

## **Auditando Seguridad en UNIX: Una guía práctica**

**Elaborado por:**  
**Departamento de Innovación**  
**[alexei@dcaa.unam.mx](mailto:alexei@dcaa.unam.mx)**

## **Contenido**

I. Introducción

II. Cuándo Auditar

III. Desarrollo de una Política sobre Seguridad

IV. Figura 1 Propuesta de un Proceso conducido para la Implementación de Seguridad

V. Permisos

VI. Alcances

VII. Herramientas

VIII. Llevando a cabo la auditoría

IX. Seguridad Física

X. Servidores

XI. Servicios de Red

XII. Firewall

XIII. Documentación

XIV. Conclusión

XV. Bibliografía

XVI. Referencia

## Introducción



**Jack Maynard**

Si se toma cualquier revista reconocida sobre computación, habrá por lo menos un artículo respecto a la seguridad en las computadoras. Algunos son muy utópicos, mientras que otros dan un punto de vista muy realista de los problemas que está enfrentando la industria de cómputo. Sea cual fuere el punto de vista, la conclusión es la misma: el mundo del cómputo no es tan seguro como alguna vez lo fue. El concepto de sistemas abiertos ha cambiado dramáticamente en los últimos 20 años: de lo que alguna vez fue acceso e intercambio de información, a algo más restringido. Ahora, tener un fuerte programa de información sobre seguridad es algo que debe hacerse. Tener un plan sobre seguridad es un buen comienzo, aunque se debe recordar que se está manteniendo un ambiente con un alto nivel de protección para los recursos de cómputo.

La seguridad en UNIX es una tarea compleja, compuesta por muchas partes, donde los errores son fáciles de cometer, evitando así que se mantenga un ambiente seguro. Con el tiempo, los permisos, las configuraciones y la instalación de nuevo software puede dejar un ambiente de cómputo inseguro y las consecuencias por los errores pueden ser costosas. War Room Research de Baltimore, Maryland, informa que el 67% de las compañías que reportan una violación en su seguridad pagan más de \$50,000 para recuperarse. Si esto parece caro, el mismo informe también dice que el 27% de estas compañías también pagan más de \$500,000 para recuperarse. Claramente, éste es un pretexto para revisar la infraestructura de la seguridad, y un método para hacer esto es la auditoría en seguridad.

## Cuándo Auditar

Dan Farmer, un reconocido experto de seguridad en UNIX y autor de programas como COPS y Satán, recomienda cuándo deben hacerse las auditorías en seguridad.

- Antes de arrancar el sistema
- Programados
- De emergencia (después de una violación en la seguridad)

**Antes de arrancar el sistema:** Los sitios donde no se implementan o refuerzan los procedimientos y estándares cuando se instalan nuevos equipos sobre la red, crean un problema; que es la facilidad de las violaciones en la seguridad. Al auditar estos sistemas antes de arrancarlos (levantarlos), se pueden eliminar los problemas de seguridad que existen en sistemas nuevos. Nunca se debe creer en los estándares y tampoco en la caja de seguridad que ofrece el distribuidor UNIX. Si se endurecen los servidores se conformará un estricto estándar en seguridad y si se eliminan los errores conocidos en los binarios, el control en el acceso y la identificación de un usuario conducirá hacia la reducción de algún riesgo.

**Programados:** Regularmente las auditorías programadas, cuando son hechas de una manera muy completa, indicarán que se están manteniendo los estándares en seguridad y reducirá de una manera exitosa el riesgo de un incidente en el área de seguridad. El tamaño de un sitio, la complejidad de éste y el personal son puntos

que deben ser considerados cuando se decida con qué frecuencia se deben hacer las auditorías programadas. También se puede usar la siguiente guía como base para hacer las auditorías de una manera programada:

- servidores individuales  
auditar cada 12 - 24 meses
- redes grandes  
auditar cada 24 meses
- redes pequeñas  
auditar cada 12 meses
- firewall  
auditar cada 6 meses (o menos)

**De emergencia:** Si alguna vez se experimenta un incidente en seguridad, se deberá determinar el tamaño del daño. Una auditoría puede ayudar, aunque es extremadamente difícil hacerlo sin la asistencia de un software para revisar la integridad del equipo antes del incidente. El sistema operativo UNIX consiste de un gran número de archivos y directorios (todo en UNIX es un archivo). Los programas de integridad como TAMU Tiger o Tripwire, cuando se implementan antes de que se hayan experimentado problemas, pueden ayudar a identificar los cambios en los permisos de los archivos y directorios, el dueño, características de archivo y modificaciones a los binarios del sistema operativo.

