UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T X.816

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(11/95)

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

SEGURIDAD

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE AUDITORÍA Y ALARMAS DE SEGURIDAD

Recomendación UIT-T X.816

(Anteriormente «Recomendación del CCITT»)

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. En el UIT-T, que es la entidad que establece normas mundiales (Recomendaciones) sobre las telecomunicaciones, participan unos 179 países miembros, 84 empresas de explotación de telecomunicaciones, 145 organizaciones científicas e industriales y 38 organizaciones internacionales.

Las Recomendaciones las aprueban los Miembros del UIT-T de acuerdo con el procedimiento establecido en la Resolución N.° 1 de la CMNT (Helsinki, 1993). Adicionalmente, la Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, aprueba las Recomendaciones que para ello se le sometan 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 UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI. El texto de la Recomendación UIT-T X.816 se aprobó el 21 de noviembre de 1995. Su texto se publica también, en forma idéntica, como Norma Internacional ISO/CEI 10181-7.

NOTA

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

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS Y COMUNICACIÓN ENTRE SISTEMAS ABIERTOS

(Febrero de 1994)

ORGANIZACIÓN DE LAS RECOMENDACIONES DE LA SERIE X

Dominio	Recomendaciones
REDES PÚBLICAS DE DATOS	
Servicios y facilidades	X.1-X.19
Interfaces	X.20-X.49
Transmisión, señalización y conmutación	X.50-X.89
Aspectos de redes	X.90-X.149
Mantenimiento	X.150-X.179
Disposiciones administrativas	X.180-X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Modelo y notación	X.200-X.209
Definiciones de los servicios	X.210-X.219
Especificaciones de los protocolos en modo conexión	X.220-X.229
Especificaciones de los protocolos en modo sin conexión	X.230-X.239
Formularios para enunciados de conformidad de implementación de protocolo	X.240-X.259
Identificación de protocolos	X.260-X.269
Protocolos de seguridad	X.270-X.279
Objetos gestionados de capa	X.280-X.289
Pruebas de conformidad	X.290-X.299
INTERFUNCIONAMIENTO ENTRE REDES	
Generalidades	X.300-X.349
Sistemas móviles de transmisión de datos	X.350-X.369
Gestión	X.370-X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400-X.499
DIRECTORIO	X.500-X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	
Gestión de redes	X.600-X.649
Denominación, direccionamiento y registro	X.650-X.679
Notación de sintaxis abstracta uno	X.680-X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700-X.799
SEGURIDAD	X.800-X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	
Cometimiento, concurrencia y recuperación	X.850-X.859
Tratamiento de transacciones	X.860-X.879
Operaciones a distancia	X.880-X.899
TRATAMIENTO ABIERTO DISTRIBUIDO	X.900-X.999

ÍNDICE

Resumen

La presente Recomendación | Norma Internacional describe un modelo básico para tratar las alarmas de seguridad y para efectuar una auditoría de seguridad para sistemas abiertos. Una auditoría de seguridad es una revisión y un examen independientes de los registros y actividades del sistema. El servicio de auditoría de seguridad otorga a una autoridad de auditoría la capacidad de especificar, seleccionar y gestionar los eventos que tienen que ser registrados en un rastreo de auditoría de seguridad.

Introducción

Esta Recomendación | Norma Internacional depura el concepto de auditoría de seguridad descrito en la Rec. UIT-T X.810 | ISO/CEI 10181-1, que incluye la detección de eventos y las acciones resultantes de los mismos. Por lo tanto, el marco trata de la auditoría de seguridad y de las alarmas de seguridad.

Una auditoría de seguridad es un análisis y examen independientes de los registros y actividades del sistema. Los objetivos de una auditoría de seguridad son los siguientes:

- facilitar la identificación y análisis de las acciones o ataques no autorizados;
- ayudar a garantizar que las acciones puedan atribuirse a las entidades responsables de esas acciones;
- contribuir al desarrollo de los procedimientos mejorados de control de daños;
- confirmar el cumplimiento de la política de seguridad establecida;
- notificar cualquier información que pueda indicar insuficiencias en los controles del sistema; y
- determinar los posibles cambios necesarios de controles, política y procedimientos.

En este marco, una auditoría de seguridad consiste en la detección, recopilación y registro de diversos eventos relacionados con la seguridad de los sistemas abiertos en un rastreo de auditoría de seguridad y el análisis de esos eventos.

Tanto la auditoría como la imputabilidad requieren que se registre la información. Una auditoría de seguridad garantiza que se registra la información relativa a eventos de rutina y excepcionales, para que las investigaciones posteriores puedan determinar si se han producido violaciones de seguridad y, en caso afirmativo, determinar qué información u otros recursos han sido comprometidos. La imputabilidad garantiza el registro de la información pertinente relativa a acciones ejecutadas por los usuarios o procesos que actúan en su nombre, de modo que las consecuencias de tales acciones puedan ser vinculadas más tarde al usuario o usuarios en cuestión, y que éstos puedan ser responsables de sus acciones. La provisión de un servicio de auditoría de seguridad puede contribuir a la provisión de imputabilidad.

Una alarma de seguridad es un aviso emitido a un individuo o a un proceso para indicar que ha surgido una situación que puede requerir una acción oportuna. La finalidad de un servicio de alarmas de seguridad incluye:

- informar sobre los intentos reales o aparentes de violar la seguridad;
- informar sobre diversos eventos relacionados con la seguridad, incluidos los eventos «normales»; e
- informar sobre los eventos activados porque se alcanzan límites de umbral.

NORMA INTERNACIONAL

RECOMENDACIÓN UIT-T

TECNOLOGÍA DE LA INFORMACIÓN – INTERCONEXIÓN DE SISTEMAS ABIERTOS – MARCOS DE SEGURIDAD PARA SISTEMAS ABIERTOS: MARCO DE AUDITORÍA Y ALARMAS DE SEGURIDAD

1 Alcance

Esta Recomendación | Norma Internacional trata de la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde el término «sistemas abiertos» incluye bases de datos, aplicaciones distribuidas, procesamiento distribuido abierto e interconexión de sistemas abiertos. Los marcos de seguridad definen los medios necesarios para proporcionar protección para sistemas y objetos dentro de sistemas y las interacciones entre sistemas. Los marcos de seguridad no se relacionan con la metodología de construcción de sistemas o mecanismos.

Los marcos de seguridad tratan de elementos de datos y de secuencias de operaciones (pero no de elementos de protocolo) que se utilizan para obtener servicios de seguridad específicos. Estos servicios de seguridad pueden aplicarse a entidades comunicantes de sistemas, así como a datos intercambiados entre sistemas y a datos gestionados por sistemas.

La finalidad de la auditoría y las alarmas de seguridad, tal como se describe en esta Recomendación | Norma Internacional, es garantizar que los eventos relacionados con la seguridad de sistemas abiertos se gestionan con arreglo a la política de seguridad de la autoridad de seguridad aplicable.

En particular, este marco:

a) define los conceptos básicos de auditoría y alarmas de seguridad;

b) proporciona un modelo general para auditoría y alarmas de seguridad; y

c) determina la relación del servicio de auditoría y alarmas de seguridad con otros servicios de seguridad.

Como ocurre con otros servicios de seguridad, una auditoría de seguridad sólo se puede proporcionar en el contexto de una política de seguridad definida.

El modelo de auditoría y alarmas de seguridad proporcionado en la cláusula 6 de este marco admite varios objetivos, no todos los cuales son necesarios o deseables en un entorno concreto. El servicio de auditoría de seguridad proporciona una autoridad de auditoría con capacidad para especificar los eventos que necesitan ser registrados en un rastreo de auditoría de seguridad.

