# SEGURIDAD INFORMÀTICA

Hay que tener en cuenta que la seguridad informática no es un producto, más bien es un proceso y, por lo tanto se puede definir a la seguridad informática como: un conjunto de métodos y herramientas destinados a garantizar la confidencialidad, integridad y disponibilidad de la información, y por ende proteger los sistemas informáticos ante cualquier amenaza.

En Infoservig Llevamos a cabo una serie de protocolos de seguridad empresarial que abarcan:


- **Análisis del estado del Sistema**
- **Fichero de datos**
- **Copias de seguridad**
- **Configuración de cuentas y perfiles de usuario**
- **Configuración de las politicas de copias de seguridad de datos**
- **Instalacion y configuración de Firewalls / Cortafuegos**
- **Instalacion y configuración de Software antivirus para pequeñas y grandes empresas.**
- **Antivirus para Servidores.**
- **Instalacion y configuración de servidores**
- **Detectores de Intrusos WiFi.**
- **Encriptación y Firma Digital.**
- **Backups centralizados y remotos. (On site y off site)**

- **Seguridad Perimetral:**

- **Firewalls (Hardware y Software)**
- **Instalaciòn de un Proxy**
- **Detectores de Intrusos.**
- **Hardening Windows Server**

Dirección: Cuzco Sur # 116 Piura
Referencia: A Espaldas del Teatro Municipal
Web: http://www.infoservig.com

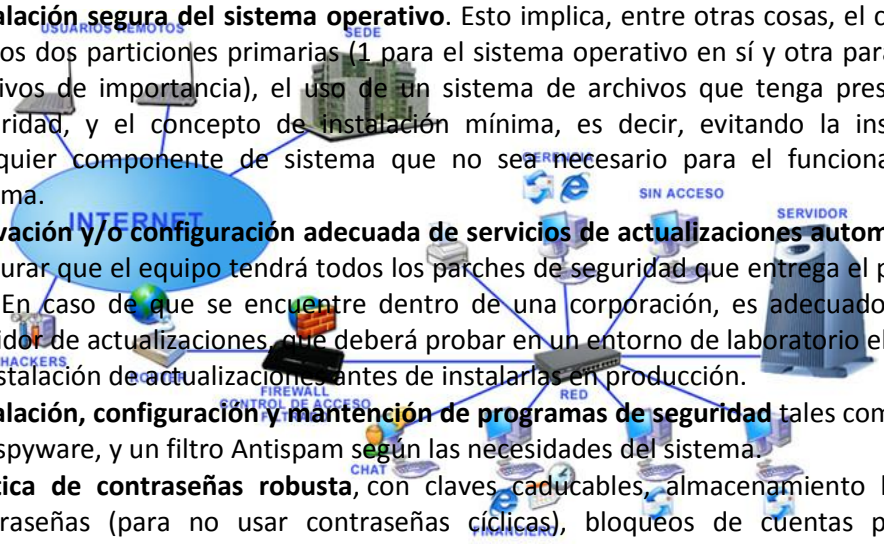
Cel.: 969297908
Rpm: #969297908
Correo: Alfredo@infoservig.com

# Hardening de Servidores Windows

Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc. Innecesarios en el sistema así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas;

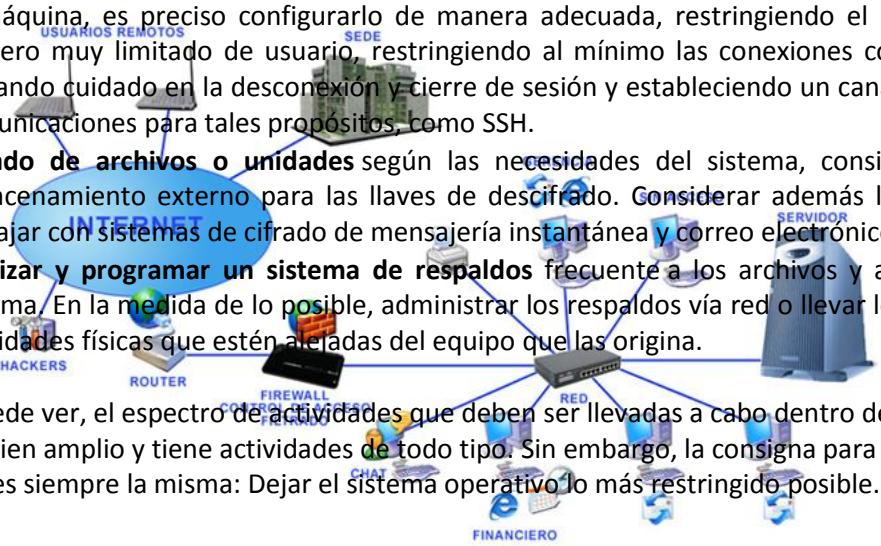
Entre las actividades propias de un proceso de hardening se pueden contar las siguientes:

