



Auditoría en Sistemas Seguros

Junio 2000

**Elaborado por:
Departamento de Control de
Calidad y Auditoría
Informática**

Contenido

Auditoría en Sistemas Seguros

- I. Introducción**
- II. Propósito**
- III. Alcance**
- IV. Objetivos de Control**
- V. Planeación de la Auditoría**
- VI. Cantidad de Datos**
- VII. Seguridad**
- VIII. Personal**
- IX. Aspectos de Seguridad en la Auditoría**
- X. Aspectos de la Revisión Eficaz**
- XI. Identificación / Verificación**
- XII. Diseño de la Base de Datos de Auditoría**
- XIII. Criterios Establecidos**
- XIV. El requisito de la auditoría C2**
- XV. El requisito de la auditoría B1**
- XVI. El requisito de la auditoría B2**
- XVII. El requisito de la auditoría B3**

- XVIII. El requisito de la auditoría A1**
- XIX. Métodos Posibles de la Puesta en Práctica**
- XX. Selección de Pre/Post de Sucesos Auditables**
- XXI. Preselección**
- XXII. Post-Selección**
- XXIII. Comprensión de Datos**
- XXIV. Registros de Auditoría Múltiples**
- XXV. Almacenamiento Físico**
- XXVI. Dispositivo de Sólo – Escritura**
- XXVII. Datos de Auditoría en Equipo Dedicado**
- XXVIII. Otros Aspectos: Reducción de Datos de la Auditoría**
- XXIX. Disponibilidad de los Datos de Auditoría**
- XXX. Pruebas**
- XXXI. Documentación**
- XXXII. Riesgos Inevitables de Seguridad**
- XXXIII. Revisión de Amenazas por Parte del Administrador o de los Usuarios**
- XXXIV. Pérdida de Datos**
- XXXV. Resumen de la Auditoría**
- XXXVI. Bibliografía**
- XXXVII. Glosario**

Introducción

Hoy en día, la cantidad de datos que se maneja en los sistemas de información, no está lejos de exceder nuestra habilidad para reducir y analizar los datos sin el uso de técnicas de análisis automatizadas, un claro ejemplo de estas situaciones se presenta en los registros de auditoría o bitácoras con que se cuentan en los sistemas operativos, mientras más detallado sea el registro de actividades, mucho mayor será la información almacenada, y por lo tanto mayor el tiempo dedicado al análisis de esta información.

Cada sistema dependiendo de la categoría que alcance en el *Libro naranja*, tiene asociado un mecanismo de auditoría, el cual se explica en este documento, también se comentan algunos cuidados que deben tenerse con la información generada y con el personal que desempeña esta tarea.

Propósito

El proceso de la auditoría en un sistema de información seguro es el proceso de la grabación, evaluación, y revisión de cualesquiera o de todas las actividades relevantes de seguridad en el sistema. Proporciona una guía a los usuarios en cómo utilizar eficazmente las capacidades de auditoría implementadas en los sistemas.

Este documento contiene información sobre los mecanismos de auditoría que se implementan en los sistemas seguros, así como de los cuidados en el registro, y algunas características de configuración.

Alcance

En esta guía de consulta, se revisarán las características de los recursos de la auditoría, cómo se aplican en los sistemas informáticos y en los productos que se están construyendo.

Objetivos de Control

Los sistemas que se utilizan para dirigir, procesar, clasificar, la información sensible deben asegurar la responsabilidad individual, siempre que se invoque una política de seguridad obligatoria o discrecional. Además, con el fin de asegurar la responsabilidad debe existir un agente autorizado y competente, que tenga acceso y evalúe la responsabilidad de la información por medios seguros, dentro de una cantidad de tiempo razonable¹.

El objetivo del control de la responsabilidad se relaciona con la revisión y conduce al objetivo siguiente:

Un sistema informático confiable debe proveer al personal autorizado la capacidad de revisar cualquier acción en la que pueda potencialmente causar el acceso, generación, o efectúe el desbloqueo de la información clasificada o sensible. Los datos de la auditoría serán adquiridos selectivamente tomando en cuenta las necesidades de la revisión de una instalación y/o de una aplicación determinadas. Sin embargo, debe haber suficiente seguridad en los datos de la auditoría que permitan rastrear los sucesos, los individuos específicos (o los procesos) que ha efectuado las acciones².

Planeación de la Auditoría

Para la planeación de la auditoría deben tenerse en cuenta varios aspectos:

- a) La cantidad de datos.
- b) La seguridad.
- c) El personal.
- d) Aspectos de seguridad en la auditoría.
- e) Aspectos generales de la revisión.
- f) El tiempo destinado a la auditoría.

Además se requiere de eficiencia debido al volumen de datos que se manejan.

¹ Tomado de: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>

² Tomado de: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>

Cantidad de Datos

Este elemento va a determinar la capacidad del sistema y la complejidad de la misma, en cuanto al volumen de datos almacenados o los elementos que intervienen.

Seguridad

Día a día, las compañías depositan su confianza en redes internas y externas como forma de enviar y recibir información crítica entre clientes, proveedores y personas, y manipular así sus bases de datos. Sin embargo, hay muchos puntos de la red donde pueden interceptarse, copiarse y desviarse los datos o mensajes.

A pesar de que las compañías aplican mecanismos de alta seguridad para mantener a los que las atacan lejos de sus redes, es probable que algunos consigan entrar. Los procesos de cifrado y autenticación garantizan que, aunque haya una violación de seguridad, externa o interna, la información de la empresa esté segura.

Los elementos básicos en la revisión de un sistema de información son:

- La revisión de la seguridad de la información.
- Que la estructura de la base de datos sea la adecuada.
- Que el modelo esté acorde con las necesidades del usuario.
- Que el acceso a la misma sea ágil, además.
- Que tenga cierta flexibilidad.

El proceso de auditoría tiene cinco metas importantes en el aspecto de seguridad.

