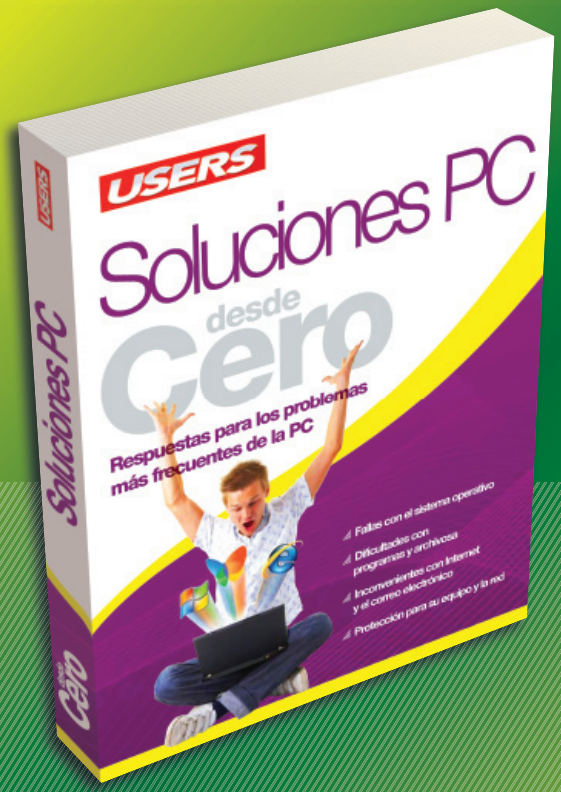
USERS

Seguridad PC desde Cero

Proteja su PC contra todas las amenazas de la Web

- Consejos para lograr un equipo blindado
- Evite intrusiones de hackers y espías
- Configuración de una red Wi-Fi segura
- Defensa contra todas las amenazas: virus, troyanos, gusanos, spam y publicidad invasiva ¡y mucho más…!

SU PC NUNCA MÁS VOLVERÁ A TOMARLO DESPREVENIDO



En esta obra encontraremos un material sin desperdicios que nos permitirá entender los síntomas que presentan los problemas graves, solucionarlos en caso de que algún imprevisto nos sorprenda y, finalmente, evitar que se repitan.

» HOME / MICROSOFT
» 192 PÁGINAS
» ISBN 978-987-663-028-3

SOBRE LA COLECCIÓN desde Cero

» Aprendizaje práctico, divertido, rápido y sencillo.
» Lenguaje simple y llano para una comprensión garantizada.
» Consejos de los expertos para evitar problemas comunes.
» Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS

Seguridad PC desde Cero

Proteja su PC contra todas las amenazas de la Web

TÍTULO: Seguridad PC
AUTOR: Alexis Burgos
COLECCIÓN: desde Cero
FORMATO: 15 X 19 cm
PÁGINAS: 192

ISBN 978-987-663-031-3

Burgos, Alexis
Seguridad PC. - 1a ed. - Banfield - Lomas de Zamora: Gradi; Buenos Aires: Fox Andina, 2010.
192 p. ; 19x15 cm. - (Desde cero; 7)
ISBN 978-987-663-031-3

1. Informática. I. Título
CDD 005.3

RedUSERS.com

Prólogo **al contenido**

El universo de la comunicación y sus tecnologías atraviesa grandes cambios todos los días. Estas últimas se trasformaron en una herramienta esencial en el proceso, veloz y global, de la difusión y distribución de los datos, la información y las noticias. ¿Quién puede imaginar hoy el trabajo cotidiano sin una computadora?

La velocidad del desarrollo informático fue otro de los factores que dio lugar al contacto instantáneo de los acontecimientos en cualquier lugar del planeta. Nunca estuvo tan cercana la idea de "aldea global" como lo está hoy, como se vive e, incluso, como se sufre. Pero también, enquistado en la vorágine de los adelantos revolucionarios, llegan los inconvenientes informáticos que acarrean grandes desilusiones y dificultades en el avance periódico de las tareas.

Gracias a los especialistas, los progresos en materia informática son más seguros y menos violables. Esto nos da tranquilidad a la hora de trabajar, comunicarnos y hasta entretenernos con las computadoras y con el intercambio constante que otorga esa herramienta colectiva llamada Internet. El uso constante de la red, tanto para trabajar como para los momentos de ocio, acarrea la permanente amenaza de abrir paso a que nuestra computadora sea un festival de gérmenes ávidos de conquistar carpetas, archivos y todo tipo de documentos que se encuentren guardados.