- **Configuraciones** necesarias para protegerse de posibles ataques físicos o de hardware de la máquina. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.
- **Instalación segura del sistema operativo**. Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (1 para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.
- **Activación y/o configuración adecuada de servicios de actualizaciones automáticas**, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una corporación, es adecuado instalar un servidor de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.
- **Instalación, configuración y mantención de programas de seguridad** tales como Antivirus, Antispyware, y un filtro Antispam según las necesidades del sistema.
- **Política de contraseñas robusta**, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.
- **Renombramiento y posterior deshabilitación de cuentas** estándar del sistema, como administrador e invitado.
- **Asignación correcta de derechos de usuario**, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.
- **Restricciones de software**, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.
- **Activación de auditorías de sistema**, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.
- **Configuración de servicios de sistema**. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.




Dirección: Cuzco Sur # 116 Piura
Referencia: A Espaldas del Teatro Municipal
Web: http://www.infoservig.com
Cel.: 969297908
Rpm: #969297908
Correo: Alfredo@infoservig.com

- **Configuración de los protocolos de Red**. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.
- **Configuración adecuada de permisos de seguridad** en archivos y carpetas del sistema. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.
- **Configuración de opciones de seguridad** de los distintos programas, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.
- **Configuración de acceso remoto.** En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.
- **Cifrado de archivos o unidades** según las necesidades del sistema, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.
- **Realizar y programar un sistema de respaldos** frecuente a los archivos y al estado de sistema. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.




Como se puede ver, el espectro de actividades que deben ser llevadas a cabo dentro de este proceso es bien amplio y tiene actividades de todo tipo. Sin embargo, la consigna para todas estas actividades es siempre la misma: Dejar el sistema operativo lo más restringido posible.

# Auditoria Informática

La rápida evolución de la tecnologia y la informática expone a riesgos constantes nuestra información, datos financieros, estructura empresarial y sistemas de información. Debido a la significativa complejidad de los diferentes sistemas que se interconectan en su organización, y a pesar de las precauciones en defensa y seguridad que podamos implementar, es necesaria una supervision que ayude a determinar el nivel de seguridad que su organización necesita. El servicio que ofrecemos, le proporcionará a su organización toda la información necesaria para poder evitar vulnerabilidades a riesgo operacional, asegurando la eficacia de la seguridad implementada a nivel corporativo. Nuestros clientes se benefician con datos reales, recibiendo completos informes con lo que podrá comprobar fehacientemente donde se encuentra la brecha de seguridad, y poder implementar las herramientas requeridas para evitar que posibles intrusos tengan acceso a su información.


**Nuestras auditorías incluyen iniciativas estratégicas de seguridad**

- Detección de vulnerabilidades e identificacion de riesgos verdaderos
- Evaluación de sistemas de seguridad, sistemas de red, aplicaciones web, y detección contra posibles amenazas
- Pruebas de penetración e intromisión que conducen a configuración eficiente de sistemas y lenguajes de programación.
- Validación de resultados en exploración de la vulnerabilidades web estableciendo claramente los riesgos mas críticos.
- Determinación del correcto funcionamiento de la seguridad externa Firewall y otras defensas.

**Nuestras auditorías tienen un impacto directo que incluye:**

- Comprensión de amenazas e incidentes de seguridad, que determinarán exactamente donde su organización se expone a los riesgos complejos.
- Servidores y sitios de trabajo de red identificando e impidiendo la explotabilidad de Sistemas y vulnerabilidades en la infraestructura en red.
- Filtro y validación de resultados por exploración, identificando debilidades críticas y de alta prioridad para la remediación.
- Uso de sistemas por usuarios finales para evitar las vulnerabilidades críticas que pueden abrir la puerta a su red.
- Determinación de suceptibilidad a phishing, a y otras amenazas de ingeniería social.
- Medición capacidad y alcance de sus aplicaciones web, comercio electrónico, servicio de atención al cliente y de otras aplicaciones web de soportar tentativas de la abertura de los datos.
- Evaluación de sus redes y su seguridad en el ambiente.

Dirección: Cuzco Sur # 116 Piura
Referencia: A Espaldas del Teatro Municipal
Web: http://www.infoservig.com
Cel.: 969297908
Rpm: #969297908
Correo: Alfredo@infoservig.com