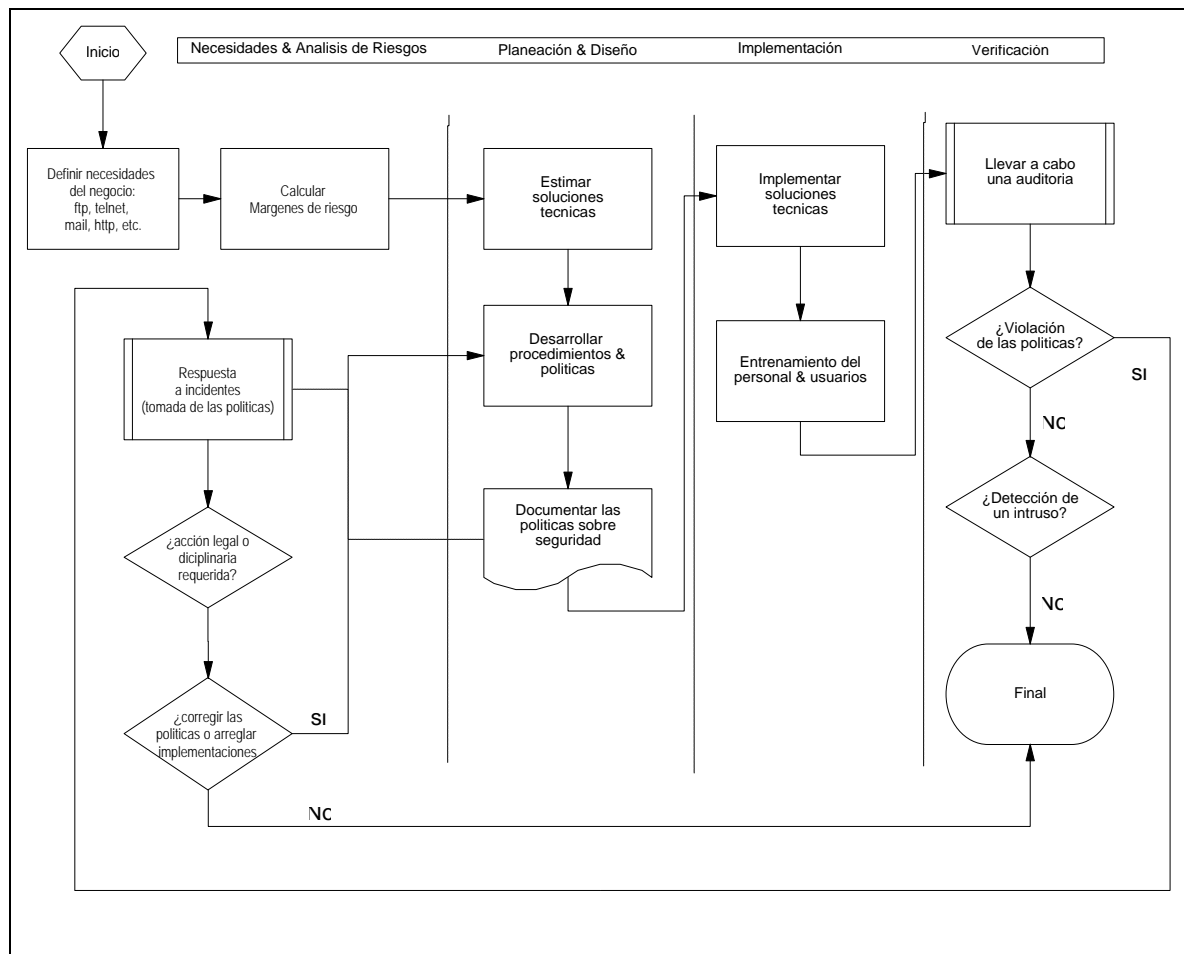
## Desarrollo de una política sobre seguridad

