

La actividad cotidiana entraña una serie de riesgos que asumimos y contrarrestamos con normalidad. La tecnología, sin embargo, ha invadido nuestras vidas a gran velocidad, lo que nos ha dejado expuestos e indefensos ante los problemas de seguridad que comporta. Al igual que se cierra con llave la puerta de casa cuando salimos, el ordenador debe estar acondicionado para proteger su integridad y los datos personales que alberga. Si está conectado a Internet, esta necesidad se acentúa. Pero no hay motivo para ser alarmistas. **Los peligros de la conexión a la Red tienen que ver sólo con la seguridad de la información, y tomando las debidas precauciones el improbable ataque de un intruso o la más factible infección de un virus pueden ser evitados.** Y no hay que esperar a que aparezca un contratiempo para ser conscientes de la amenaza y actuar.

La principal causa de los problemas de seguridad, por encima de los fallos del equipo o de sus programas, es la falta de información y formación de

los usuarios. Éstos, a los que se premia a conectarse a la Red y formar parte de la Sociedad de la Información, se encuentran a la postre con que la responsabilidad de la seguridad de su equipo recae íntegramente sobre sus hombros.

La primera línea de defensa

Las barreras de protección -que no se pueden dejar de levantar- limitan los peligros de las herramientas más utilizadas de Internet. Actualmente son los virus que llegan por correo electrónico el peligro más importante. Protegerse contra ellos y evitar su propagación es un deber del internauta.

El usuario sólo necesita un par de armas para estar vacunado contra la gran variedad de 'bichos' —virus, gusanos, troyanos...— que pululan por la Red: **un antivirus actualizado y un poco de cibereducación.** Para lo primero basta una pequeña inversión económica o utilizar periódicamente las herramientas gratuitas *online* de los fabricantes (como la de www.virus-portal.com); para lo segundo, un poco

de información resumida en dos reglas básicas: **recelar de los mensajes de personas desconocidas y, sobre todo, jamás abrir un archivo adjunto que no sea de entera confianza.**

El email también está relacionado con otra de las grandes plagas de la Red: los mensajes publicitarios no deseados o *spam*. Aquí la formación deviene esencial, ya que las herramientas *antispam* no son del todo eficaces (o dejan pasar demasiada 'basura', o se llevan por delante emails amigos). **El internauta avezado sabe que para mantener limpio su buzón debe cuidar a quién da su dirección electrónica, nunca firma con su dirección auténtica en foros o grupos de noticias, y en ningún caso reenvía mensajes en cadena o avisos de virus sin contrastar.** Conviene hacerse con una dirección gratuita (como las de Yahoo.es o Mixmail.com) para usarla con quien no tengamos confianza (registros de webs, por ejemplo) y reservar el buzón principal para dársela a los remitentes más allegados y/o seguros.

Proteger el PC

Al ordenador hay que ponerle un candado, igual que a la verja del jardín



>>> **Navegar a la carta**

Campañas de seguridad
 ↗ www.seguridadenlared.org

La Asociación de Internautas (AI) ha promovido cuatro campañas para limpiar los PCs de virus, evitar intrusiones, preservar la intimidad y formar e informar a los internautas sobre el uso de las herramientas de seguridad.

Laboratorio
 ↗ www.hispasec.com

HispaSec Sistemas mantiene desde 1998 "*una-al-día*", un servicio diario de información técnica sobre seguridad informática muy útil para conocer las nuevas amenazas y saber cómo hacerles frente.

A medida que el usuario va estrechando su relación con la Red, también debe ir aumentando el nivel de seguridad. Así, **al contratar una conexión de alta velocidad ADSL, la primera línea de defensa debe ser un firewall (cortafuegos)**. Programas como ZoneAlarm (www.zone-labs.com), que pueden descargarse gratis en su versión básica, controlan la conexión a Internet, avisando si algún programa intenta enviar información a la Red o si alguien trata de acceder al ordenador desde fuera.

Extraños en el disco duro

La amenaza a la integridad del equipo presenta varios frentes, además del correo electrónico, ya que también puede llegar a través de la mensajería instantánea, la descarga de programas, por medio de los sistemas de intercambio de archivos o, simplemente, al navegar.

Hay sitios web capaces de cambiar la página de inicio del navegador, añadir nuevos favoritos o instalar barras de navegación sin el permiso del usuario.

UN ATAQUE INFORMÁTICO SÓLO HARÁ PERDER DATOS, NUNCA ESTROPEARÁ FÍSICAMENTE EL EQUIPO

Y, más perniciosas, aquellas que modifican la conexión a Internet rediriéndola a un número 906 disparando la factura telefónica.

Para este último problema, uno de los fraudes más denunciados en Internet, conviene controlar que el programa de conexión (el de "Acceso telefónico a redes") no marque un número que empieza por 906.

También hay que tener cuidado con cierto tipo de programas, normalmente los de uso limitado (*shareware*) descargado de la Red. Al instalarlo, el PC puede quedar 'infectado' por programas desconocidos a no ser que el usuario, en el mejor de los casos, lea la letra pequeña durante la instalación. Se trata de sistemas que bombardean con publicidad intrusiva o de aplicaciones espía (*spyware*), utilizadas para enviar información sobre los movimientos del

internauta. Conviene usar de forma regular unos programas gratuitos que contrarrestan sus efectos dañinos; uno de los más efectivos es Ad-aware de Lavasoft (www.lavasoft.com).

PC a la última

Es raro el programa que no precisa de una actualización al poco de ser comercializado. El usuario debe visitar cada cierto tiempo la página web del fabricante para estar al tanto de las actualizaciones para su equipo, muchas de las cuales son un compendio de parches de seguridad que tapan los agujeros de los programas imperfectos. Microsoft cuenta con una página (<http://v4.windowsupdate.microsoft.com/es/>) que no deben perder de vista los usuarios de este sistema operativo si no quieren que su equipo acabe siendo un colador para toda clase de peligros. ◀

LOS ENEMIGOS

La principal amenaza que se cierne sobre el PC conectado a Internet es el 'código malicioso' (*malware*), que se conoce genéricamente como virus aunque abarca varios tipos que, si bien son diferentes entre sí, se pueden combinar para causar mayor daño.

→ Los **virus** son pequeños programas informáticos que se ocultan en el sistema y son capaces de multiplicarse mediante la infección de otros programas mayores. Se introducen subrepticamente en el sistema de diversas formas y pueden ocasionar simples molestias o

daños irreparables en la información.

- Los **gusanos**, en cambio, no necesitan infectar otros archivos para multiplicarse, pues se limitan a realizar copias de sí mismos. Los más comunes llegan a través de archivos adjuntos en el email y al ejecutarlos se reenvían a todos los contactos de la libreta de direcciones.
- Los caballos de Troya o **troyanos** se instalan en el ordenador y realizan acciones que permiten a un intruso tomar el control del ordenador desde un lugar remoto. Son los más peligrosos.

Pioneros

➤ www.kriptopolis.com

Desde 1996, esta revista online comenzó a cubrir la carencia de información especializada en español sobre programas de cifrado, campo que ha ido ampliando hacia la seguridad en general.