Primero: El proceso de auditoría debe *permitir la revisión de los modelos de acceso a los objetos individuales, a las bitácoras de acceso de procesos específicos, de los individuos, y del uso de varios mecanismos de protección utilizados por el sistema para su protección.*

Segundo: El proceso de auditoría debe *permitir el descubrimiento de tentativas de los usuarios autorizados de desviar los mecanismos de protección, así como identificar las tentativas realizadas por parte de intrusos para ingresar al sistema.*

Tercero: El proceso de auditoría debe *permitir el descubrimiento de cualquier uso de privilegios o permisos, que pueden ocurrir cuando un*

usuario asume funciones con privilegios mayores a los suyos o realiza algún proceso para el que requiere permisos mayores a los que tiene asignados.

Cuarto: El proceso de auditoría debe actuar como impedimento contra tentativas habituales de intrusos de desviar o alterar los mecanismos de protección del sistema.

Quinto: La meta del proceso de auditoría es proporcionar al usuario, una forma adicional de asegurarse de la efectividad del mecanismo de protección.

Los registros de auditoría se utilizan para detectar y para disuadir la penetración en un sistema informático y para revelar las acciones que identifican su uso erróneo. En la discreción del auditor, los registros de auditoría pueden limitarse a los sucesos específicos o pueden abarcar todas las actividades dentro del sistema.

Debe ser posible que el blanco del proceso de auditoría sea un usuario o un objeto. Es decir, el mecanismo de auditoría debe ser capaz de vigilar cada vez que Juan tuvo acceso al sistema X, así como vigilar cuando el archivo Z fue leído o ejecutado; y además cada vez que Juan tuvo acceso al archivo Z.

Personal

Todas las bases de datos y personal de auditoría señalados como responsables de los procedimientos de auditoría deben estar plenamente identificados. Los deberes de los operadores de la base de datos podrían abarcar todas las funciones incluyendo las del auditor en bases de datos pequeñas; pero para bases de datos de infraestructuras mayores, estas funciones deben realizarse por personal especializado para ello.

Aspectos de Seguridad en la Auditoría

El software que se encarga del registro de auditoría, así como el registro de auditoría en sí mismo, deben protegerse debido a la información que contienen y deben estar bajo controles de acceso restringidos.

Los requisitos de la seguridad del mecanismo de la auditoría son los siguientes:

- El mecanismo de grabación del suceso o evento auditado será parte del archivo de auditoría y será protegido contra cualquier modificación no autorizada.
- El registro de auditoría será protegido por el ARCHIVO DE AUDITORÍA contra el acceso no autorizado (es decir, sólo el personal de auditoría puede tener acceso al registro de auditoría). El registro de auditoría también será protegido contra la modificación no autorizada.
- El mecanismo para habilitar o bloquear la auditoría de sucesos/eventos será parte del ARCHIVO DE AUDITORÍA y seguirá siendo inaccesible para los usuarios no autorizados.

Finalmente, los datos del registro de auditoría deben considerarse como datos sensibles, y el registro de la auditoría en sí mismo será considerado tan sensible como los datos más sensibles contenidos en el sistema.

Aspectos de la Revisión Eficaz

Identificación/Verificación.

El ingreso a un sistema requiere de una forma de identificación por parte del usuario (p.e., identificación de la conexión, identificación por tarjeta magnética) y de una clave de acceso (o de otro mecanismo) para la autenticación. Si esta acción es exitosa o fallida, es un procedimiento auditable. Se recomienda que la información de la autenticación, tales como claves de acceso, no sean enviadas al registro de auditoría, es decir se registra la clave del usuario, no su contraseña.

Identificación -
Verificación

En caso que la identificación incorporada no sea reconocida como válida, el sistema debe omitir esta información del registro de auditoría. La razón de esto es que un usuario pudo haber incorporado una clave de acceso cuando el sistema contaba con una identificación de conexión. Si esta información hubiera sido escrita al registro de auditoría comprometería la clave de acceso y la seguridad del sistema.

Diseño de la Base de Datos de Auditoría

El diseño de la base de datos debe incluir un mecanismo para invocar la función de la auditoría a petición del administrador de seguridad del sistema. Debe incluirse un mecanismo para determinar si el suceso va a ser seleccionado para la inclusión como entrada del registro de auditoría. Si la preselección de sucesos no se pone en ejecución, entonces todos los sucesos auditables deben remitirse al registro de auditoría.

El requisito de los criterios del administrador para poder seleccionar los sucesos basados en la clasificación de la identidad del usuario o de la seguridad del objeto o ambos, debe ser satisfecho. Este requisito puede ser resuelto permitiendo la post-selección de sucesos por medio de políticas de seguridad. Existen herramientas de búsqueda o selección utilizadas para analizar el registro de auditoría las cuales pueden ser proporcionadas por algún proveedor.

Criterios Establecidos

Esta sección discutirá los requisitos de auditoría en los criterios marcados por el *Libro naranja* y presentará un número de recomendaciones adicionales. Hay cuatro niveles de los requisitos de la auditoría.

El primer nivel está en los criterios C2 y los requisitos continúan desarrollándose a través de la clase de los criterios B. En cada uno de estos niveles, la guía de consulta enumerará algunos de los sucesos que deben ser auditables, qué información debe estar en el registro de auditoría, y en qué sucesos de la base pueden seleccionarse para ser revisados.