La palabra auditar significa "examinar con la intención de verificar". Una auditoría en seguridad es un intento para verificar que día con día la operación del ambiente de cómputo esté alineado con la información de las políticas sobre seguridad. Las políticas sobre seguridad deberán ser la base para una auditoría. Este es el estándar contra el que las configuraciones son medidas. Hasta que se tengan políticas comprensivas sobre seguridad, no se podrá medir si se está alcanzando la meta de mantener un ambiente seguro. La información en las políticas sobre seguridad varían de sitio a sitio, mientras que otros no la tienen. Si existen políticas, entonces una auditoría podrá verificar si las operaciones están cumpliendo con ellas. Si no, se puede auditar usando lo que es considerado "una buena práctica", pero se necesitará la asistencia de alguien que esté familiarizado con esta. Muchos libros sobre seguridad muestran una lista de pasos que se enfocan

a una buena seguridad, pero estos realmente atacan el problema desde una dirección equivocada -desde un modelo bottom up (del fondo hacia arriba). Cualquier implementación en la seguridad que no dirige el resultado desde un enfoque de procesos conducidos es un intento mal hecho, y fallará al proveer seguridad comprensiva.

La figura 1 muestra un proceso conducido con un enfoque top-down para la implementación en la seguridad. Si no se tiene alguna política, entonces se necesitará empezar por la parte de "Necesidades y Análisis de riesgos". Aquí se identifican las necesidades del negocio, los activos de cómputo y los posibles riesgos a estos activos. Desde aquí se pueden estimar y desarrollar soluciones técnicas y operacionales convenientes para las necesidades del negocio y así proteger los activos de cómputo.

**Figura 1 Propuesta de un proceso conducido para la implementación de seguridad**



## Permisos

La documentación de cómo se implementarán estas soluciones será la información de las políticas sobre seguridad. Hay muchos recursos disponibles que ayudan a desarrollar un escrito sobre las políticas. Una manera rápida para implementar una política es con una copia del libro de Charles Cresson Wood titulado *Information Security Policies Made Easy*. El libro y un disquete que acompaña al primero viene con 730 políticas prescritas, y una explicación para cada política. El libro cubre casi todas las áreas relacionadas con la información sobre seguridad. Usando los estilos de las políticas proporcionadas, se puede hacer rápidamente una política para un sitio en particular.

Se puede enviar también un correo electrónico a: [charles@baselinesoft.com](mailto:charles@baselinesoft.com) para obtener información sobre cómo obtener una copia.

Otro recurso informativo es el completamente gratis RFC1244, Manual

sobre seguridad en sitios, publicado por el Personal de Tareas sobre Ingeniería en Internet (the Internet Engineering Task Force, o IETF). Los RFC son "solicitados para comentarios", y son usualmente precursores de estándares de Internet para una tecnología en particular. Este documento FYI de 100 páginas ayuda a los administradores de sistemas a preparar políticas sobre seguridad de un sitio específico. Éste proporciona información sobre políticas para ingresar a los recursos de cómputo, procedimientos para prevenir problemas sobre seguridad y recomendaciones para manejar incidentes en la seguridad. Se puede encontrar en el Web en:

<http://ds.internic.net/rfc/rfc1244.txt>

O

<ftp://info.cert.org/pub/irtf/ssphwg/rfc1244.txt>

## Alcances

Antes de verificar algo, se debe conocer qué se está verificando. Dependiendo del tamaño de la compañía, una auditoría deberá cubrir plenamente los límites o deberá por lo menos; ser muy minuciosa. Es importante identificar el objetivo y los límites de lo que se intenta auditar. Una auditoría comprensiva deberá cubrir cada sección de las políticas sobre seguridad. Las áreas más comunes para una auditoría incluyen:

- Seguridad física
- Servidores

- Servicios de red
- Firewall

Una vez que se han identificado los alcances de la auditoría y se han obtenido los debidos permisos, se puede empezar. Como se mencionó anteriormente, una auditoría es un procedimiento para comparar las operaciones diarias con las políticas establecidas. Esto puede ser un trabajo tedioso si no se tiene alguna herramienta que pueda ayudar, así que aquí se mencionan algunas de las más comunes.