Existen varios tipos diferentes de normas que utilizan este marco:

1) las normas que incorporan el concepto de auditoría y alarmas;

2) las normas que especifican servicios abstractos que incluyen auditoría y alarmas;

3) las normas que especifican usos de auditoría y alarmas;

4) las normas que especifican el medio para proporcionar auditoría y alarmas en una arquitectura de sistema abierto; y

5) las normas que especifican mecanismos de auditoría y alarmas.

Estas normas pueden utilizar este marco de la forma siguiente:

– los tipos de normas 1), 2), 3), 4) y 5) pueden utilizar la terminología de este marco;

– los tipos de normas 2), 3), 4) y 5) pueden utilizar las facilidades definidas en la cláusula 8; y

– el tipo de norma 5) puede basarse en las características de mecanismos definidos en la cláusula 9.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales 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 Normas son objeto de revisiones, por 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 citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

2.1 Recomendaciones | Normas Internacionales idénticas

- Recomendación UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*
- 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 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.*
- Recomendación X.740 del CCITT (1992) | ISO/CEI 10164-8:1993, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Función de pista de auditoría de seguridad.*
- Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos – Visión general.*

2.2 Pares de Recomendaciones | Normas Internacionales de contenido técnico equivalente

- Recomendación X.700 del CCITT (1992), *Marco de gestión para la 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.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.*

3 Definiciones

A los efectos de esta Recomendación | Norma Internacional, se aplican las definiciones siguientes.

3.1 Definiciones del modelo de referencia básico

La presente Recomendación | Norma Internacional utiliza los términos siguientes definidos en la Rec. UIT-T X.200 | ISO/CEI 7498-1:

a) entidad;

b) facilidad;

c) función;

d) servicio.

3.2 Definiciones de la arquitectura de seguridad

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

a) imputabilidad;

b) disponibilidad;

c) auditoría de seguridad;

d) rastreo de auditoría de seguridad;

e) política de seguridad.

3.3 Definiciones del marco de gestión

Esta Recomendación | Norma Internacional utiliza los términos siguientes definidos en la Rec. UIT-T X.700 del CCITT | ISO/CEI 7498-4:

– objeto gestionado.

3.4 Definiciones de la visión general del marco de seguridad

Esta Recomendación | Norma Internacional utiliza los términos siguientes definidos en la Rec. UIT-T X.810 | ISO/CEI 10181-1:

– dominio de seguridad.

3.5 Definiciones adicionales

A los efectos de la presente Recomendación | Norma Internacional, se aplican las definiciones siguientes:

3.5.1 procesador de alarmas: Función que genera una acción adecuada en respuesta a una alarma de seguridad y genera un mensaje de auditoría de seguridad.

3.5.2 autoridad de auditoría: Gestor responsable de definir los aspectos de una política de seguridad aplicable a la realización de una auditoría de seguridad.

3.5.3 analizador de auditoría: Función que comprueba un rastreo de auditoría de seguridad para producir, en caso necesario, mensajes de alarma de seguridad y mensajes de auditoría de seguridad.

3.5.4 archivador de auditoría: Función que archiva una parte del rastreo de auditoría de seguridad.

3.5.5 expedidor de auditoría: Función que transfiere partes o la totalidad de un rastreo de auditoría de seguridad distribuido a la función de colector de rastreo de auditoría.

3.5.6 examinador de rastreo de auditoría: Función que elabora informes de seguridad de uno o más rastreos de auditoría de seguridad.

3.5.7 registrador de auditoría: Función que genera registros de auditoría de seguridad y los almacena en un rastreo de auditoría de seguridad.

3.5.8 proveedor de auditoría: Función que proporciona registros de rastreo de auditoría de seguridad con arreglo a ciertos criterios.

3.5.9 colector de rastreo de auditoría: Función que recopila registros de un rastreo de auditoría distribuido en un rastreo de auditoría de seguridad.

3.5.10 discriminador de eventos: Función que proporciona un análisis inicial de un evento relacionado con la seguridad y, si procede, genera un mensaje de auditoría y/o de alarma de seguridad.

3.5.11 alarma de seguridad: Mensaje generado cuando se ha detectado un evento relacionado con seguridad que está definido por la política de seguridad como una condición de alarma. Una alarma de seguridad está concebida para informar a las entidades adecuadas de forma oportuna.

3.5.12 administrador de alarmas de seguridad: Individuo o proceso que determina la disposición de las alarmas de seguridad.

3.5.13 evento relacionado con la seguridad: Cualquier evento que la política de seguridad ha definido como una violación potencial de la seguridad, o que pueda ser pertinente a la seguridad. Un ejemplo de evento relacionado con seguridad es cuando se alcanza un valor de umbral predefinido.

3.5.14 mensaje de auditoría de seguridad: Mensaje generado como resultado de un evento relacionado con la seguridad auditable.

3.5.15 registro de auditoría de seguridad: Un único registro en un rastreo de auditoría de seguridad.

3.5.16 auditor de seguridad: Individuo o proceso al que se le permite acceder al rastreo de auditoría de seguridad y elaborar informes de auditoría.

3.5.17 informe de seguridad: Informe que resulta del análisis del rastreo de auditoría de seguridad y puede ser utilizado para determinar si se ha producido una violación de la seguridad.

4 Abreviaturas

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

5 Notación

Mientras no se especifique otra cosa, los términos «servicio» y «mecanismo» se utilizan para indicar un «servicio de auditoría de seguridad» y un «mecanismo de auditoría de seguridad», respectivamente. Asimismo, mientras no se especifique otra cosa, el término «auditoría» indica una «auditoría de seguridad» y el término «alarma», una «alarma de seguridad».

6 Análisis general de la auditoría y las alarmas de seguridad

Esta cláusula describe un modelo para tratar alarmas de seguridad y para realizar una auditoría de seguridad para sistemas abiertos.

Una auditoría de seguridad permite evaluar la adecuación de la política de seguridad, prestar ayuda en la detección de violaciones de seguridad, facilitar que los individuos se responsabilicen de sus acciones (o de las acciones de entidades que actúan en su nombre), ayudar a detectar el uso incorrecto de recursos, y actuar como un factor disuasivo para aquellos individuos que pudieran intentar dañar el sistema. Los mecanismos de auditoría de seguridad no participan directamente en la prevención de las violaciones de seguridad; están relacionados con la detección, el registro y el análisis de eventos. Esto permite realizar cambios de procedimientos operativos en respuesta a eventos anormales como son las violaciones de seguridad.

Una alarma de seguridad se genera cuando se detecta un evento relacionado con seguridad que ha sido definido por la política de seguridad como una condición de alarma. Esto podría incluir el caso cuando se alcanza un umbral predefinido. Algunos de estos eventos pueden requerir una acción de restablecimiento inmediato, mientras que otros pueden requerir una investigación ulterior para determinar, si fuera el caso, la acción requerida.

Para aplicar el modelo de auditoría y alarmas de seguridad, puede ser necesario utilizar otros servicios de seguridad para apoyar al servicio de auditoría y alarmas de seguridad y para garantizar su funcionamiento correcto y asegurado. Esta cuestión se trata más adelante en la cláusula 10.

Aunque los rastreos de auditoría de seguridad y las auditorías de seguridad tienen características especiales, otros rastreos de auditoría y auditorías (que no son de seguridad) pueden utilizar las facilidades y mecanismos descritos en este marco.

Como ocurre con otros aspectos de la seguridad, la eficacia máxima se consigue garantizando que se diseñan requisitos de auditoría de seguridad específicos en el sistema. Por lo tanto, los diseñadores de sistemas deben tener en cuenta la necesidad de auditar (es decir, la disponibilidad de examinar y analizar) tanto el proceso de diseño como el sistema en desarrollo.

NOTA – El modelo de auditoría y de alarmas de seguridad no muestra cómo se relacionan otras características de gestión y funcionamiento del sistema con este modelo.

6.1 Modelo y funciones

El modelo presentado a continuación ilustra las funciones utilizadas en la prestación de un servicio de auditoría y alarmas de seguridad.