El Requisito de la Auditoría C2

Sección: 2.2.2.2
Apartado: Auditoría

El TCB podrá crear, mantener, y proteger contra la modificación, el acceso o la destrucción no autorizada y proporcionar una ruta de auditoría de accesos a los objetos que protege. Los datos de la auditoría serán protegidos por el TCB de modo que el acceso de lectura a ellos se limitará sólo a aquellas personas que tienen autorización para este tipo de datos. El TCB deberá registrar los siguientes tipos de acontecimientos: uso de identificadores y mecanismos de autenticación, introducción de objetos dentro del espacio direccionable de los usuarios (p.e., apertura de archivos, arranque de programas), borrar objetos, y acciones tomadas por operadores del sistema y administradores del sistema o encargados del sistema de seguridad y ambos, y otros acontecimientos relevantes de seguridad. Para cada acontecimiento registrado, el expediente de auditoría identificará: fecha y hora del evento, usuario, tipo de acontecimiento, y si la operación fue exitosa o fallida. Para los eventos de identificación/autenticación, deberá ser incluido en el expediente de la auditoría el origen de la petición (p.e., identificación de terminal). Para los eventos que introducen un objeto en el espacio direccionable de un usuario y para los eventos de cancelación del objeto, el expediente de auditoría incluirá el nombre del objeto. El administrador de sistema ADP podrá revisar selectivamente las acciones de cualquier usuario (uno o más) a partir de la identidad individual.

Base de la Auditoría

En el nivel C2, el administrador de sistema ADP podrá realizar la auditoría basándose en la identidad individual y en la identidad del objeto.

El Requisito de la Auditoría B1

Sección: 3.1.2.2
Apartado: Auditoría

El TCB podrá crear, mantener, y proteger contra la modificación, el acceso o la destrucción no autorizada y proporcionar una ruta de auditoría de accesos a los objetos que protege. Los datos de la auditoría serán protegidos por el TCB de modo que el acceso de lectura a ellos se limitará sólo a aquellas personas que tienen autorización para este tipo de datos.

El TCB deberá registrar los siguientes tipos de eventos: uso de identificadores y mecanismos de autenticación, introducción de objetos dentro del espacio direccionable de los usuarios (p.e., apertura de archivos, arranque de programas), borrar objetos, y acciones tomadas por operadores del sistema y administradores del sistema o encargados del sistema de seguridad o ambos, y otros acontecimientos relevantes de seguridad. El TCB también podrá revisar cualquier invalidación de marcas de salida legibles al humano. Para cada evento registrado, el expediente de la auditoría identificará: fecha y hora del evento, del usuario, del tipo de evento, y del éxito o el fracaso de la operación. Para los acontecimientos de identificación/autenticación, deberá ser incluido en el expediente de la auditoría el origen de la petición (p.e., identificación de la terminal). Para los eventos que introducen un objeto en el espacio direccionable de un usuario y para los eventos de cancelación de objetos, el registro de auditoría incluirá el nombre del objeto y del nivel de seguridad del mismo. El administrador de sistema ADP podrá revisar selectivamente las acciones de cualquier usuario (uno o más) a partir de la identidad individual o del nivel de seguridad del objeto o ambos.

Base de la Auditoría

Además de los criterios de selección anteriores, en el nivel B1 los criterios requieren específicamente que el administrador de sistema del ADP pueda realizar la auditoría basada en nivel individual de la identidad y/o de la seguridad del objeto.

El Requisito de la Auditoría B2

Sección: 3.2.2.2
Apartado: Auditoría

El TCB podrá crear, mantener, y proteger contra la modificación, el acceso o la destrucción no autorizada y proporcionar una ruta de auditoría de accesos a los objetos que protege. Los datos de la auditoría serán protegidos por el TCB de modo que el acceso de lectura a ellos se limitará sólo a aquellas personas que tienen autorización para este tipo de datos.

El TCB deberá registrar los siguientes tipos de eventos: uso de identificadores y mecanismos de autenticación, introducción de objetos dentro del espacio direccionable de los usuarios (p.e., apertura de archivos, arranque de programas), borrar objetos, y acciones tomadas por operadores del sistema y administradores del sistema o encargados del sistema de seguridad o ambos, y otros acontecimientos relevantes de seguridad. El TCB también podrá revisar cualquier invalidación de marcas de salida legibles al humano. Para cada evento registrado, el expediente de la auditoría identificará: fecha y hora del evento, del usuario, del tipo de evento, y del éxito o el fracaso de la operación. Para los acontecimientos de identificación/autenticación, deberá ser incluido en el expediente de la auditoría el origen de la petición (p.e., identificación de la terminal). Para los eventos que introducen un objeto en el espacio direccionable de un usuario y para los eventos de cancelación de objetos, el registro de auditoría incluirá el nombre del objeto y del nivel de seguridad del mismo. El administrador de sistema ADP podrá revisar selectivamente las acciones de cualquier usuario (uno o más) a partir de la identidad individual o del nivel de seguridad del objeto o ambos. El TCB deberá ser capaz de revisar los eventos identificados que pueden ser utilizados en la explotación de los canales secretos de almacenamiento.

Base de la
Auditoría

El TCB debe proporcionar la capacidad para revisar el uso de los mecanismos secretos de almacenamiento con el ancho de banda determinado.

El Requisito de la Auditoría B3

Sección: 3.3.2.2
Apartado: Auditoría

El TCB podrá crear, mantener, y proteger contra la modificación, el acceso o la destrucción no autorizada y proporcionar una ruta de auditoría de accesos a los objetos que protege. Los datos de la auditoría serán protegidos por el TCB de modo que el acceso de lectura a ellos se limitará sólo a aquellas personas que tienen autorización para este tipo de datos. El TCB deberá registrar los siguientes tipos de eventos: uso de identificadores y mecanismos de autenticación, introducción de objetos dentro del espacio direccionable de los usuarios (p.e., apertura de archivos, arranque de programas), borrar objetos, y acciones tomadas por operadores del sistema y administradores del sistema o encargados del sistema de seguridad o ambos, y otros acontecimientos relevantes de seguridad. El TCB también podrá revisar cualquier invalidación de marcas de salida legibles al humano.