## Herramientas

Las herramientas para la auditoría en seguridad caen en dos tipos: comerciales o productos comunes de anaquel (common off the shelf, COTS) y contribuidos o de dominio público. Algunos son útiles para auditorías, mientras que otros ayudan en la seguridad llevada por los sistemas y por la red.

Algunas de las categorías son:

- Herramientas de auditoría basada en servidores
- Herramientas de auditoría para redes amplias
- Herramientas para el análisis de tráfico en red
- Herramientas para el manejo de la seguridad
- Herramientas para la seguridad del perímetro y firewall
- Herramientas para encriptamiento
- Herramientas para la verificación

Cualquiera que esté relacionado con UNIX podrá recomendar una herramienta o podrá dar algún consejo. UNIX proporciona una variedad de comandos, utilerías y lenguajes que ayudan en el desarrollo de un programa para alguna necesidad.

Hay más herramientas dentro de la categoría de dominio público para la información sobre seguridad que, tal vez, en otra subcategoría de la administración de sistemas. Aunque algunos de nosotros no tengamos el tiempo o la habilidad de escribir un paquete comprensivo de herramientas para la auditoría en seguridad, muchas de las herramientas de dominio público están escritas por especialistas muy respetados en seguridad, mientras que otros, son de gente de la que jamás se ha escuchado. Esto nos lleva a una pregunta fundamental: ¿A quién creer?. Se deberá creer en los resultados de las herramientas en auditoría. Para hacer esto, se debe verificar que todas las

herramientas usadas en una auditoría no hayan sido falsificadas.

Algunas compañías tienen como política prohibir el uso de software de dominio público. Si no está limitando en el uso de soluciones tipo COTS, hay muchas herramientas para seguridad de dominio público muy respetadas que son consideradas "el standard de la industria". El código fuente para casi todos estos programas está disponible para su inspección, lo cual reduce el riesgo de un programa caballo de Troya dentro del software. Si se es paranoico, se puede examinar el código fuente, o si se cree en el autor y la organización de distribución, entonces la integridad de estos programas, los cuales son distribuidos sobre Internet, pueden ser validados con la ayuda de firmas digitales.

Una firma digital indica si un archivo o un mensaje ha sido modificado. El tipo de firma digital más usado es el resumen de mensajes. Un resumen de mensajes (también conocido como cryptographic checksum o cryptographic hash-code) es un número especial producido por una función que es muy difícil ( si no imposible) de invertir. Usando un programa de resumen de mensajes como MD5, que genera 128 bits de salida, habrá  $1.7 * 10^{38}$  posibles valores de salida de la misma longitud para intentar encontrar una entrada que genere la correcta salida. Otro fuerte método de verificación - también usado para verificar la integridad de los archivos- es PGP, Muy Buen Programa de Privacidad de Phil Zimmerman (Pretty Good Privacy program), el cual usa una clave pública de encriptamiento para proteger archivos de datos y correos electrónicos. El autenticador usa su clave privada para encriptar una firma digital, la que puede ser verificada por cualquiera usando el autenticador de claves públicas para desencriptarlo. Estos métodos



proporcionan un medio de verificación para verificar la integridad de las herramientas de auditoría.