6.1.1 Funciones de auditoría y alarmas de seguridad

Son necesarias varias funciones para apoyar un servicio completo de auditoría y alarmas de seguridad, a saber:

- el **discriminador de eventos** que proporciona un análisis inicial del evento y determina si hay que enviar el evento al registrador de auditoría o al procesador de alarmas;
- el **registrador de auditoría** que genera registros de auditoría a partir de mensajes recibidos y almacena los registros en un rastreo de auditoría de seguridad;
- el **procesador de alarmas** que genera un mensaje de auditoría y una acción adecuada en respuesta a una alarma de seguridad;
- el **analizador de auditoría** que comprueba un rastreo de auditoría de seguridad y, en caso necesario, produce alarmas de seguridad y mensajes de auditoría de seguridad;
- el **examinador de rastreo de auditoría**, que elabora informes de seguridad a partir de uno o más rastreos de auditoría de seguridad;
- el **proveedor de auditoría**, que proporciona registros de auditoría con arreglo a ciertos criterios; y
- el **archivador de auditoría** que archiva parte de un rastreo de auditoría de seguridad.

Pueden ser necesarias las siguientes funciones adicionales para rastreos y alarmas de auditoría de seguridad:

- el **colector de rastreo de auditoría**, que recopila registros de un rastreo de auditoría distribuido en un rastreo de auditoría de seguridad; y
- el **expedidor de auditoría** que transfiere partes o la totalidad de un rastreo de auditoría de seguridad distribuido a la función de colector de rastreo de auditoría.

6.1.2 Modelo de auditoría y alarmas de seguridad

El modelo de auditoría y alarmas de seguridad descrito más adelante comprende varias fases. Una vez que se ha detectado un evento, debe determinarse si el evento es pertinente o no a la seguridad. El *discriminador de eventos* evalúa el evento para determinar si debe generarse un mensaje de auditoría de seguridad y/o un mensaje de alarma de seguridad. Los mensajes de auditoría de seguridad se envían al *registrador de auditoría*: las alarmas de seguridad se envían al *procesador de alarmas* para proceder a su evaluación y ejecutar las acciones necesarias. A continuación, se formatan los mensajes de auditoría de seguridad y se transforman en registros de auditoría de seguridad que serán incluidos en el rastreo de auditoría de seguridad. Se pueden archivar las partes más antiguas del rastreo de auditoría de seguridad, y el rastreo de auditoría de seguridad así como los archivos del mismo pueden utilizarse para elaborar informes de auditoría, seleccionando determinados registros de rastreo de auditoría de seguridad con arreglo a criterios especificados. Es decir, se puede analizar el rastreo de auditoría de seguridad y se puede generar informes de auditoría de seguridad y/o alarmas de seguridad. En la Figura 1 se muestra el modelo de auditoría y alarmas de seguridad.

6.1.3 Agrupación de las funciones de auditoría y alarmas de seguridad

Las funciones mostradas en el modelo se pueden coubicar en un componente de un sistema o distribuirlas entre varios componentes del sistema. Estas funciones se pueden ubicar también en diferentes sistemas extremos y se pueden duplicar. En algunos casos, por consideraciones relacionadas con la calidad de funcionamiento, será ventajoso que las funciones estén agrupadas. En particular, un *registrador de auditoría*, un *expedidor de auditoría* y un *proveedor de auditoría* y un *analizador de auditoría* que funcionan en el mismo rastreo de auditoría de seguridad pueden formar parte de un sistema extremo no atendido.

Otra agrupación que resultaría útil al auditor de seguridad podría comprender un *examinador de rastreo de auditoría* y un *analizador de auditoría*.

Una disposición posible podría ser una cadena de funciones ordenadas de forma jerárquica, especialmente en una auditoría de seguridad distribuida (véase la Figura 2). En este caso, un *colector de rastreo de auditoría* de un componente recopila mensajes de auditoría del *expedidor de auditoría* de otro componente. Esta cadena finaliza cuando un componente no admite un *expedidor de auditoría*, ya que en este caso el componente debe admitir un *archivador de auditoría* que pueda archivar su rastreo de auditoría de seguridad.

La decisión sobre las funciones que se han de agrupar, si las hubiere, es una cuestión de la implementación. Los ejemplos anteriores sirven sólo como ilustración.