Para cada evento registrado, el expediente de la auditoría identificará: fecha y hora del evento, del usuario, del tipo de evento, y del éxito o el fracaso de la operación. Para los acontecimientos de identificación/autenticación, deberá ser incluido en el expediente de la auditoría el origen de la petición (p.e., identificación de la terminal). Para los eventos que introducen un objeto en el espacio direccionable de un usuario y para los eventos de cancelación de objetos, el registro de auditoría incluirá el nombre del objeto y del nivel de seguridad del mismo. El administrador de sistema ADP podrá revisar selectivamente las acciones de cualquier usuario (uno o más) a partir de la identidad individual o del nivel de seguridad del objeto o ambos. El TCB deberá ser capaz de revisar los eventos identificados que pueden ser utilizados en la explotación de los canales secretos de almacenamiento. El TCB contendrá un mecanismo que pueda vigilar la ocurrencia o la acumulación de los eventos de seguridad auditables que pueden indicar una violación inminente de la política de seguridad. Este mecanismo podrá notificar inmediatamente al administrador de seguridad cuando se excedan los umbrales, y si la ocurrencia o la acumulación de estos eventos relevantes de seguridad continúa, el sistema ejecutará las acciones mínimas con el fin de interrumpir o para terminar el acontecimiento o ambas.

Base de la Auditoría

Además de los criterios de selección anteriores, en el nivel B3 los criterios requieren específicamente que " el ARCHIVO DE AUDITORÍA contenga un mecanismo que pueda vigilar la ocurrencia o la acumulación de los sucesos auditables de la seguridad que pueden indicar una violación inminente de la política de la seguridad. Este mecanismo podrá notificar inmediatamente al administrador de la seguridad del sistema cuando se exceden los umbrales y, si la ocurrencia o la acumulación de estos sucesos continúa, el sistema tomará la acción necesaria para terminar el evento."

El Requisito de la Auditoría A1

No se han agregado requisitos en la clase A1.

Base de la Auditoría:

No se han agregado requisitos en la clase A1.

Métodos posibles de la práctica

Las técnicas para poner los requisitos de la auditoría en ejecución variarán de sistema en sistema dependiendo de las características del software, del firmware, y del equipo físico implicado (hardware) y de cualquier característica opcional que esté disponible. Los avances tecnológicos y las nuevas técnicas que están disponibles deben utilizarse con el fin de obtener la mayor ventaja en el diseño del sistema para proporcionar la seguridad necesaria así como rendimiento óptimo y el desempeño adecuado.

Selección de Pre/Post de Sucesos Auditables

Un requisito indispensable para calificar un sistema dentro de las clases C2 y superiores es tener la capacidad de auditar eventos de seguridad. Sin embargo, estos sucesos pueden o no ser escritos en el registro de auditoría.

Las opciones que pueden ser seleccionadas al ejecutar los sucesos que deben ser revisados incluyen una característica de preselección y una característica de post-selección. Un sistema puede elegir ambas opciones, una opción de la preselección, o ejecutar una opción de post-selección.

Si un responsable del sistema elige no poner una opción general en la selección en ejecución de pre/post, todavía hay un requisito para permitir que el administrador revise selectivamente las acciones de los usuarios especificados para todas las clases de los criterios. Si comienza en la clase B1, el administrador también podrá realizar la auditoría tomando en cuenta el nivel de seguridad de los objetos.

Debe haber opciones para permitir la selección de los individuos o de los grupos de usuarios. Por ejemplo, el administrador puede seleccionar los sucesos relacionados con un individuo específico, o seleccionar los sucesos relacionados con los usuarios incluidos en un grupo determinado. También, el administrador puede establecer que los eventos que se relacionan con el archivo de auditoría estén seleccionados o, en las clases B1 y superiores, que los accesos a los objetos con un nivel dado de sensibilidad, tal como los altamente secretos estén seleccionados. Aunque no sería recomendado, el administrador de seguridad del sistema puede tener la capacidad a seleccionar que no se registre suceso alguno sin importar los requisitos de los criterios. La intención aquí es proporcionar flexibilidad. El propósito de diseñar políticas en la auditoría de un sistema no es imponer los criterios a los usuarios, sino simplemente proporcionar la capacidad al instrumento de fijar requisitos y darles seguimiento.

Una desventaja de la preselección es que es muy difícil predecir qué sucesos pueden ser de interés relevante en la seguridad en una fecha futura. Siempre existe la posibilidad de que los sucesos no preseleccionados un día podrían ser relevantes en la seguridad, y la pérdida potencial de estos sucesos al no revisarse sería imposible de determinar. La ventaja de la preselección podría ser un funcionamiento mejor como resultado de no revisar todos los sucesos en el sistema.

Preselección

Para cada suceso auditable el *Archivo de Auditoría* debe contener un mecanismo para indicar si el suceso va a ser anotado en el registro de auditoría. El administrador o el diseñador de la seguridad del sistema será la única persona autorizada para seleccionar los sucesos a ser registrados. La preselección puede definirse por la identidad del (de los) usuario(s), y en la clase B1 y superior, la preselección también puede hacerse por el nivel de seguridad del objeto. Aunque al administrador de seguridad del sistema tenga la autorización de seleccionar qué sucesos deben ser registrados, el administrador de seguridad del sistema no debe poder excluirse de esta revisión.

Post- Selección

Si la opción de post-selección está seleccionada y se especifican solamente sucesos de un registro de auditoría existente y se ejecuta otra vez, sólo el personal autorizado podrá rehacer esta selección. La inclusión de esta opción requiere que el sistema confíe en sus recursos para validar peticiones de selección/recuperación, de ampliar cualquier dato comprimido, y de obtener los datos solicitados. La ventaja principal de la post-selección es que la información puede comprobarse y de ser útil en el futuro, ya está escrita en un registro de auditoría que puede ser consultada en cualquier momento.

La desventaja que implica la post-selección es que posiblemente degrade el funcionamiento o el rendimiento del sistema debido a la frecuencia con que escriba cada evento al almacenarlo, además es posible obtener un registro de auditoría muy grande.

Compresión de Datos

En el supuesto de que en un sistema se seleccionen todos los sucesos para revisarlos, se generará una gran cantidad de datos por lo que es necesario contar con la capacidad de comprimir para conservar el espacio y reducir al mínimo el tiempo de procesamiento requerido para registrar los eventos a auditar, pero si el registro de auditoría necesita ser comprimido, debe incluirse un mecanismo complementario para descomprimirlo los datos cuando éstos sean requeridos.

