.1.3.2.2	nonSpecificForm	m			
E.10.1.3.2.3	localDistinguishedName	m			
E.10.1.4	additionalText	m			
E.10.1.5	additionalInformation	m			
E.10.1.5.1	identifier	m			
E.10.1.5.2	significance	m			
E.10.1.5.3	information	m			

Anexo F
Relación con el marco de auditoría de seguridad

(Este anexo no es parte integrante de esta Recomendación | Norma Internacional)

Esta Recomendación | Norma Internacional proporciona facilidades para la inclusión en fichero registro cronológico de eventos relacionados con la seguridad y que son de uso potencial en una auditoría de seguridad. No define una auditoría de seguridad ni cómo efectuarla. Esta Recomendación | Norma Internacional es justamente una de las facilidades que pueden utilizarse para incluir eventos relacionados con la seguridad que pueden ser de interés para una auditoría de seguridad.

ISO | CEI 10181-7 define los conceptos y objetivos de una auditoría de seguridad y proporciona una descripción de las funciones de auditoría de seguridad. Así pues, ISO | CEI 10181-7 describe lo que puede hacerse con la información asociada a los eventos relacionados con la seguridad, y no cómo registrar esa información.