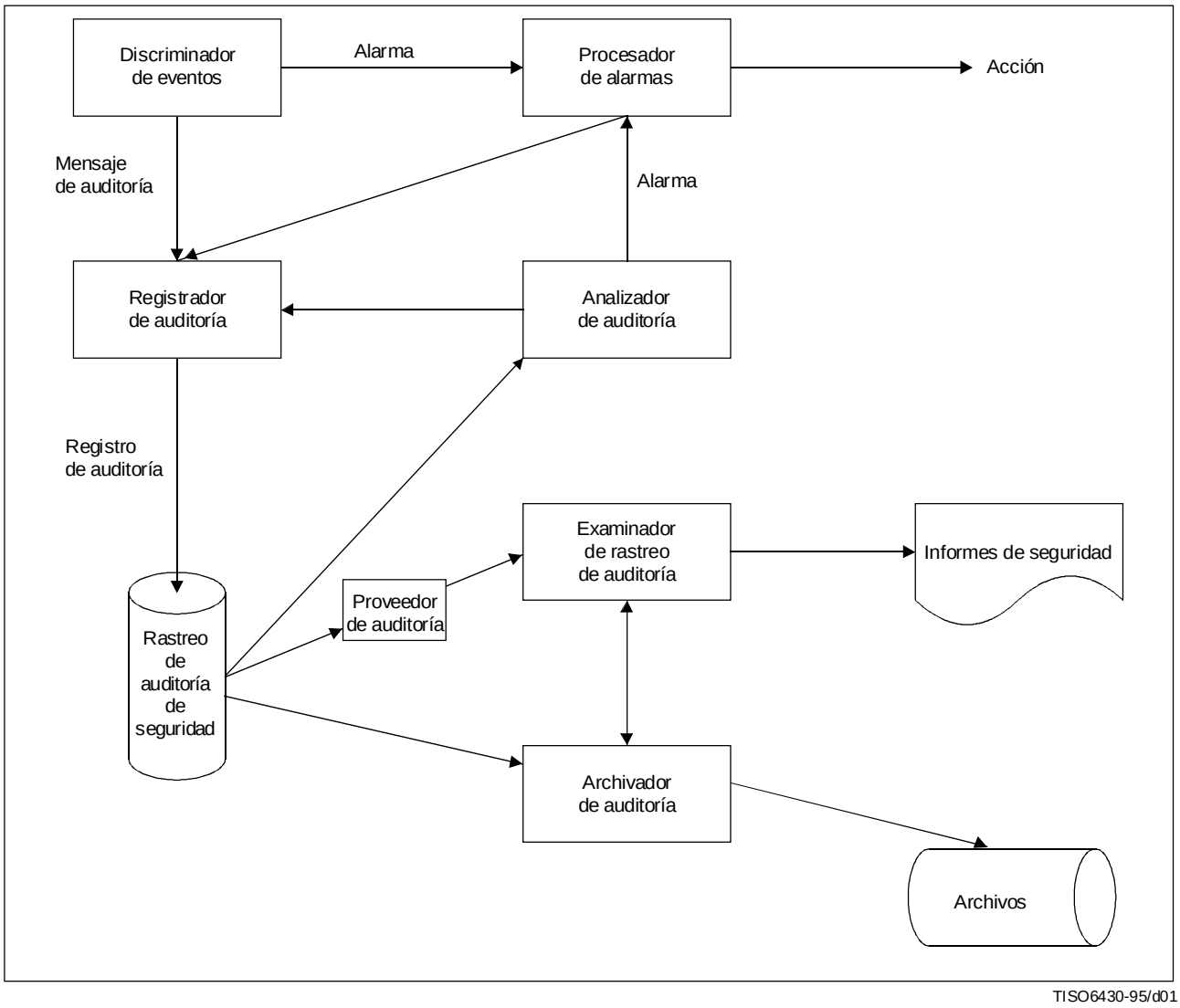

Figura 1 – Modelo de auditoría y alarmas de securidad

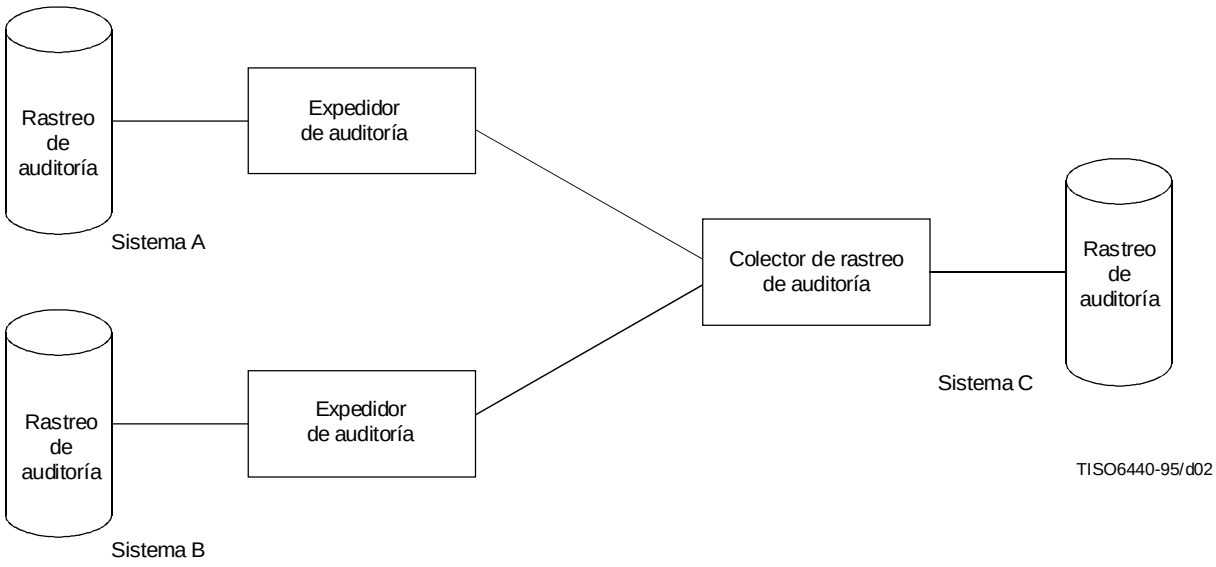

Figura 2 – Modelo de rastreo de auditoría distribuido

6.2 Fases de los procedimientos de auditoría y alarmas de seguridad

El servicio de auditoría de seguridad proporciona una autoridad de auditoría con capacidad para especificar y seleccionar los eventos que necesitan ser detectados y registrados en un rastreo de auditoría de seguridad, y los eventos que necesitan activar una alarma de seguridad y mensajes de auditoría de seguridad.

En los procedimientos de auditoría, pueden producirse las fases siguientes:

- fase de detección, durante la cual se detecta un evento relacionado con la seguridad;
- fase de discriminación, durante la cual se determina inicialmente si es necesario registrar el evento en el rastreo de auditoría de seguridad o dar una alarma;
- fase de procesamiento de alarmas, durante la cual se puede emitir una alarma de seguridad o un mensaje de auditoría de alarma;
- fase de análisis, durante la cual se evalúa un evento relacionado con la seguridad junto con y en el contexto de eventos detectados previamente, tal como fueron registrados cronológicamente en el rastreo de auditoría y se determina un plan de acción;
- fase de recopilación, durante la cual los registros de rastreo de auditoría de seguridad distribuidos se recopilan en un solo rastreo de auditoría de seguridad;
- fase de generación de informes, durante la cual se elaboran los informes de auditoría a partir de registros de rastreo de auditoría de seguridad; y
- fase de archivo, durante la cual se transfieren los registros del rastreo de auditoría de seguridad al archivo de rastreo de auditoría de seguridad.

Las fases aquí descritas no se producen necesariamente en momentos diferentes, es decir, pueden superponerse.

6.2.1 Fase de detección

La fase de detección supone determinar que se ha producido un evento que puede estar relacionado con la seguridad. La determinación efectiva de cualquier acción, si la hubiera, ejecutada en respuesta a este evento, es tarea del *discriminador de eventos* (véase 6.2.2), pero, en algunos casos, determinados por la política de seguridad, puede dar una alarma inmediata.

6.2.2 Fase de discriminación

Una vez que se ha detectado un evento relacionado con la seguridad, el discriminador de eventos determinará la acción inicial adecuada, que será una de las siguientes:

a) no se ejecutará ninguna acción;

b) se genera un mensaje de auditoría de seguridad; o

c) se genera una alarma de seguridad y un mensaje de auditoría de seguridad.

La decisión relativa a la acción que se ha de ejecutar para cada evento, depende de la política de seguridad en vigor.

6.2.3 Fase de procesamiento de alarmas

El procesador de alarmas analiza la alarma para determinar la acción correcta, que será una de las siguientes:

a) no se ejecutará ninguna acción;

b) se inicia una acción de restablecimiento; o

c) se inicia una acción de restablecimiento y se genera un mensaje de auditoría de seguridad.

La decisión relativa a la acción que se ha de ejecutar para cada evento, depende de la política de seguridad en vigor.

NOTA – b) y c) podrían entrañar que se señala el evento a una persona, que puede ser un agente de seguridad o un administrador de auditoría.

6.2.4 Fase de análisis

Durante la fase de análisis, se procesa un evento relacionado con la seguridad, para determinar la acción apropiada. Este procesamiento también puede hacer uso de la información relativa a eventos relacionados con la seguridad acaecidos anteriormente, registrados en el rastreo de auditoría de seguridad. La acción será una de las siguientes:

a) no se ejecuta ninguna acción;

b) se genera una alarma de seguridad;

c) se genera un registro de auditoría de seguridad; o

d) se generan una alarma de seguridad y un registro de auditoría de seguridad.

La decisión relativa a la acción que se ejecutará para cada evento, dependerá de la política de seguridad en vigor.

Como parte integrante del proceso de análisis, puede hacerse referencia a eventos previos, examinando los registros del rastreo de auditoría de seguridad y del archivo del rastreo de auditoría de seguridad.

6.2.5 Fase de recopilación

Los registros de auditoría de seguridad individuales provenientes de un rastreo de auditoría distribuido deben recopilarse periódicamente en un solo rastreo de auditoría. Este proceso, que incluye la utilización de un *colector de rastreo de auditoría* (en el punto de recogida) y la utilización de una función de *expedidor de auditoría* (en los sistemas distantes), se denomina recopilación. (Como se señaló en 6.1.3, este proceso podrá ser jerárquico.)

6.2.6 Fase de generación de informes

El rastreo de auditoría de seguridad puede ser procesado cuando así lo requiera u ordene la política de seguridad. Este procesamiento comprenderá un elemento de análisis y también puede incluir la manipulación de los registros de auditoría de seguridad en un formato adecuado. El resultado del análisis de un rastreo de auditoría de seguridad es un informe de seguridad que puede indicar que se ha intentado quebrantar la seguridad de un sistema, en cuyo caso, puede ser necesario emprender acciones para restablecer la seguridad. El análisis del rastreo de auditoría de seguridad se puede utilizar para evaluar el alcance de un ataque y para determinar los procedimientos adecuados de control de daños.

Con miras a restablecer la seguridad, se puede utilizar un informe de seguridad para determinar el alcance de los daños producidos por un problema de seguridad. Concretamente, se puede utilizar para identificar los recursos empleados por un usuario autorizado que ha estado usando sus derechos de forma anormal. También se puede usar para evaluar cualquier daño, de modo que pueda intentarse la acción de restablecimiento necesaria.

