10 CONSEJOS PARA MANTENER TU NEGOCIO LIBRE DE **AMENAZAS INFORMÁTICAS**

Virus, troyanos, spyware, robo de identidad, phishing, hackers...
Las amenazas que acechan a tu empresa desde Internet son cada vez más numerosas y sofisticadas.

Protégete ya de la forma más fácil, aplicando en tu trabajo diario estos sencillos consejos de seguridad de Panda Software.

© Panda Software International, 2006.

01. Instala una buena solución de seguridad

El primer consejo de seguridad es el más básico. Para proteger tu negocio es vital contar con un buen antivirus o suite de seguridad.

¡Pon en práctica este consejo!

Estas son las características fundamentales que debe cumplir una buena solución de seguridad:

- Debe proteger frente a **todo tipo de amenazas** (virus, gusanos, troyanos, spyware, hackers...), con especial atención al robo de identidad y las estafas online.
- Debe incluir **tecnologías preventivas**, diseñadas específicamente para proteger de los virus y otras amenazas "desconocidas" (aquellas que no están "fichadas" por los antivirus).
- Debe **cubrir todos los puntos de tu red**: estaciones de trabajo, servidores, oficinas remotas y dispositivos móviles.
- Tiene que **actualizarse** automáticamente y con frecuencia, ser **fácil de usar** y **no penalizar** el rendimiento de tus equipos.
- Tiene que incluir unos excelentes servicios de apoyo, sobre todo un **soporte técnico** siempre disponible.

02. Mantén tu protección siempre activa y actualizada

Tu solución de seguridad debe tener activada la protección automática de forma permanente. Sólo así podrá vigilar todas las operaciones realizadas en el ordenador que puedan suponer algún riesgo.

Además, es imprescindible que esté siempre actualizada para que pueda protegerte de las amenazas más recientes, que suelen ser las más activas y peligrosas.

¡Pon en práctica este consejo!

- Asegúrate de tener **siempre activada la protección automática** de tu antivirus o suite de seguridad. Si no sabes cómo hacerlo, consulta la guía de uso (por ejemplo, las soluciones de Panda muestran un icono en la barra de escritorio indicando que está activa).
- Comprueba que tienes activada la opción de **actualizaciones automáticas** de tu solución de seguridad.
- Asegúrate de **mantener siempre en vigor las actualizaciones y demás servicios** asociados a tu solución de seguridad, renovando tu suscripción cuando proceda.

03. Precaución con el robo de identidad y los cibercriminales

Los hackers se están profesionalizando y ahora tienen una motivación básicamente económica, convirtiéndose en auténticos "cibercriminales".

En muchos casos, las víctimas de sus ataques son las empresas. Delitos como el espionaje industrial vía Internet, el robo de identidad (claves de acceso y otros datos confidenciales) y todo tipo de estafas online (como el phishing) son cada vez más frecuentes. Por tanto, es imprescindible extremar las precauciones.

¡Pon en práctica este consejo!

El cibercrimen es difícil de combatir sólo con consejos, ya que en muchos casos nos enfrentamos a malware diseñado "a medida", pero hay prácticas muy recomendables, sobre todo para defenderse de las estafas online:

- Instala en tus ordenadores **suites de seguridad** diseñadas para bloquear los intentos de estafa online y el robo de identidad.
- **No te fíes de las apariencias**. Por ejemplo, los correos electrónicos de "phishing" utilizan el nombre o la imagen de compañías reales y suelen llevar como remitente el nombre de un empleado real.
- No contestes a ningún correo que solicite **información personal o financiera**.
- Nunca entres en la web de tu banco **pulsando en links** incluidos en correos electrónicos.
- Antes de introducir tus datos, **asegúrate de estar en una web segura**. Para comprobarlo, fíjate en que su dirección empiece por https:// y que aparece en la barra de estado de tu navegador un pequeño candado cerrado.
- Recuerda: ante la mínima duda, **abstente de facilitar información confidencial**.