Para los neófitos, la aparición de virus informáticos y las incompatibilidades entre programas y aplicaciones ha sido la peor pesadilla. Se pierden datos, se esfuma información importante para desarrollar trabajos, se borran notas y entramos en un estado de alarma ante la imposibilidad de resolver estos inconvenientes.

Por eso, no sólo es adecuado conocer la existencia de un antivirus, sino que además, es imprescindible saber el mecanismo y la forma de instalación, ejecución y vigencia de éste y de otros antídotos que van a velar por la permanente tranquilidad del usuario y su equipo. De ahí la importancia de firewalls, antispyware, filtros de todo tipo y políticas de seguridad de red.

La humanidad siempre encontró obstáculos que superar, y los avances tecnológicos no quedaron exentos de ellos. Pero el tiempo y el perfeccionamiento de los sistemas de protección ayudaron a solucionar algunos problemas. Con las aplicaciones adecuadas y la ayuda de este libro, estaremos, cuanto menos, a salvo.

El libro **de un vistazo**

Este libro está orientado a usuarios básicos e intermedios del sistema operativo Windows que pretendan mejorar su nivel de seguridad digital en la computadora, y la red del hogar y de la pequeña oficina. Paso a paso, el volumen explicará cómo configurar cada elemento de seguridad, desde el antivirus hasta el router Wi-Fi, para minimizar la posibilidad de un ataque.

CAPÍTULO 1
INTRODUCCIÓN

En este primer capítulo empezaremos a conocer, en líneas generales, las principales herramientas con las que contamos para defendernos de las grandes amenazas del mundo informático moderno. Además, analizaremos rápidamente las características de esas amenazas y ajustaremos la configuración básica del sistema operativo.

CAPÍTULO 2
PRIMER PASO: INSTALAR UN ANTIVIRUS

La primera herramienta de seguridad por configurar, aun antes de conectarnos a Internet, es el antivirus. En este capítulo aprenderemos a utilizar el programa AVG Free Edition AntiVirus. Y no solo lograremos utilizarlo a la perfección, sino que además ajustaremos su configuración para no dejar ningún punto librado al azar.

CAPÍTULO 3
SEGUNDO PASO: PROTECCIÓN CONTRA ADWARE, SPYWARE Y MALWARE

Una vez instalado el antivirus, necesitamos una suite antispyware a la altura de las circunstancias. En este capítulo aprenderemos todo sobre Spybot Search & Destroy, el mejor de su género. Además, conoceremos las herramientas extras que nos ofrece el programa para aumentar la protección activa del sistema.

CAPÍTULO 4
TERCER PASO: BLINDAR EL EQUIPO

Ni antivirus ni antispyware son herramientas suficientes para conectar un equipo a Internet sin correr el riesgo de que éste se infecte de manera automática. Es imprescindible contar con un firewall que filtre los paquetes de datos entrantes y salientes. En este capítulo, analizamos todo sobre el Firewall de Windows incluido en Vista.

CAPÍTULO 5
CUARTO PASO: CONFIGURACIÓN SEGURA DE LA RED WI-FI

Las redes sin cables son cada vez más fáciles de encontrar en hogares y pequeñas oficinas.

Sin embargo, son aún muchos los usuarios que compran un router y lo conectan sin antes configurar correctamente el apartado de seguridad. Aquí aprenderemos a hacer de nuestro router uno de los más importantes componentes de defensa de la red.

CAPÍTULO 6
QUINTO PASO: ESTABLECER POLÍTICAS DE SEGURIDAD Y PRIVACIDAD EN LA RED LOCAL

Luego de asegurarnos de contar con una red local cableada y Wi-Fi segura, debemos ocuparnos de establecer políticas de red coherentes y eficientes para evitar poner en riesgo los datos que circulan por la LAN. Aprenderemos en este apartado a sacar el máximo provecho del Centro de redes y recursos compartidos de Vista, y sus herramientas.

CAPÍTULO 7
SEXTO PASO: NAVEGAR DE FORMA SEGURA

Son muchos los casos en los cuales el principal motivo de una infección reside, ni más ni menos, que en el usuario. Por eso, debemos aprender cuáles son las prácticas más seguras en lo que a navegación respecta y cuáles podrían, definitivamente, dejarnos al descubierto. Aprenderemos además a crear contraseñas seguras y a administrarlas.