6.2.7 Fase de archivo

Puede ser necesario conservar los rastreos de auditoría de seguridad durante largos periodos de tiempo. En la fase de archivo, parte del rastreo de auditoría de seguridad se transfiere a un medio de almacenamiento a largo plazo. El almacenamiento utilizado para archivar debe mantener la integridad del registro o los registros originales. El archivo del rastreo de auditoría de seguridad puede ser local o distante con respecto a la fuente original del rastreo de auditoría. Pueden proporcionarse mecanismos para el archivo distante.

6.3 Correlación de la información de auditoría

Los registros de auditoría pertenecientes a uno o más rastreos de auditoría de seguridad pueden estar interrelacionados. Por ejemplo, se puede transmitir una petición de conexión a través de varios sistemas intermedios y, como resultado, generar varios registros de auditoría de seguridad en diferentes rastreos de auditoría de seguridad. Puede ser importante que estos registros de auditoría de seguridad estén fechados o identificados con exactitud puesto que están interrelacionados. Otro ejemplo es el registro de dos eventos diferentes en dos rastreos de auditoría de seguridad diferentes, cuando es importante poder determinar el evento que se produjo primero. En el Anexo D aparece un examen de los problemas de la correlación de tiempos de eventos de diferentes generadores de eventos.

7 Política y otros aspectos de la auditoría y alarmas de seguridad

7.1 Política

Una política de auditoría de seguridad define eventos relacionados con la seguridad y determina reglas que habrán de aplicarse para la recopilación, el registro (en un rastreo de auditoría) y el análisis de los diversos eventos relacionados con la seguridad. Cabría hacer varias consideraciones con respecto a las políticas de auditoría y cómo plasmarlas en reglas. Se podría aplicar una o más de estas consideraciones a una política de seguridad determinada.

Una política de auditoría de seguridad debe definir los requisitos necesarios para realizar varios niveles y tipos de auditoría de seguridad y debe definir asimismo los criterios para la generación de alarmas de seguridad. La comprobación de la adecuación de los controles de sistemas, la confirmación relativa al cumplimiento de la política de seguridad y la determinación de los cambios indicados en la política, controles y procedimientos, requerirán el análisis de los registros de rastreo de auditoría de seguridad y muchos otros aspectos sobre diseño, configuración y funcionamiento de los sistemas.

NOTA – La manera de definir eventos relacionados con la seguridad en una política de seguridad, cae fuera del ámbito de esta Recomendación | Norma Internacional.

7.2 Aspectos jurídicos

En muchos países existen leyes destinadas a proteger la privacidad de los ciudadanos. En algunos casos, esto significará que un registro de rastreo de auditoría que contenga información de naturaleza personal, se verá afectado por las leyes nacionales, relacionadas con la privacidad y el acceso a la información. Tales registros necesitarán ser protegidos contra la divulgación no autorizada.

En aquellos casos en que los registros de auditoría de seguridad se utilizan como evidencia legalmente admisible, pueden existir requisitos específicos con respecto a la utilización, almacenamiento y protección de los registros de auditoría de seguridad.

7.3 Requisitos de protección

Se pueden considerar dos aspectos de protección:

- la protección del rastreo de auditoría de seguridad y de la información de auditoría; así como
- la protección del servicio de auditoría de seguridad.

7.3.1 Protección de la información de auditoría

La información recopilada en un rastreo de auditoría de seguridad puede venir directamente de los mensajes de auditoría o de otros rastreos de auditoría de seguridad. Por lo tanto, un rastreo de auditoría de seguridad podría ser el conjunto de registros de rastreo de auditoría de seguridad generados por una o más fuentes. En el caso más simple, un rastreo de auditoría de seguridad contiene todos los registros de auditoría de seguridad generados por un solo sistema.

El rastreo de auditoría de seguridad debe estar protegido contra la divulgación y/o modificación no autorizadas. Se pueden utilizar mecanismos de control de acceso, confidencialidad, integridad y autenticación para protegerlo. Una técnica de protección específica que se utiliza consiste en almacenar registros de auditoría en un medio en que sólo pueda escribirse una vez, de modo que no pueda utilizarse la sobreescritura para borrar el registro de un evento.

Los mensajes de auditoría de seguridad, las alarmas de seguridad y los informes de seguridad también deben protegerse contra la divulgación y/o modificación no autorizadas. Por añadidura, es importante que el emisor y el receptor de la información tengan la seguridad de que tanto la fuente como el destino de los datos son los declarados, y que la información no ha sido corrompida en modo alguno.

También puede ser necesaria la confidencialidad al menos de parte de la información, por diversas razones:

- los aspectos jurídicos con respecto a la privacidad personal;
- la necesidad de ocultar cuáles eventos de auditoría están o no registrados;
- la necesidad de encubrir la identidad de los destinatarios (o no destinatarios) de las acciones resultantes de alarmas.

7.3.2 Protección del servicio de auditoría y alarmas

El servicio de auditoría y alarmas de seguridad depende de que exista un alto nivel de disponibilidad. La denegación de servicio constituye una amenaza para el servicio de auditoría y alarmas. La información destinada al administrador de alarmas de seguridad o al auditor de seguridad, podría retrasarse hasta el extremo de que la información dejara de tener valor. Es de importancia primordial que la información llegue a los destinatarios previstos oportunamente.

En la cláusula 10, se examinan más detalladamente estos aspectos de la protección.

8 Información y facilidades de auditoría y alarmas de seguridad

Se puede considerar que el procesamiento de la información de auditoría de seguridad consta de dos aspectos:

- el procesamiento de mensajes generados en respuesta a un evento no esperado (es decir, la información de auditoría de seguridad no solicitada); y
- el procesamiento de peticiones para una información de auditoría de seguridad determinada (es decir, la información solicitada).

Los servicios de gestión tienen que controlar diversos aspectos del proceso de auditoría y alarmas de seguridad, incluidos los mecanismos de rastreo de auditoría de seguridad, los criterios que definen las acciones específicas ejecutadas debido a la detección de un evento relacionado con seguridad y los procesos relacionados con el tratamiento de la información y alarmas de auditoría.

8.1 Información de auditoría y alarmas

La información de auditoría y alarmas incluye alarmas de seguridad, mensajes de auditoría de seguridad, registros de auditoría de seguridad e informes de seguridad.

8.1.1 Mensajes de auditoría de seguridad

Un *mensaje de auditoría de seguridad* es un mensaje generado como resultado de un evento auditable relacionado con la seguridad.

Un mensaje de auditoría de seguridad puede ser generado, por ejemplo, a partir del análisis inicial de un evento relacionado con la seguridad por el *discriminador de eventos* o como resultado de una evaluación subsiguiente por el *procesador de alarmas* o el *analizador de alarmas.*

8.1.2 Registros de auditoría de seguridad

El término *registro de auditoría de seguridad* se utiliza para describir un único registro en un rastreo de auditoría de seguridad. En muchos casos, esto corresponderá a un solo evento relacionado con la seguridad, pero también es concebible, que para algunas aplicaciones, un registro de auditoría de seguridad puede ser generado como resultado de más de un evento relacionado con la seguridad.

Un registro de auditoría de seguridad típico incluye información acerca del origen y la causa del mensaje, y podría contener información relativa a las entidades que participan en la detección y procesamiento del mensaje.

8.1.3 Alarmas de seguridad

Una *alarma de seguridad* es un mensaje generado tras la detección de un evento relacionado con la seguridad, considerado como una violación potencial de la seguridad, y que constituye una condición de alarma. Esto puede ser un evento o puede ser el resultado de haber alcanzado un umbral. En ambos casos, la política de seguridad especifica la definición de lo que constituye una condición de alarma.

Las alarmas de seguridad pueden ser iniciadas por el *discriminador de eventos* (como resultado de la evaluación inicial de un evento de seguridad) o por el *analizador de auditoría* si, en cualquier momento, determina que existe una condición de alarma.