La decodificación del registro de auditoría puede hacerse como un preproceso antes de que los expedientes de auditoría sean alcanzados por la base de datos o como un postproceso después de que se haya localizado un expediente relevante. El decodificador necesita presentar los datos en una forma comprensible en la terminal de los administradores y en informes adecuados.

El costo de comprimir el registro de auditoría será el tiempo requerido para los procesos de compresión y de descompresión. La ventaja de contar con los datos comprimidos es el ahorro en el espacio de almacenamiento.

Registros de Auditoría Múltiples

Todos los eventos incluidos en el registro de auditoría pueden escribirse como parte de un mismo registro de auditoría, pero en algunos sistemas puede preferirse contar con varios registros de auditoría distintos, por ejemplo, uno exclusivo para los eventos del *usuario*, otro para los eventos del *sistema*, y otro más para los eventos del *administrador de seguridad del sistema*. Esto daría lugar a varios registros más pequeños para el análisis subsecuente.

En algunos casos, sin embargo, puede ser necesario combinar la información de los registros cuando ocurren sucesos cuestionables para obtener un panorama de la secuencia de cada evento. En casos donde hay registros de auditoría múltiples, es preferible que haya algún dato exacto, o sincronizar los grupos por medio de la fecha y hora de los registros múltiples.

Aunque existe la preferencia por varios registros de auditoría distintos, es importante observar que frecuentemente, es más útil el ARCHIVO DE AUDITORÍA que presenta todos los datos de la auditoría como un registro de auditoría comprensible.

Almacenamiento Físico

Un factor a considerar en la selección del medio de almacenamiento a ser utilizado para el registro de la auditoría sería el uso previsto del sistema.

El volumen de entradas/salidas para un sistema con pocos usuarios que ejecutan pocas aplicaciones sería totalmente diferente de un sistema grande con una multiplicidad de usuarios que realizan una variedad de aplicaciones. En cualquier caso, sin embargo, el sistema debe notificar al operador o al administrador del sistema cuando el medio de almacenamiento en el que reside el registro de auditoría está cercano a su límite. La notificación adecuada al operador es especialmente necesaria si se requiere la auditoría humana.

Si se satura el medio de almacenamiento del registro de auditoría antes de que se substituya o se haga espacio necesario, el sistema operativo detectará esto y tomará una acción apropiada por ejemplo:

1. La notificación al administrador de que el medio esta *lleno* y deberá tomar las acciones necesarias. El sistema puede parar y requerir la reanudación. Aunque es una opción válida, esta acción crea una amenaza severa de los ataques de *negación de servicio*.
2. Guardar los expedientes actuales de la auditoría en un medio temporal con la intención de una migración posterior al medio de almacenamiento que se ocupa normalmente, y así permitir continuar el registro. A este medio de almacenamiento temporal debe incorporarse la misma protección que al medio de almacenamiento normal para prevenir cualquier tentativa de tratar de forzarle.
3. Retrasar la entrada de información de nuevas acciones o retrasar o ambas operaciones actuales para prevenir cualquier acción que requiera el uso del mecanismo de auditoría. Detener la operación hasta que el personal administrativo depure el sistema para obtener más espacio disponible para la escritura del registro.
4. Detener completamente la auditoría como resultado de una decisión del administrador de seguridad del sistema. Cualquier acción que se tome en respuesta a la saturación del medio de almacenamiento será revisada. Existen sin embargo, casos en los cuales la acción tomada no merece ser revisada. Es posible tener las decisiones del sistema del administrador de seguridad incluidas en la lógica del sistema. Tales opciones preprogramadas, incluidas en la lógica del sistema, pueden ser accionadas automáticamente, este tipo de acciones no pueden ser revisadas.

Otra consideración es la velocidad con la que funciona el medio de almacenamiento. Debe poder resolver la condición del *peor caso*, por ejemplo, cuando hay una gran cantidad de usuarios en el sistema y todos los sucesos auditables deben ser registrados.

Esta situación del *peor caso* debe estimarse durante la fase del diseño del sistema y (cuando es posible) el equipamiento físico debe seleccionarse para este propósito.

Sin importar cómo el sistema maneje los desbordamientos del registro de auditoría, debe existir una manera de archivar todos los datos de la misma.

Dispositivo de Sólo-Escritura

Para las clases más bajas de los criterios del *Libro naranja* (p.e., C2, B1) el registro de auditoría puede ser la herramienta principal usada en la detección de los compromisos de seguridad (huecos potenciales). Implícito está que los recursos de la auditoría deben proporcionar la máxima protección posible.

Una técnica que puede emplearse para proteger el registro de auditoría es guardarlo en un mecanismo diseñado para ser un dispositivo de sólo escritura. Otras opciones serían fijar el dispositivo señalado de modo write-once invalidando el mecanismo de lectura. Este método podría evitar que un atacante borre o modifique los datos ya escritos en el registro de auditoría porque el atacante no podrá entrar y leer o buscar los datos que desea modificar.

Si un dispositivo físico está disponible únicamente con los permisos de escritura de datos sobre un medio de almacenamiento, la modificación de los datos ya registrados será muy difícil. Pero es posible introducir mensajes falsos y estos ser escritos en el registro, pero localizar y modificar un mensaje ya registrado será difícil.

El uso de un dispositivo de sólo lectura no previene de modificaciones al registro de auditoría por parte de un atacante, tampoco asegura que los datos residentes en memoria, incluyendo los que están en algún dispositivo de almacenamiento intermo, no sean alterados antes de ser registrados en el archivo de auditoría actual.

Si un dispositivo de sólo lectura se utiliza para almacenar el registro de auditoría, el medio puede cambiarse más adelante a un dispositivo compatible, con permiso de lectura, para permitir que el personal autorizado analice la información sobre el registro de auditoría para detectar cualquier tentativa de penetrar al sistema. Si un atacante modificara la lógica del software de auditoría para evitar escribir los expedientes en el registro de auditoría, la ausencia de datos durante un periodo prolongado indicaría un posible compromiso de la seguridad.

