

# La Auditoria de Seguridad en las empresas: puntos a tener en cuenta

Juan E. Pecantet

Artículo originalmente publicado en

<http://www.shellsec.net/articulo/auditoria-empresas/>

05 de enero de 2006

**Nota de [www.segu-info.com.ar](http://www.segu-info.com.ar):** El artículo no hace referencia a ninguna otra fuente ni contacto. Se publica tal como está sin ninguna garantía y no se asume ninguna responsabilidad por el contenido del mismo.

La información es el activo mas importante para las empresas, lo cual se puede confirmar si consideramos el hecho de la perdida de información critica, y la post recuperación con la cual la entidad podría retomar sus operaciones normales en un menor tiempo, que si ocurre lo contrario. Por este motivo la información adquiere una gran importancia para la empresa moderna debido a su poder estratégico y a que se invierten grandes cantidades de dinero en tiempo de proporcionar un buen sistema de información para tener una mayor productividad.

## La importancia en que radica auditoria de sistemas en las organizaciones son:

- Se puede difundir y utilizar resultados o información errónea si los datos son inexactos o los mismos son manipulados, lo cual abre la posibilidad de que afecte seriamente las operaciones, tomas de decisiones o la imagen de la empresa.
- Las computa, servidores y centros de base de datos se han convertido en blanco para fraudes, espionaje, delincuencia y terrorismo informático.
- La continuidad de las operación, administración y organización de la empresa no debe permanecer en un sistema mal diseñado, ya que podría convenirse en un serio peligro para la empresa.
- Existen grandes posibilidades de robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problemas en un lapso razonable, es decir, el usuario percibirá que está abandonado y desatendido permanentemente, esto dará una mala imagen de la organización.
- En el Departamento de Sistemas se observa un incremento de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio, la elaboración y la actualización de los planes de contingencia para lograr este objetivo.

- El inadecuado uso de la computadora para usos ajenos a la organización que puede llegar a producir problemas de infiltración, borrado de información y un mal rendimiento.
- Las comunicaciones es el principal medio de negocio de las organizaciones, una débil administración y seguridad podría lograr una mala imagen, retraso de negocios, falta de confianza para los clientes y una mala expectativa para la producción.

La Auditoria de la Seguridad Informática en la informática abarca el concepto de seguridad física y lógica. La seguridad física se refiere a la protección de hardware y los soportes de datos, así también como la seguridad del los edificios y las instalaciones que lo albergan. Esto mismo contempla situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

Por su parte la seguridad lógica se refiere a la seguridad del uso de software, protección de la información, procesos y programas, así como el acceso ordenado y autorizado de los usuarios a la información.

El auditar la seguridad de los sistemas, también implica que se debe tener cuidado que no existan copias piratas, o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.

### **En la auditoria para aplicaciones de Internet se produce una verificación de los siguientes aspectos:**

- Evaluación de los riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
- Evaluación de vulnerabilidades y arquitectura de seguridad implementada.
- Verificar la confidencialidad e integridad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

### **Metodología de trabajo de Auditoria**

El método del auditor pasa por las siguientes etapas:

- Alcances y Objetivos de la Auditoria Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoria.
- Elaboración de Plan y de los Programas de trabajo.
- Actividades propiamente dichas de la auditoria.
- Confección y elaboración del informe final.

Como he dicho antes las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Para esta razón, es necesario que las organizaciones mantengan a sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos.

La privacidad de las redes es un factor muy importante ya que las empresas se sienten amenazadas por el crimen informático. El mantener una red segura fortalece la confianza entre los clientes de la organización y mejora su imagen corporativa, ya que muchos son los criminales informáticos que acechan día a día.

Por lo cual el auditor o consultor informático ayuda a mantener la privacidad de las redes, trabajando en los siguientes factores: Disponibilidad - Autenticación - Integridad - Confidencialidad

Es preciso tener en cuenta todos los factores que puedan amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

#### **Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:**

- Interceptación de las comunicaciones.
- Acceso no autorizado a ordenadores o Redes de ordenadores
- Perturbación de las redes.
- Ejecución de programas que modifiquen o dañen los datos.
- Declaración falsa.
- Accidentes no provocados.
- Robo de datos.
- Infiltración de datos críticos.

#### **Los beneficios de un sistema de seguridad son:**

- Aumento de la productividad
- Aumento de la motivación del personal
- Compromiso con la misión de la compañía
- Mejoras de las relaciones laborales
- Mejoras del rendimiento
- Mayor profesionalismo
- Ayuda a formar equipos competentes
- Mejora los climas laborales de los RR.HH

Desarrollar un sistema de seguridad significa "planear, organizar, coordinar dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa".

### **Etapas para implementar un sistema de seguridad**

- Introducir el tema de seguridad en la visión de la empresa.
- Definir los procesos de flujo de la información y sus riesgos en cuento a todos los recursos participantes.
- Capacitar a los gerentes y directivos, contemplando el enfoque global.
- Designar y capacitar supervisores de área.
- Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras en menor tiempo.
- Mejorar las comunicaciones internas
- Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel
- Capacitar a todos los trabajadores en los elementos de seguridad básica, riesgo de manejo de software y seguridad física.