8.1.4 Informes de seguridad

Los *informes de seguridad* son información producida como resultado del análisis del rastreo de auditoría de seguridad. El *examinador de rastreo de auditoría* se utiliza para elaborar los informes a partir de uno o más rastreos de auditoría de seguridad.

8.1.5 Ejemplo de la composición de la información de auditoría y alarmas

Típicamente, la información de auditoría y alarmas contiene lo siguiente:

- el tipo de información/mensaje (es decir, alarma de seguridad, mensaje de auditoría de seguridad, o informe de seguridad);
- el identificador distintivo de los elementos (por ejemplo, el iniciador/objetivo del evento relacionado con la seguridad o el sujeto/objeto de la acción);
- la causa del mensaje;
- el identificador distintivo del *discriminador de eventos*, *proveedor de auditoría* y/o *registrador de auditoría*.

8.2 Facilidades de auditoría y alarmas de seguridad

Para aplicar una auditoría efectiva y permitir un análisis eficaz de los eventos, es necesario un método que determine los eventos que están relacionados con la seguridad y cómo procesarlos. El análisis de mensajes se efectúa mediante un mecanismo de filtrado que determina la acción adecuada que se ha de ejecutar al recibir un mensaje de auditoría. El filtro actúa de acuerdo con criterios (determinados por la autoridad de auditoría de seguridad) que establecen la acción que ha de ejecutarse para cada tipo de mensaje. Los criterios aplicables incluyen:

- la hora del día;
- un contador de umbral;
- el tipo de evento; y
- la entidad que origina el evento.

A efectos de gestión, el filtro puede definirse como un objeto gestionado con un comportamiento y unos parámetros especificados.

Las facilidades relacionadas con la gestión de auditoría proporcionan un medio para establecer los criterios de selección de modo que un usuario pueda procesar la información necesaria para la prestación del servicio de auditoría y alarmas de seguridad. En general, estas facilidades son:

a) crear, modificar y suprimir los criterios para procesar los eventos relacionados con la seguridad;

b) permitir e impedir la generación de determinados mensajes de auditoría de seguridad;

c) permitir e impedir la generación de rastreos de auditoría de seguridad;

d) permitir e impedir la generación y el procesamiento de alarmas.

Las facilidades relacionadas con el funcionamiento y las alarmas de auditoría son las siguientes:

a) generar información de auditoría y de alarmas (por ejemplo, generar una alarma, un mensaje de auditoría, un informe de seguridad);

b) registrar información de auditoría y de alarmas;

c) recopilar/reunir información de auditoría y de alarmas;

d) analizar información de auditoría y de alarmas; y

e) archivar información de auditoría y de alarmas.

8.2.1 Determinación y análisis de los eventos de seguridad – Criterios para las funciones de auditoría y alarmas

Tanto una alarma de seguridad como un mensaje de auditoría de seguridad determinan el tipo y la causa del evento, la hora en que se detectó el mismo, la identidad del detector del evento y las identidades de las entidades asociadas con el evento (es decir, el sujeto y objeto de la acción que origina el evento).

Se han establecido los siguientes criterios para especificar la acción que se ejecutará cuando se procesan diferentes tipos de información:

Criterios 1 – Discriminación de eventos

Estos criterios determinarán la acción que se ha de ejecutar cuando se detecta un evento relacionado con la seguridad.

Posibles parámetros de entrada:

- tipo de evento relacionado con la seguridad;
- hora del día;
- entidad que origina el evento.

Posibles parámetros de salida:

- la acción que se ha de ejecutar;
- el mensaje de alarma de seguridad que se ha de generar;
- el mensaje de auditoría de seguridad que se ha de generar.

Criterios 2 – Examen de rastreo de auditoría

Estos criterios ofrecen una base para seleccionar la información contenida en uno o más rastreos de auditoría de seguridad a efectos de compilación de informes de seguridad.

Posibles parámetros de entrada:

- tipo de registro de auditoría;
- tipo de evento relacionado con la seguridad;
- hora del evento examinado;
- entidad sobre la cual se solicita información.

Posibles parámetros de salida:

- lista de los registros seleccionados.

Criterios 3 – Criterios de análisis del rastreo de auditoría

Los rastreos de auditoría serán analizados evaluando la incidencia y frecuencia de los eventos antes de determinar la acción que se ha de ejecutar.

Posibles parámetros de entrada:

- tipo de evento;
- número de incidencias;
- periodo de tiempo.

Posibles parámetros de salida:

- acción que se ha de ejecutar.

NOTA – No se necesitan criterios para el registro de auditoría de seguridad ni para el archivo de auditoría de seguridad.

9 Mecanismos de auditoría y alarmas de seguridad

El servicio de auditoría difiere de los demás servicios de seguridad descritos en esta serie de Recomendaciones | Normas Internacionales en que no hay un solo mecanismo de seguridad específico que pueda utilizarse para proporcionar el servicio. Los mecanismos de auditoría pueden describirse como procedimientos basados en varios métodos de gestión y funcionamiento. Por este motivo, no se incluye un examen detallado sobre los mecanismos de auditoría. Sin embargo, a título de ejemplo del tipo de métodos utilizados para auditoría, los mecanismos para el análisis de eventos pertinentes a la seguridad pueden incluir:

- la comparación de la actividad de una entidad con un perfil conocido, por ejemplo, un acceso poco usual basado en el tiempo o la geografía, un uso poco habitual de los recursos, etc.;
- la detección de la acumulación de uno o varios tipos de eventos en un periodo de tiempo; y
- la observación de que no se producen uno o varios tipos de eventos durante el mismo periodo de tiempo.

Esta lista de ejemplos no es exhaustiva.

10 Interacción con otros servicios y mecanismos de seguridad

10.1 Autenticación de entidad

La transferencia de un rastreo de auditoría de seguridad entre un *expedidor de auditoría* y un *colector de auditoría* requiere la autenticación mutua, para que el *expedidor de auditoría* envíe el rastreo de auditoría de seguridad para el *colector de auditoría* futuro, y el *colector de auditoría* reciba el rastreo de auditoría de seguridad del expedidor previsto.

10.2 Autenticación del origen de los datos

La autenticación del origen de los datos es utilizada para que se pueda conocer el origen de los mensajes de auditoría de seguridad y de los mensajes de alarma de seguridad. También la utiliza el *analizador de auditoría* para garantizar que se rechazan los mensajes procedentes de generadores de eventos desconocidos o analizadores de auditoría desconocidos.

10.3 Control de acceso

Se deben utilizar servicios de control de acceso en el almacenamiento y la transferencia de los registros de rastreo de auditoría de seguridad. El control de acceso también podría utilizarse para impedir un acceso no autorizado a un rastreo de auditoría de seguridad.

10.4 Confidencialidad

Los servicios de confidencialidad pueden ser utilizados durante la transferencia de los rastreos de auditoría de seguridad, los registros de auditoría de seguridad seleccionados, los mensajes de auditoría de seguridad y los mensajes de alarma de seguridad. El servicio de confidencialidad también puede ser utilizado para proteger los registros de auditoría almacenados.

10.5 Integridad

Es de importancia primordial detectar cualquier modificación no autorizada del rastreo de auditoría de seguridad, de un conjunto de registros de auditoría de seguridad seleccionados, de un mensaje de auditoría de seguridad o de un mensaje de alarma de seguridad, para lo cual se puede utilizar un servicio de integridad.

10.6 No repudio

Por lo general no se utilizará un servicio de no repudio, ya que la transferencia de los rastreos de auditoría suele realizarse dentro del mismo dominio de seguridad.

Anexo A

Principios generales de auditoría y alarmas de seguridad para OSI

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

Se recomienda auditar siempre los siguientes tipos de eventos relacionados con la seguridad:

- las operaciones relacionadas con la gestión de información de seguridad;
- las operaciones que cambian el conjunto de eventos que han de auditarse; y
- las operaciones que cambian la identificación de los objetos auditados.