04. Aplica cuanto antes los parches de seguridad

En algunos casos, los programas presentan anomalías de funcionamiento, conocidas como vulnerabilidades, que pueden ser aprovechadas por los hackers con fines ilícitos.

Cuando los fabricantes detectan una nueva vulnerabilidad, ponen a disposición de los usuarios los “parches” de seguridad para solucionarlos.

¡Pon en práctica este consejo!

- Es muy importante **mantenerse al tanto de las actualizaciones** que vayan publicando los fabricantes del software instalado en tu empresa. Por ejemplo, Microsoft las reúne en su página **Windows Update**.
- Activa las “Actualizaciones Automáticas” de tu sistema operativo. Por ejemplo, Windows suele tener esta opción en el Panel de Control (accesible desde el botón de Inicio).
- **Instala el “parche” en un entorno restringido**, antes de extenderlo a toda la red. Así evitarás posibles colisiones y problemas con otras aplicaciones.

05. Haz copias de seguridad con frecuencia

Es muy recomendable realizar copias de seguridad de tu información. Es una precaución básica, que te puede salvar en caso de cualquier "catástrofe" informática, aunque muy poca gente las hace de forma sistemática.

¡Pon en práctica este consejo!

• **Elige bien el soporte** (CDs, DVDs, discos externos...) en el que vas a guardar las copias y **protégelas físicamente**, junto con los discos de arranque, en armarios independientes e ignífugos. También es una buena medida tener una copia fuera de tus instalaciones.

• Realiza las copias **con la mayor frecuencia posible**. Te recomendamos hacerlo de forma mensual y copias incrementales cada semana.

• Si tienes mucho volumen de información, quizás te interese **seleccionar la más importante**, para hacer más ágiles las copias periódicas.

06. Bloquea las entradas no autorizadas a tu red

Las conexiones ADSL son una puerta abierta para los hackers. A través de los puertos de comunicación de tus ordenadores te pueden robar información confidencial o incluso utilizar tus sistemas como plataforma para realizar ataques a otros equipos.

¡Pon en práctica este consejo!

• **Instala un firewall** en tu red, eligiendo el más adaptado a tus necesidades. Puede ser una funcionalidad integrada en el propio software de tu solución de seguridad, un servidor dedicado o un appliance de última generación.

• **Fíjate muy bien en los mensajes que te envía el firewall**: cuando te pregunte si puede dejar acceder a Internet a una determinada aplicación, dile que sí sólo en aquellos casos que sepas bien de qué se trata.

07. No satures tus equipos con información y programas innecesarios

Saturar los ordenadores con todo tipo de programas y aplicaciones reduce drásticamente su rendimiento. Además, muchas veces supone un peligro para la seguridad (el carácter gratuito de algunas herramientas es una artimaña muy habitual para introducir malware y software ilícito en los equipos).

¡Pon en práctica este consejo!

- **Supervisa bien todo lo que se instala en tu red**, permitiendo sólo las aplicaciones y programas realmente necesarios. Un ejemplo son los programas P2P (Kazaa, eMule...) o de mensajería instantánea (Messenger, Skype...), que suelen ser una de las principales entradas de amenazas informáticas.
- Establece **niveles de seguridad medio-altos** en los navegadores.
- Evita descargas desde **sitios poco fiables**.
- No aceptes **contratos de licencia de software gratuito** si no tienes claro lo que implican.
- Además, para optimizar el rendimiento:
  - **Defragmenta tus ordenadores al menos una vez al mes** (en Windows, la utilidad suele estar en Inicio / Todos los programas / Herramientas del sistema). Asegúrate de dejar siempre libre al menos un 40% de disco duro, ya que a partir de ese porcentaje el rendimiento de los equipos desciende en picado.
  - **Deja en estado residente sólo a los programas realmente imprescindibles**, como el antivirus. ¿Cómo hacerlo? Generalmente, todos los programas que aparecen con un icono en el extremo inferior derecho de tu barra de programas están configurados como residentes. Para desactivarlos, pulsa sobre ellos con el botón derecho del ratón y selecciona la opción correspondiente.