La desventaja de utilizar un dispositivo de sólo lectura es la necesidad de tener un dispositivo de lectura, lo que implica un retardo antes de que el registro de auditoría esté disponible para su análisis por parte del administrador.

Esta desventaja puede ser compensada permitiendo al administrador de seguridad del sistema revise el registro de auditoría en tiempo real, consiguiendo las copias de todos los expedientes de auditoría de manera inmediata al dispositivo con permiso de lectura.

Datos de Auditoría en Equipo Dedicado

Si los recursos están disponibles, otro método de proteger el registro de auditoría sería remitirlo a un procesador dedicado. El registro de auditoría debe entonces estar más fácilmente disponible para el análisis del administrador de la seguridad del sistema.

Otros Aspectos: Reducción de Datos de la Auditoría

Dependiendo de la cantidad de actividades de un sistema y del proceso de selección de la auditoría usados, el tamaño del registro de auditoría puede variar. Es una suposición segura sin embargo, que el registro de auditoría tendrá el tamaño que hará necesario un cierto mecanismo de reducción de los datos de auditoría. La herramienta de reducción de datos será muy probablemente un programa de tratamiento por lotes que se interconectará con el administrador de seguridad del sistema. Este funcionamiento de tratamiento por lotes podría ser una combinación del lenguaje de consulta de la base de datos y de un generador de reportes con la entrada de información que será un archivo de auditoría estandarizado.

Aunque no necesariamente sea una parte del ARCHIVO DE AUDITORÍA, las herramientas de reducción de auditoría deben mantenerse bajo el mismo sistema de control de configuración que el resto del mismo.

Disponibilidad de los Datos de la Auditoría

En la mayoría de los sistemas, se registra la información de la auditoría al momento en que ocurre. Aunque para la mayoría de la información no se necesita que esté disponible inmediatamente para el análisis en tiempo real, el administrador de seguridad del sistema debe tener la capacidad de recuperar la información de auditoría dentro de los siguientes minutos a su registro. El retardo entre la información registrada en la auditoría y la disponibilidad de la misma, para su posterior análisis debe ser mínimo, en el rango de acción de varios minutos.

Para los eventos que requieren atención inmediata, en la clase B3 y superior, una alarma deberá ser enviada al administrador de seguridad del sistema. En los sistemas que guardan el registro de auditoría en un archivo intermedio, el administrador de seguridad del sistema debe tener la capacidad para hacer que el archivo intermedio sea puesto por escrito. Con respecto a las alarmas en tiempo real, el lugar a donde se envían es dependiente de la configuración del sistema.

Retención de los Datos de Auditoría

El tiempo necesario para conservar el registro de auditoría depende del lugar y debe documentarse con los manuales de procedimientos de funcionamiento de la organización. Cuando se intenta llegar a un tiempo óptimo para conservar el registro de auditoría, existen restricciones en el medio de almacenamiento que deben ser considerados en todo momento. El medio de almacenamiento usado debe ser capaz de conservar confiablemente los datos de auditoría durante el tiempo requerido por el sitio.

El registro de auditoría debe revisarse por lo menos una vez por semana, pero es probable que sea un tiempo de espera demasiado largo para revisar el registro de auditoría, esto dependerá de la cantidad de datos esperados por el sistema provenientes de la auditoría, este parámetro debe ajustarse. Las revisiones periódicas promedio recomendadas para el registro de auditoría deben documentarse en el manual del recurso correspondiente.

Pruebas

Los recursos de la auditoría, junto con el resto de los recursos protegidos por el archivo de auditoría, tienen requisitos que aumentan la seguridad conforme se califica en una clase más alta de los criterios del *Libro naranja*. Para las clases más bajas, un registro de auditoría sería un factor importante en la detección de tentativas de penetración. Desafortunadamente, en las clases más bajas, los recursos de la auditoría son más susceptibles a la penetración y a la corrupción. "El archivo de auditoría debe proporcionar un cierto aseguramiento que los datos todavía estén allí cuando el administrador intente utilizarlos".

Existen requisitos de prueba que reconocen la vulnerabilidad del registro de auditoría, y comienzan con la clase C2, incluye una búsqueda para los defectos obvios que corromperían o destruirían el registro de auditoría. Si se corrompe o se destruye el registro de auditoría, la existencia de estos defectos indica que el sistema puede ser penetrado. También debe realizarse una prueba para descubrir cualquier forma de evitar los mecanismos de auditoría. Los *defectos encontrados en la prueba deben neutralizarse*

Un recurso disponible para el diseñador de sistema es revisar todas las aplicaciones del mecanismo en las cuales se encontraron los defectos y registrar tales eventos. Este proceso puede hacerse para eliminar el defecto.

En la clase B2 y superiores, se requiere que todos los defectos detectados sean corregidos o bien se otorgará al sistema un grado más bajo. Si durante las pruebas el registro de auditoría aparece como válido, el análisis de estos datos puede verificar que funcione correctamente o de que no refleje exactamente los sucesos que deben ser incluidos en el registro de auditoría. Aunque los requisitos del sistema pueden aumentar en las clases más altas, el registro de auditoría sigue siendo una herramienta eficaz durante la fase de prueba así como operacionalmente permite la detección de compromisos internos reales o potenciales de la seguridad.

Documentación

Comenzando en la clase C2, la documentación referente a los requisitos de auditoría será contenida en el manual del recurso confiable. El manual del recurso confiable explicará los procedimientos del registro, examinará, y mantendrá archivos de auditoría. Detallará la estructura de registro de auditoría para cada tipo de evento de auditoría, y deberá incluir el tipo de cada campo y cuál es su tamaño.