Este anexo especifica los eventos OSI que potencialmente producirán un evento relacionado con la seguridad. Puede ser necesario auditar condiciones tanto normales como anormales, por ejemplo, cada petición de conexión puede ser objeto de un registro de rastreo de auditoría de seguridad, si la petición fue anormal o no y sin tener en cuenta si fue aceptada o no.

Los eventos siguientes, entre otros, pueden estar sujetos a auditoría. Esta lista no es exhaustiva y se proporciona únicamente como orientación.

Eventos relacionados con la seguridad asociados a una conexión específica:

- peticiones de conexión;
- conexión confirmada;
- peticiones de desconexión;
- desconexión confirmada;
- estadísticas pertenecientes a la conexión.

Eventos relacionados con la seguridad asociados a la utilización de los servicios de seguridad:

- peticiones de servicios de seguridad;
- utilización de mecanismos de seguridad;
- alarmas de seguridad.

Eventos relacionados con la seguridad asociados a la gestión:

- operaciones de gestión;
- notificaciones de gestión.

La lista de eventos auditables debe incluir, como mínimo:

- denegar acceso;
- autenticar;
- cambiar atributo;
- crear objeto;
- suprimir objeto;
- modificar objeto;
- utilizar privilegio.

Desde el punto de vista de los servicios individuales de seguridad, son importantes los siguientes eventos relacionados con la seguridad:

- autenticación: verificar éxito;
- autenticación: verificar fallo;
- control de acceso: decidir éxito de acceso;
- control de acceso: decidir fallo de acceso;
- no repudio: origen de mensaje no repudiable;
- no repudio: recepción de mensaje no repudiable;

– no repudio: repudio de evento infructuoso;
– no repudio: repudio de evento fructuoso;
– integridad: utilización de blindaje;
– integridad: utilización de desblindaje;
– integridad: validar éxito;
– integridad: validar fallo;
– confidencialidad: utilización de ocultamiento;
– confidencialidad: utilización de revelación;
– auditoría: seleccionar evento para auditoría;
– auditoría: descartar evento para auditoría;
– auditoría: cambiar criterios de selección del evento de auditoría.

NOTA – Cuando se utiliza el control de acceso como base de los mecanismos de integridad o de confidencialidad, los registros de auditoría asociados con «decidir fallo de acceso» pueden convertirse en una indicación explícita de intento de violación de la confidencialidad o integridad.

Todos los registros de rastreo de auditoría pertenecientes a un caso particular de comunicación se deben identificar sin ambigüedad, para garantizar que se puedan rastrear los registros.

Los servicios de la Rec. X.734 del CCITT | ISO/CEI 10164-5 pueden utilizarse para gestionar el servicio de envío de eventos y para configurar los discriminadores de envío de eventos que especifican los criterios de selección para los eventos relacionados con la seguridad pertinentes a una auditoría de seguridad.

El servicio de notificación del rastreo de auditoría de seguridad de la Rec. X.740 del CCITT | ISO/CEI 10164-8 puede ser utilizado por las entidades para generar mensajes de auditoría de seguridad.

Los servicios de la Rec. X.735 del CCITT | ISO/CEI 10164-6 pueden utilizarse para especificar la selección de los mensajes de auditoría de seguridad almacenados en los rastreos de auditoría de seguridad.

El servicio de notificación de alarmas de seguridad de la Rec. X.736 del CCITT | ISO/CEI 10164-7 puede ser utilizado por una aplicación de rastreo de la auditoría de seguridad para generar alarmas de seguridad.

Anexo B

Realización del modelo de auditoría y alarmas de seguridad

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

Las funciones básicas del modelo de auditoría y alarmas de seguridad se muestran en la Figura 1. Todo el procedimiento puede ser distribuido entre muchos sistemas abiertos diferentes, siendo cada sistema responsable de uno o más aspectos del procedimiento. La Figura B.1 muestra un ejemplo.

Un ejemplo de un evento de seguridad podría ser un intento de conexión a un sistema, utilizando una contraseña no válida en una cuenta. El análisis del rastreo de auditoría podría revelar que éste formaba parte de una serie de intentos para conectarse a la cuenta con una contraseña falsa y que podría activarse una alarma cuando se alcanzara el umbral.

S1 es capaz de detectar eventos relacionados con la seguridad y analizarlos con arreglo a criterios definidos (criterios 1), pero no posee capacidad de rastreo de auditoría de seguridad, de modo que sus alarmas de seguridad son enviadas a S2 y sus mensajes de auditoría de seguridad son enviados a S3 para inclusión en el rastreo de auditoría de seguridad.

S3 es responsable de actualizar el rastreo de auditoría de seguridad. S3 también suministra a S6 acceso al rastreo de auditoría de seguridad y a los archivos de rastreo de auditoría de seguridad, para que puedan seleccionarse los registros de rastreo de auditoría de seguridad de acuerdo con criterios definidos (criterios 2) y recopilarlos en un informe de seguridad.

S4 es responsable del archivo y recuperación de los registros de rastreo de auditoría.

S5 contiene una aplicación que analiza los registros de rastreo de auditoría (y los registros archivados) con arreglo a criterios definidos (criterios 3) y envía alarmas a S2 cuando se rebasan los límites de umbral o cuando se detectan otras condiciones de alarma.