Hay muchas fuentes para obtener herramientas de seguridad de dominio público en Internet. Tal vez uno de los más respetados es el archivo de seguridad Coast, localizado en el Departamento de Ciencias de Cómputo de la Universidad de Purdue. Coast quiere decir Herramientas de Seguridad, Auditoría y Operaciones de Cómputo (Computer Operations, Audit, an Security tools). Se puede encontrar en:

<http://www.cs.purdue.edu/coast>  
o también

<ftp://coast.cs.purdue.edu/pub/tools/unix>

Según Coast, ellos tienen el más largo archivo en Internet de información, herramientas, estándares, reportajes, listas de correo y otra información relacionada a la seguridad en cómputo, leyes, respuesta a incidentes y protección de la información. Se puede ver este sitio y encontrar algo interesante. Este sitio deberá ser la primera parada para información y recursos sobre información de seguridad. Si se prefiere usar soluciones desarrolladas por empresas, hay muchas opciones. Una variedad de productos comerciales son ofrecidas por varias empresas de seguridad como:

Los Sistemas de Seguridad en Internet (Internet Security Systems), el cual está localizado en:

<http://www.iss.net>

en donde se ofrece un rango completo de exploradores de Internet, de red, de firewall y de servidores conocido colectivamente como "SAFEsuite".

Otro recurso es Datalinx, localizado en:

<http://www.dlxguard.com>

Aquí se ofrecen varios productos incluyendo "Guardian", "Stalker" y "suGuard". Guardian permite control en las cuentas y el control en el acceso, y Stalker provee un sistema de monitoreo el cual dice quién hizo qué cosa, cuándo, dónde y cómo. SuGuard permite asignar responsabilidades del sistema sin revelar contraseñas.

Si se cuenta con algún sistema HP-UX, se puede visitar el siguiente sitio:

<http://www.hp.com/go/security>

Estos son algunos ejemplos de varias compañías que ofrecen soluciones comerciales. Una vez que se halla revisado las opciones comerciales y las de dominio público, se deben obtener aquellas, herramientas con las cuales se cubrirán las necesidades para cada categoría en la que se planea auditar (física, servidores, red, firewall).

## Llevando a cabo la auditoría

Un buen principio para llevar a cabo una auditoría es entrevistando a un porcentaje de los usuarios y del personal técnico y de administración. El sentido de las entrevistas es entender de que manera estos individuos creen que trabaja la seguridad, y cómo están implementando las políticas de la misma. Por ejemplo, en las entrevistas de usuarios se puede preguntar qué tan seguido cambian sus contraseñas (passwords) y si entienden las reglas de cómo debe estar compuesta una contraseña; al hacerlo se tendrá una idea de la forma en que el usuario entiende las políticas sobre seguridad. Para obtener una completa cooperación por parte de los usuarios, lo anterior deberá estar hecho de una manera clara, advirtiéndoles que no habrá ninguna sanción por una respuesta incorrecta y que ningún nombre será usado en el reporte de la auditoría. Al entrevistar a varios usuarios, se verá si entienden las políticas publicadas y si éstas están siendo

cumplidas como parte de la responsabilidad de su trabajo. Se recomienda para la realización adecuada del reporte de auditoría que los usuarios tengan un entrenamiento en el cual adquieran conciencia de la importancia de la seguridad en la red. Una entrevista similar puede ser hecha al personal de administración, preguntándoles si se les comunicó de la renuncia de un empleado o de una baja temporal, permitiendo así la desactivación de la cuenta del usuario. Cuando las entrevistas se hayan realizado, se tendrá una perspectiva de lo que se encontrará cuando se audite a los servidores y a las redes.

Se han definido cuatro áreas para examinar durante una auditoría. Éstas son física, servidores, redes y firewall. Aunque es imposible cubrir cada dispositivo que se quiera revisar, aquí se discutirán los más comunes.

## Seguridad Física

Esta área se refiere al acceso físico en los recursos de cómputo: Los concentradores, ruteadores, bridges, sistemas y otros componentes de la red son propensos a abusos si son fácilmente accesados. Todos los recursos de cómputo deben ser accesados solamente con una autorización individual. El acceso a los sistemas y a las consolas debe ser restringido a una área segura. Las claves o códigos deben ser cambiados regularmente y también cuando alguien con una clave o código deja la compañía. Los ductos y canaletas de cableado no deberán ser accesados fácilmente, porque alguien se puede conectar al backbone y rastrear las contraseñas (passwords) u otra información crítica de la red.