08. Realiza análisis exhaustivos de forma periódica

Para detectar los virus y cualquier otro tipo de malware oculto en tus ordenadores, hay que realizar análisis en profundidad con frecuencia.

Esta medida es una precaución adicional, aunque tengas activada la protección automática de tu solución de seguridad.

¡Pon en práctica este consejo!

- Como suelen llevar mucho tiempo, programa los análisis exhaustivos para que se realicen **fuera del horario laboral**. Así no interferirás en la actividad normal de tus equipos.
- Recuerda que los antivirus y demás soluciones de seguridad suelen tener activada por defecto la protección automática, pero los análisis exhaustivos normalmente **hay que lanzarlos de forma manual**.

09. Ten mucho cuidado con las conexiones WIFI

Saturar los ordenadores con todo tipo de programas y aplicaciones reduce drásticamente su rendimiento. Además, muchas veces supone un peligro para la seguridad (el carácter gratuito de algunas herramientas es una artimaña muy habitual para introducir malware y software ilícito en los equipos).

¡Pon en práctica este consejo!

• Emplea **claves de acceso** a tu conexión WiFi y a toda tu información confidencial. Cuando instales un nuevo router WiFi, no te olvides de **cambiar las contraseñas** que vienen de fábrica (suelen ser conocidas por los hackers).

• Utiliza, siempre que puedas, el **protocolo de cifrado WPA**.

• Comparte tus carpetas, ficheros o dispositivos sólo cuando sea r**ealmente necesario**.

• Si tienes la posibilidad, **desactiva el broadcasting** (envío público) de SSID, para evitar la publicación del nombre de tu red.

10. Establece una política de seguridad global para tu empresa

Buena parte de los problemas y fallos de seguridad se deben a errores humanos. Para evitarlo, hay que establecer unas pautas de actuación básicas y recogerlas en una política de seguridad unificada, involucrando en su cumplimiento a todo el personal de la empresa.

Por ejemplo, una buena práctica para empezar es enviar esta animación a tus empleados.

¡Pon en práctica este consejo!

• Define **perfiles en función del cargo de cada persona** y de su actividad concreta, permitiendo utilizar solamente las herramientas que requiera para su puesto. Para facilitarte esta tarea, hay soluciones de seguridad que te permiten definir los perfiles de forma centralizada, como Panda AdminSecure.

• Por regla general, **los usuarios de tu red no deben tener permisos para instalar** libremente el software que quieran. Esta función debe estar restringida al administrador de la red.

• Pon **especial atención a las vías más habituales de entrada de malware**:

- Los **dispositivos de almacenamiento** como CDs, DVDs y USBs pueden servir para introducir documentos infectados y además, pueden ser la vía de escape de información confidencial.

- Las visitas incontroladas a **páginas web** suelen suponer una notable reducción del rendimiento laboral.

- El **correo basura (spam)** también interrumpe el ritmo de trabajo. Además, los archivos adjuntos en los e-mails pueden ser peligrosos.

• **Documenta por escrito**, de una forma clara y comprensible, todos los aspectos relacionados con la política de seguridad de tu empresa. Así no se perderá la información.

• Si necesitas ayuda, contrata a una **empresa o asesor especializado en seguridad** corporativa.

GLOSARIO

ADSL (Asymmetric Digital Subscriber Line): Se trata de un tipo de conexión a Internet que se caracteriza por su elevada velocidad

Appliance de seguridad: Dispositivo que une hardware y software y que instalado en la conexión entre la red de la empresa e Internet proporciona una protección unificada contra todo tipo de amenazas.

Broadcasting (desactivación de): Es uno de los métodos más básicos de proteger una red inalámbrica y consiste en desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso.