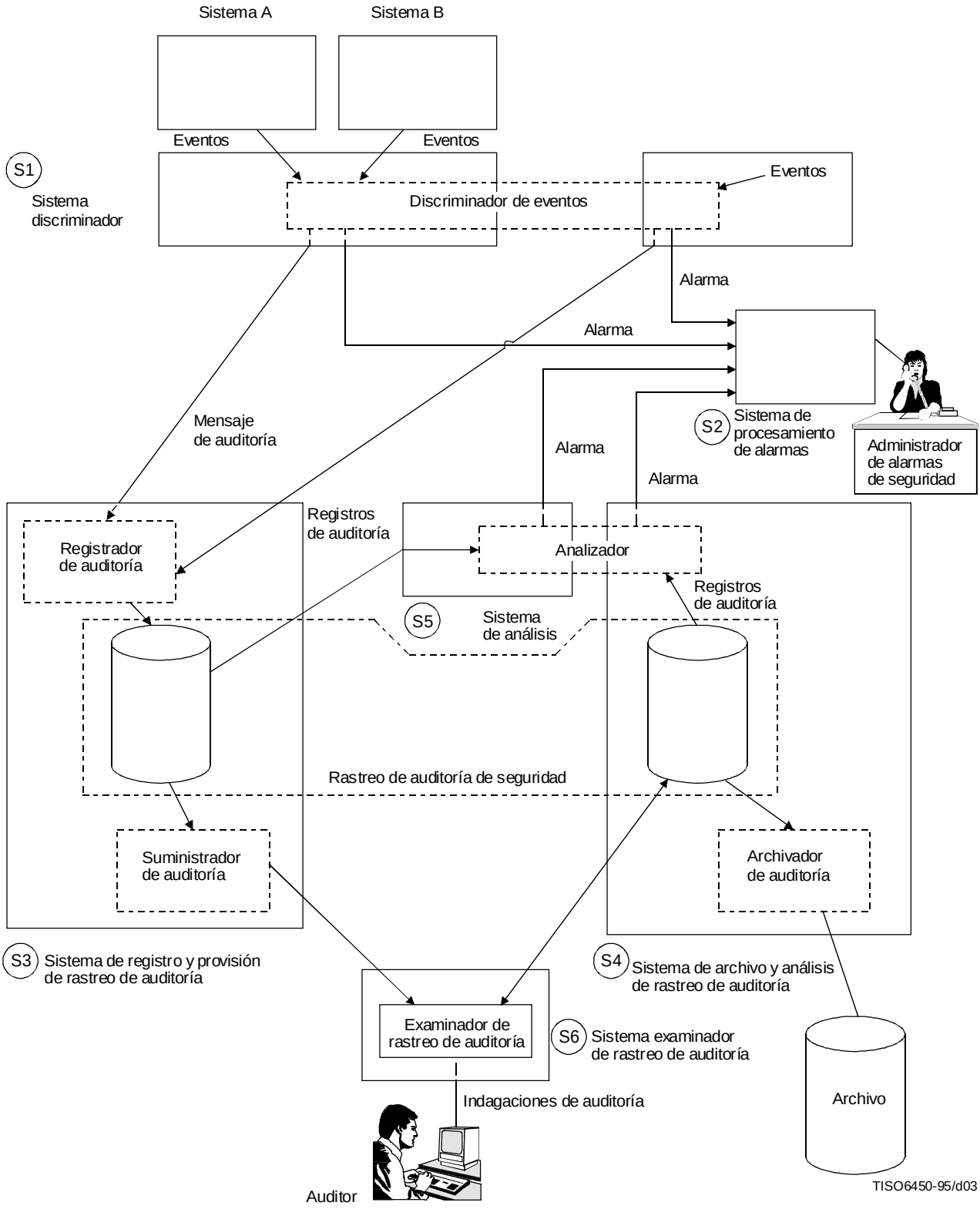

Figura B.1 – Realización de un servicio de auditoría y alarmas de seguridad

Anexo C

Esquema de las facilidades de auditoría y alarmas de seguridad

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

<table>
<tr><td colspan="2" rowspan="4">Esquema de las facilidades de seguridad</td><td rowspan="3">Elemento</td><td colspan="3">Entidades: autoridad de auditoría; administrador de alarmas; auditor de seguridad.</td></tr>
<tr><td colspan="3">Funciones: discriminador de eventos; registrador de auditoría; procesador de alarmas; analizador de auditoría; examinador de rastreo de auditoría; proveedor de auditoría; expedidor de auditoría; colector de rastreo de auditoría.</td></tr>
<tr><td colspan="3">Objetos de información: mensajes de auditoría de seguridad; registros de auditoría de seguridad; informes de seguridad.</td></tr>
<tr><td colspan="4">Objetivo de servicio: garantizar que la información relacionada con la seguridad de los sistemas abiertos de información se registra y cuando proceda, se notifica.</td></tr>
<tr><td rowspan="6">FACILIDADES</td><td>Entidad</td><td colspan="4">Autoridad de auditoría</td></tr>
<tr><td>Función</td><td colspan="4">Determinación y análisis de eventos relacionados con la seguridad</td></tr>
<tr><td>Actividad relacionada con la gestión</td><td colspan="4">Criterio 1: discriminación de eventos
Criterio 2: examen de rastreo de auditoría
Criterio 3: análisis de rastreo de auditoría</td></tr>
<tr><td>Entidad</td><td>Administrador de alarmas</td><td>Auditor de seguridad</td><td>Iniciador/objetivo sujeto/objeto</td></tr>
<tr><td>Función</td><td>Discriminador de eventos
Procesador de alarmas
Analizador de auditoría</td><td>Discriminador de eventos
Analizador de auditoría
Registrador de auditoría
Examinador de rastreo de auditoría
Proveedor de auditoría
Archivador de auditoría</td><td></td></tr>
<tr><td>Facilidades relacionadas con funcionamiento</td><td>Generar INFO.
Recopilar INFO.
(INFO. significa alarma)</td><td>Generar INFO.
Recopilar INFO.
Analizar INFO.
(INFO. significa mensaje de auditoría)</td><td></td></tr>
<tr><td rowspan="4">INFORMACIÓN</td><td rowspan="2">Elemento de datos gestionado por la autoridad de auditoría</td><td>Criterios 1
– tipo de evento
– hora
– entidad</td><td>Criterios 2
– tipo de registro
– tipo de evento</td><td>Criterios 3
– tipo de evento
– número de incidencias
– periodo de tiempo</td></tr>
<tr><td>– Acción que ha de ejecutarse
– Información de seguridad que ha de generarse</td><td>– Registrar listas</td><td>– Acción que ha de ejecutarse</td></tr>
<tr><td>Tipo de información utilizada durante el funcionamiento</td><td colspan="3">– Tipo de mensaje/información
– Identificador distintivo de elementos
– Causa del mensaje
– Identificador distintivo del discriminador de eventos, proveedor de auditoría y/o registrador de auditoría</td></tr>
<tr><td>Información de control</td><td colspan="3">– Hora, incidencias</td></tr>
</table>

Anexo D

Registro de fecha y hora de eventos de auditoría

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

En la práctica, no es posible la sincronización perfecta entre los diferentes generadores de eventos o registradores de eventos. En tal caso, se necesita un medio para relacionar el tiempo dentro del rastreo de auditoría de seguridad. Se crea un registro de auditoría de seguridad a partir de un mensaje de auditoría de seguridad que puede o no contener una indicación de tiempo. Si contiene una indicación de tiempo, se crea un registro de auditoría de seguridad utilizando la indicación de tiempo proporcionada en el mensaje de auditoría de seguridad. En el segundo caso, el registro de seguridad creado en el momento de la recepción del evento de seguridad relacionado con la auditoría contiene una indicación de tiempo que utiliza la referencia temporal del *registrador de auditoría*. En ambos casos se debe crear un registro de auditoría de la relación de tiempo entre el generador de eventos y el *registrador de auditoría.*

En el primer caso, debe efectuarse una evaluación de la diferencia entre la referencia de tiempo del generador de eventos y la referencia de tiempo del *registrador de auditoría*. El registro de auditoría debe incluir la identificación del generador de eventos, la referencia de tiempo del generador de eventos, la referencia de tiempo del *registrador de auditoría*, el retardo entre las referencias de tiempo y un margen de tolerancia sobre el retardo. En el último caso, el registro de auditoría debe indicar la identificación del generador de eventos, la referencia de tiempo del *registrador de auditoría* y la estimación del retardo entre el generador de eventos y el *registrador de auditoría* así como un margen de tolerancia sobre el retardo.

No sería práctico crear tales registros para cada evento. Estos registros se pueden crear según la naturaleza de la vinculación o deriva entre las referencias de tiempo. Si tras un periodo de observación, se advierte que el retardo es despreciable, podrán omitirse tales registros. Puede utilizarse interpolación lineal cuando faltan mediciones del retardo.

El mismo tipo de problema surge entre la referencia de tiempo de un *registrador de auditoría* y la referencia de tiempo de un *expedidor de auditoría* ubicado en otro sistema de extremo. Sin embargo, en este caso, ambos sistemas tendrán una referencia de tiempo. Las mediciones de las diferencias de tiempo pueden efectuarse en cualquier momento entre los dos sistemas correspondientes o en el momento de la transferencia de un rastreo de auditoría de seguridad. El registro incluirá la identificación del generador de eventos, la identificación del *expedidor de auditoría*, la referencia de tiempo del *registrador de auditoría*, la estimación del retardo entre el *registrador de auditoría* y el *expedidor de auditoría* y un margen de tolerancia sobre el retardo.

Para determinar cuál de los dos eventos ocurrió primero, se pueden sumar o restar los retardos entre una serie de referencias de tiempo y sumar todos los márgenes de tolerancia. Si el retardo resultante es menor que el margen de tolerancia, no podrá realizarse la distinción.

Se aplica el mismo argumento cuando hay que crear un registro de auditoría de seguridad. Utilizando la información suministrada en el rastreo de auditoría, es posible clasificar los eventos con arreglo a las diferentes referencias de tiempo. No obstante, la ordenación de un evento sólo puede garantizarse si el margen de tolerancia del retardo es menor que la diferencia de tiempo, más el margen de tolerancia del evento siguiente. Con este fin, debe ser posible calcular un margen de tolerancia acumulativo para cada evento.