Otra área sujeta a abusos es la información guardada en medios de respaldo. Cualquiera con acceso a estos medios pueden reinstalar los respaldos a una máquina de otro sitio y recuperar los datos guardados. La información importante de impresiones o medios magnéticos deberá ser destruido o guardado si no se utiliza. Una técnica común para obtener información guardada es la llamada "clavado al basurero" (dumpster diving), la cual consiste en examinar la basura de una compañía en busca de desperdicios en binarios con la esperanza de encontrar una contraseña o información referente a la red. El contenido de estos binarios deberá ser destruido para prevenir la divulgación accidental de este tipo de información.

## Servidores

La seguridad en los servidores se refiere principalmente al control y autenticación en el acceso. Esta es una área que con el tiempo se debilita. Casi todos los sistemas UNIX son configurados para usar lo que es conocido como Control de Acceso Discreto (Discretionary Access Control), el cual permite al dueño de algún recurso asignar diferentes permisos (leer, escribir y ejecutar) a las tres categorías de usuarios, conocidos como: usuario (el dueño del archivo), grupo (los usuarios en el grupo al que pertenece el archivo) y otros (todos los demás usuarios). Casi todos los servidores están compuestos de una serie de privilegios que pueden aumentar con el tiempo. Todo lo que requiere un intruso para ganar la entrada al sistema es utilizar un usuario con pocos permisos en los archivos o con una débil contraseña; desde aquí, el intruso puede incrementar los privilegios a través de un débil control en el acceso hasta que finalmente gana el acceso y los privilegios de

root. Algunas de las áreas claves para auditar a la seguridad del servidor son:

- Composición de las contraseñas
- Formato del archivo de contraseñas
- Formato del archivo de grupos
- Permisos en los dispositivos de archivos
- Bitácoras de sistema
- Programas QUID y SIGA
- Propiedad y permisos para root
- Permisos por omisión en la creación de archivos
- Programas de inicio del sistema
- Permisos para los directorios de los usuarios
- Permisos para programas temporizados
- Software Instalado por el distribuidor
- Modems no asegurados
- Errores conocidos en binarios
- Parches en los programas del distribuidor

## Servicios de Red

Los motivos para tener seguridad en la red son simples: proteger los servidores de algún acceso sin autorización y de los ataques a la red. También protegerse de algún protocolo débil que haya sido explotado en el pasado. Las políticas deben definir qué servicios están permitidos. Todos los demás servicios no permitidos explícitamente por las políticas deberán ser negados. Algunas áreas para auditar con respecto a la seguridad de la red incluyen:

- Archivos de configuración y servicios de red
- Sistemas de exportación de archivos NFS
- NIS
- DNS
- Sistemas de monitoreo
- Configuraciones de ftp y tftp
- Equivalencia de servidores y relaciones

## Firewall

Un firewall es asignado para la defensa del perímetro, al englobar la custodia de la red. Tradicionalmente, los firewalls son el punto de demarcación entre la red custodiada y el mundo exterior. Muchas veces la estrategia ha sido endurecer la seguridad del firewall para disminuir la necesidad de seguridad en el interior de las redes. Muchas compañías, aunque se dan cuenta de los múltiples incidentes en la seguridad ocurren con mayor frecuencia dentro de la red que desde afuera. Esto ha conducido al incremento en el uso de firewalls en departamentos claves, como los de investigación y desarrollo o finanzas. En cualquier caso, debe otorgarse una atención particular a la seguridad de los firewalls. Algunos firewalls son simplemente ruteadores empaquetadores de protección. Esto no es la solución ideal, pero puede ser un impedimento suficiente en algunas situaciones. Si se usan ruteadores de protección, CERT recomienda filtrar los siguientes servicios:

- Transferencia de zona DNS - puerto 53 (TCP)
- tftpd - puerto 69 (UDP)
- enlace - puerto 87 (TCP)