El manual del recurso confiable también incluirá una descripción completa de la interfaz del mecanismo de auditoría, la forma en que debe ser utilizado, su configuración y sus valores predeterminados, precauciones sobre los riesgos implicados al usar varias configuraciones y distintas capacidades, y cómo instalar y ejecutar el sistema de forma tal que los datos de auditoría producidos tengan la protección apropiada.

Si los eventos de auditoría pueden estar pre o post seleccionados, el manual debe describir también las herramientas y los mecanismos disponibles así como la forma en que deben ser utilizados.

Riesgos Inevitables de Seguridad

Hay ciertos riesgos involucrados en el proceso de auditoría, existen porque no hay manera de evitar que ocurran estos sucesos. Porque hay ciertos factores imprevisibles implicados en la revisión, es decir, por parte del hombre, de la naturaleza, etc., el proceso de auditoría nunca puede ser ciento por ciento confiable. Las medidas preventivas que pueden tomarse, pueden reducir al mínimo la probabilidad de cualquiera de estos factores que afectan la seguridad proporcionada por el mecanismo de auditoría, pero no existe un mecanismo de auditoría libre de riesgo.

Revisión de Amenazas por Parte del Administrador o de los Usuarios

Incluso con la revisión de los mecanismos para detectar y disuadir violaciones de seguridad, la amenaza por parte de intrusos, administradores o alguna persona involucrada con la seguridad del sistema, estará siempre presente. También es posible que el administrador de seguridad del sistema de un sistema seguro pudiera detener el registro de actividades, mientras que ingresa a los archivos del sistema y los altera para obtener una ventaja personal. Los administradores autorizan al personal, pero como también pueden tener acceso a los datos de identificación y de autenticación, podrían también elegir ingresar el sistema disfrazado como otro usuario para cometer crímenes bajo una identidad falsa.

La gerencia debe estar enterada de este riesgo y debe seleccionar adecuadamente al administrador de seguridad del sistema. La persona que sea seleccionada para una posición tan crítica, como la administración de seguridad del sistema, debe estar conciente de esta responsabilidad antes de que le sean concedidos los privilegios que un día podría utilizar contra la organización.

El administrador de seguridad del sistema también podría ser observado para asegurarse de que no hay variaciones sin explicación en actividades normales. Cualquier desviación de la norma de operaciones puede indicar que una violación de la seguridad ha ocurrido o es inminente de ocurrir.

Una medida de seguridad adicional para controlar esta amenaza potencial, es asegurarse de que el administrador del sistema y la persona responsable de la auditoría son dos personas distintas. La separación de las funciones del auditor de las bases de datos, y del administrador del sistema es una acción importante al separar los privilegios de acceso. Si tal separación no se realizara, y si se permitiera al administrador emprender funciones del auditor o viceversa, la función entera de la seguridad quedaria en la responsabilidad de un solo individuo.

Otra alternativa puede ser emplear papeles separados del auditor. Tal situación puede dar a una persona la autoridad para desactivar el mecanismo de auditoría, mientras que otra persona puede tener la autoridad para activar el mecanismo. En este caso que no existe un individuo pueda desactivar el mecanismo de auditoría, de forma que pueda comprometer el sistema, y después pueda activar el mecanismo de auditoría.

Pérdida de Datos

Aunque la lógica del software y hardware para la auditoría de seguridad sean mecanismos confiables, no son infalibles; como el resto del sistema, son dependientes sobre fuentes de potencia y están expuestos fácilmente a la interrupción debido a los apagones o aspectos mecánicos. Un accidente puede causar la pérdida o destrucción de datos valiosos de la auditoría. El administrador de seguridad del sistema debe estar conciente de este riesgo y debe establecer un procedimiento para asegurar que se tenga un respaldo del registro de auditoría en alguna parte.

El administrador de la seguridad del sistema debe duplicar el registro de auditoría en un medio móvil a ciertos intervalos de tiempo para reducir al mínimo la pérdida de datos en el caso de una falla del sistema. El manual del recurso seguro debe incluir cuáles son las posibilidades y la naturaleza de la exposición de pérdida de datos, y cómo éstos pueden ser recuperados en caso que ocurra una catástrofe.

Si un apagón o una falla mecánica ocurre, el administrador de seguridad del sistema debe asegurarse de que los mecanismos de auditoría funcionan correctamente después de la recuperación de sistema. Por ejemplo, cualquier opción del proceso de auditoría de pre-selección antes de la falla del sistema debe estar seleccionadas después de la recuperación de sistema.

Resumen de la Auditoría

Para las Clases C2 y superiores, se requiere que el Archivo de Auditoría sea capaz de crear, mantener, proteger de la modificación, o de la destrucción del registro de auditoría y restringir el acceso no autorizado a los objetos por él protegidos. El registro auditoría juega un papel importante en el caso de que ocurra un daño grave que logre corromper el sistema.

El registro de auditoría no debe perder de vista los eventos relevantes de seguridad y utilizar los mecanismos de identificación y autenticación, al momento de introducir los en el espacio de algún usuario, o la cancelación de algún objeto del sistema, así como cualquier acción del sistema de administración y cualquier otro evento que pretenda violar la política de seguridad del sistema. Debe existir la opción de que todas las actividades sean auditadas o que el administrador de seguridad del sistema seleccione los eventos a revisar. Si se decide que deben revisarse todas las actividades, deben considerarse los factores mencionados en los párrafos anteriores.

El espacio de almacenamiento necesario para una auditoría total requerirá generalmente de un mayor cuidado por parte del administrador, para prevenir cualquier pérdida de datos y proporcionar la protección adecuada. También existe la necesidad de que el personal autorizado pueda leer todos los eventos escritos en el registro de auditoría. El análisis de todo el registro de auditoría sería una tarea difícil y se desperdiciaría mucho tiempo del administrador. Bajo estas condiciones, se requiere una opción de seleccionar los eventos, ya sea por una pre-selección o por una post-selección.

La información contenida en el registro de auditoría debe ser la suficiente para reconstruir una secuencia completa de los eventos y de los procesos relevantes de seguridad para el sistema.