Firewall: Su traducción literal es muro de fuego, también conocido a nivel técnico como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

Gusano: Es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él.

Hacker: Persona que accede a un ordenador de forma no autorizada e ilegal.

Malware (MALicious softWARE): Cualquier programa, documento o mensaje susceptible de causar perjuicios a los usuarios de sistemas informáticos.

Memoria USB (Universal Serial Bus) o Pendrive: Pequeño dispositivo de almacenamiento portátil, con un formato generalmente similar a un lápiz óptico o a un llavero. Estas memorias son más resistentes a los rasguños y al polvo que otras formas de almacenamiento, como los CDs y los disquetes, además de ser más fácilmente "portables".

Mensajería instantánea: La mensajería instantánea (conocida también en inglés como IM) sirve para enviarse mensajes a través de Internet y se caracteriza porque permite mantener conversaciones en tiempo real (los más conocidos son el Messenger de Microsoft y Skype).

Parche de seguridad: Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades o defectos de funcionamiento.

Phishing: Acrónimo para Password Harvesting Fishing (Pesca y Recolección de Contraseñas). Es un tipo de ataque de ingeniería social, en el que alguien se hace pasar por una fuente confiable y engaña al usuario para que desvele información privada (contraseñas, número de tarjeta de crédito, etc.), que será empleada con fines fraudulentos (por ejemplo, suplantación de identidad).

Programas P2P: Programas empleados para prestar servicios a través de Internet (generalmente intercambio de ficheros), que los virus y otros tipos de amenazas utilizan para distribuirse. Algunos ejemplos de estos programas son KaZaA, Emule o eDonkey.

Protección automática: Se trata de un análisis continuo que algunos antivirus realizan sobre todos los ficheros que intervienen en cualquier tipo de operación (realizada por el usuario o por el propio sistema operativo). También es conocido como centinela o residente.

Puerto de comunicación: Punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información del ordenador con el exterior y viceversa.

Residente: Cuando se instalan, muchos programas se quedan en estado residente (o sea, que se inician automáticamente al encender el ordenador y están siempre funcionando, lo que afecta también al rendimiento de los equipos).

Robo de identidad: Robo de los datos personales que identifican a una persona (números de cuentas bancarias, números de seguridad social, claves y contraseñas de acceso, etc.), generalmente para suplantar su identidad con fines fraudulentos.

Router: Un router (en español enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes, para pasar paquetes de datos de una a otra.

Spyware: Programa que recopila datos sobre los hábitos de navegación, preferencias y gustos del usuario, generalmente sin su consentimiento. Esta información es usada luego con diversos fines y suele tener consecuencias muy molestas, como la aparición de continuos pop ups publicitarios.

SSID (Service Set IDentifier): Código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Tecnologías preventivas / protección preventiva: Capacidad de proteger un ordenador de malware desconocido analizando el comportamiento de los programas, sin necesidad de disponer de un archivo de identificadores de virus que deba ser actualizado periódicamente.

Troyano: Se trata de un programa que llega al ordenador de manera encubierta (aparentando ser inofensivo), se instala y realiza determinadas acciones que suelen afectar a la confidencialidad del usuario atacado, además de otros efectos nocivos, como destrucción de información, etc.

Virus: Los virus son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, infectando otros archivos y produciendo efectos molestos, nocivos e incluso irreparables.

Vulnerabilidades: Fallos o huecos de seguridad detectados en algún programa o sistema informático, que los virus utilizan para propagarse e infectar.

WPA (Wi-Fi Protected Access - Acceso Protegido Wi-Fi): Es un sistema para proteger las redes inalámbricas (Wi-Fi), creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy).

Wi-Fi: Es la más conocida tecnología de transmisión inalámbrica de información. También es una marca de la Wi-Fi Alliance, la organización comercial que prueba y certifica que los equipos cumplen los estándares IEEE 802.11x.