- SunRPC y NFS - puerto 111 y 2049 (UDP/TCP)
- BSD UNIX comandos "r" puertos 512, 513 y 514 (TCP)
- lpd - puerto 515 (TCP)
- uucpd - puerto 540 (TCP)
- Openwindows - puerto 2000 (UDP/TCP)
- X windows - puerto 6000+ (UDP/TCP)

Hay otros puertos que deberán ser filtrados dependiendo de las políticas asignadas. Debido a que hay una gran variedad de implementaciones firewall, no se puede discutir todo lo que debe ser auditado con respecto a los firewalls, pero varios principios deben ser mantenidos a pesar de las implementaciones:

- Poner atención a los puertos y servicios configurados
- Deshabilitar todos los servicios y programas no esenciales
- Borrar todos los manejadores no esenciales del kernel
- Recordar que el firewall es sólo la puerta delantera, otros servicios (Modems) pueden permitir la entrada por la puerta lateral.

## Documentación

Una vez que se ha completado la fase de investigación de la auditoría, se deben documentar los resultados de las investigaciones. Esta documentación debe incluir lo que está funcionando bien y lo que no está funcionando. Al hacer un resumen de lo que tiene éxito, se podrá validar si la inversión en el desarrollo y entrenamiento en seguridad ha valido la pena. También se debe documentar los puntos que son diferentes de las políticas asignadas.

Debido a la naturaleza clave de un reporte sobre auditoría, la distribución inicial debe ser limitada sólo a los directivos y sólo como necesidad de información; todas las copias debe ser numeradas y firmadas. Si una auditoría descubre violaciones serias en las políticas o incluso actividad criminal, en este caso los directivos deben decidir cómo manejar el incidente. Las políticas sobre seguridad deben también tener una sección respondiendo sobre los incidentes.

Después de que el reporte inicial ha sido revisado con los directivos, las acciones pueden ser asignadas al personal de soporte y a los administradores de sistemas para que realicen las correcciones correspondientes. El reporte de la auditoría nunca debe ser guardado electrónicamente en un sistema

sin algún tipo de seguridad efectiva. Todas las copias del reporte de la auditoría deberán ser también aseguradas. Con el tiempo, si se realizan más auditorías, los reportes previos ofrecerán una información valiosa sobre cómo mejorar las políticas y los procedimientos.

## Conclusión

La clave para mantener un ambiente seguro de cómputo es la consistencia. Siendo consistente en la forma como se implementa la seguridad en los servidores, en las redes y el ambiente físico, y en el conjunto con auditorías regulares, se podrán descubrir inconsistencias y se podrán reducir de una manera excelente los riesgos de incidentes relacionados con la seguridad.

Se debe recordar que las auditorías no deben ser un sustituto de una revisión periódica de las bitácoras (log files). Por lo tanto debe mantener el rastreo de quienes estén accedando los servicios de red. Una revisión activa de las bitácoras de manera diaria o semanal permitirá detectar las actividades no autorizadas antes de una auditoría programada.

## Bibliografía

Garfinkel, S. y Spafford, G. 1996  
***Practical UNIX and Internet Security***. pp. 167-168  
O'Reilly & Associates, Sebastopol, CA

Bernsein, T., Bhimani, A., Schultz, E., y Siegel, C 1996  
***Internet Security For Business***. pp 77-82  
John Wiley & Sons.

Wood, C.C. 1996  
***Information Security Policies Made Easy***.  
Baseline Software.

Site Security Policy Handbook Working Group, 1991.  
***Site Security Handbook***. RFC 1244  
Internet Engineering Task Force

Pipkin, D.L 1997  
***Halting the Hacker***, pp. 88-90  
Prentice Hall.

Wietse, V., y Farmer, D. 1996  
***Security Auditing & Risk Anasysis***  
Internet

## Referencia

Maynard, Jack "***UNIX Security Auditing: A Practical Guide***".  
Sys Admin TM. The journal for UNIX Systems Administrators  
Mayo 1997, Volumen 6 Número 5. Páginas 67 - 72.