Para hacer esto posible, el registro de auditoría contendrá la siguiente información: fecha y hora del evento, el usuario, el tipo de evento, si la acción fue ejecutada o rechazada, el origen de la petición, el nombre del objeto introducido en el espacio direccionable del usuario, si guardó o borró algún objeto del sistema, y para la clase B1 y superiores, la determinación de la sensibilidad del objeto.

Debe recordarse que el registro de auditoría será incluido en el TCB y contar con la misma protección que el Archivo de Auditoría. El registro de auditoría estará conforme a los controles de acceso bien definidos.

Un registro de auditoría eficaz es necesario para detectar y evaluar ataques hostiles contra un sistema.

Glosario

Administrador

Cualquier persona o grupo de personas asignados para supervisar todo o una parte del sistema ADP

Administrador de Seguridad del Sistema

Es la persona responsable de la seguridad de un sistema y posee la autoridad para hacer cumplir las políticas de seguridad, posee el acceso a la información de seguridad del sistema.

ADP

Automatic Data Processing (Procesamiento automático de datos). La unión del hardware, de firmware, y software, configurado con el fin de clasificar, de calcular, de analizar, de resumir, de transmitir o recibir o ambas actividades, de guardar, y extraer datos con una mínima intervención del ser humano.

Archivo de auditoría

La totalidad de los mecanismos de protección dentro de un sistema informático, incluyendo el hardware, firmware, y el software, la combinación de estos elementos es responsable de hacer cumplir la política de seguridad.

Un archivo de auditoría consiste en uno o más componentes que juntos hagan cumplir una política centralizada de seguridad concluyendo en un producto o un sistema. La capacidad de un archivo de auditoría de hacer cumplir correctamente una política de seguridad depende solamente de los mecanismos dentro del mismo y del adecuado ingreso de información de los parámetros del personal administrativo del sistema (p.e., separación de los usuarios) relacionado con la seguridad

Auditor

Persona autorizada para actividades administrativas, las actividades incluyen seleccionar los eventos en el sistema para ser revisados, indicar qué eventos de la auditoría van a ser registrados, y analizar el registro de la auditoría.

Auditoría

Conducir la revisión y el análisis de los expedientes independientes y de las actividades del sistema.

Canal Secreto

Un canal de comunicaciones que permite a un proceso transferir información de una manera que omita la seguridad del sistema

Canal Secreto de Almacenamiento

Un canal secreto que implica la escritura directa o indirecta de una dirección de almacenamiento por un proceso y la lectura directa o indirecta de la dirección de almacenamiento por otro proceso. Los canales secretos de almacenamiento implican típicamente un recurso finito (p.e., sectores en un disco) que sea compartido por dos objetos con distinto nivel de seguridad.

Canal Secreto de Sincronización

Un canal secreto por el cual se envía la información de las señales de un proceso a otro, modificando el uso de los recursos de sistema (p.e., tiempo de procesamiento) de manera tal que esta manipulación afecta el tiempo de reacción verdadero observado por el segundo proceso.

Categoría	Es agrupar la información sensible clasificada o sin clasificar, a la cual se aplica la escritura de una etiqueta restrictiva adicional (p.e., propietario, información compartida) que significa que conceden al personal el acceso a la información solamente si se tiene la aprobación formal u otra autorización apropiada
Defecto	Un error de asignación, de omisión o descuido en un sistema que permite que los mecanismos de protección sean violados.
Mecanismo de la Auditoría	El dispositivo que recoge, revisa , y/o examina actividades del sistema.
Nivel de Sensibilidad	El nivel de sensibilidad de los objetos a los cuales el evento ha leído o escrito o ambos un acceso. El nivel de la sensibilidad de un evento debe siempre ser menor o igual que el del usuario al que el evento ha sido asociado
Objeto	Es una entidad pasiva que contiene o recibe información. El acceso a un objeto implica el potencial acceso a la información que contiene. Los ejemplos de objetos son: expedientes, bloques, páginas de memoria, segmentos, archivos, directorios, árboles del directorio y programas, así como dígitos binarios, octetos, palabras, campos, procesadores, dispositivos de video, teclados, relojes, impresoras, nodos de red, etc.
Política de Seguridad	El conjunto de normas, reglas, y prácticas que regulan cómo una organización maneja, protege, y distribuye información sensible
Post - Selección	Selección, por personal autorizado, de eventos específicos que habían sido escritos en el registro de auditoría.

Preselección

Selección, por personal autorizado, de los eventos auditables que deben ser escritos en el registro de auditoría.

Registro de auditoría

Un conjunto de expedientes que proporcionan una justificación de los procesos colectivos, se usan para ayudar a rastrear transacciones originales hacia adelante: de los expedientes a los informes relacionados, o de manera inversa, de los informes a los expedientes y de ahí a su fuente.

Suceso

Una entidad activa, generalmente en la forma de un usuario, un proceso, o un dispositivo que hace fluir la información entre los objetos o cambia el estado del sistema.

Seguridad Llana

La combinación de una clasificación jerárquica y de un conjunto de categorías no-jerárquicas que representa la sensibilidad de la información.

Suceso Auditable

Cualquier suceso que pueda seleccionarse para ser incluido en el registro de la auditoría. Estos sucesos auditables deben incluir, además de los sucesos relevantes de seguridad, las acciones tomadas para recuperar el sistema después del incidente y cualquier acción que pudiera demostrar ser relevante para la seguridad en una ocasión posterior.

TCB

Trusted Computers Bases (Base de computadora confiable).

Usuario

Cualquier persona que interactue directamente con un sistema de cómputo.

Usuario Identificado

Usuario que ha tenido acceso a un sistema por medio de un identificador y una combinación válida de autenticación como el uso de una clave de acceso y una contraseña.

Bibliografía

URL: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>
Computer Security Basics,
Deborah Russell and G.T. Gangemi Sr.
O'Reilly & Associates, Inc.