APÉNDICE A
SPAM

Ningún libro sobre seguridad hogareña puede dejar de lado una de las más molestas y constantes amenazas que sufren los usuarios: el spam. Para lograr este objetivo, aprenderemos a utilizar y a configurar SPAMFighter.

APÉNDICE B
PROGRAMAS ALTERNATIVOS

A lo largo del libro, se detalla una lista de aplicaciones que colaboran con el usuario en lo que se refiere a proteger la seguridad de su equipo. En este apéndice, analizaremos las mejores herramientas alternativas, para tener una opción a los productos de seguridad detallados en los capítulos anteriores.

SERVICIOS
AL LECTOR

En este último apartado del manual, encontraremos un índice temático con los conceptos que explica el libro. Nos ayudará a encontrar los términos más significativos de esta obra y nos permitirá un fácil acceso a ellos, dentro de ésta.

Contenido **del libro**

CAPÍTULO 7
SEXTO PASO: NAVEGAR DE FORMA SEGURA 139

APÉNDICE A
SPAM 155

APÉNDICE B
PROGRAMAS ALTERNATIVOS 173

SERVICIOS AL LECTOR 185

Introducción **a Seguridad PC**

En la actualidad, y a diferencia de lo que pasaba hace unos años, los niveles de protección de una computadora deben ser altísimos para que un equipo pueda considerarse realmente seguro. Lejos quedaron los tiempos en los que un antivirus con un archivo de definiciones de dos o tres de semanas de antigüedad era suficiente; hoy un antivirus actualizado de manera constante, de ninguna forma alcanza, para estar bien protegidos. De hecho, ni siquiera un buen antivirus y un firewall resultan una dupla certera: son muchas más las herramientas que en conjunto nos permitirán, si logramos configurarlas en forma correcta, sentirnos del todo seguros.

Necesitaremos, además de los componentes que ya nombramos, un buen antispyware que nos proteja de los infinitos malware que merodean Internet. Un router con firewall por hardware, que asegure nuestra red Wi-Fi, ya que éste es un componente que, de contar con una mala configuración, puede suponer un agujero de seguridad enorme. Una red local con una configuración de seguridad correcta que nos permita intercambiar archivos y, a la vez, asegurar nuestros documentos privados. Un gestor de archivos encriptados que esconda de los fisgones los datos confidenciales. Los conocimientos suficientes para navegar sin que nosotros mismos pongamos en peligro un sistema seguro y, también, probablemente, un antispam para lidiar con esta molesta amenaza.

En este libro aprenderemos, paso a paso, cómo utilizar todos y cada uno de estos elementos para convertir con ellos a nuestro equipo en el más seguro de la Intranet. Estudiaremos, al menos, dos aplicaciones de cada tipo para poder elegir cuál se adecua más a nuestras necesidades, así como también conoceremos terceras opciones para investigar.

En épocas donde la seguridad se presenta como un tema central, este libro pretende traer un poco de tranquilidad para poder pensar mejor, y dedicarnos a disfrutar de una vida digital plena y sin sobresaltos. ¡Bienvenidos!

Capítulo 1
Introducción

Tendremos el primer contacto
con los principales programas
que utilizaremos a lo largo del libro.

Al adquirir una computadora para nuestro hogar, además de preocuparnos por contar con el mejor hardware y de que el sistema operativo corra sin problemas, es fundamental protegerla de las amenazas informáticas. Para esto, debemos encargarnos de que nuestra estadía en Internet o en una red sea del todo segura. A partir de este capítulo, comenzaremos a aprender cómo convertir una computadora en una verdadera fortaleza digital. Para empezar, tendremos el primer contacto con los principales programas que utilizaremos a lo largo del libro y analizaremos las amenazas que pueden vulnerarlo.

Hacia un equipo **seguro**

Aunque con el tiempo los sistemas operativos se volvieron cada vez más seguros y menos vulnerables a los ataques de todo tipo, aún es imprescindible establecer políticas de seguridad que exceden ampliamente aquellas que equipan a Windows. ¿Por qué? Porque la cantidad de amenazas a las que se ve expuesta una computadora con conexión a Internet **son tantas y de tan variados tipos** que una sola aplicación no es suficiente para combatirlas (**Figura 1**).

El **antivirus**

El programa llamado **Elk Corner** tiene el honor de ser sindicado como el primer virus esparcido entre computadoras fuera de un laboratorio. Fue creado en 1982 por el norteamericano **Richard Skrenta** y atacaba a los equipos que utilizaban el sistema operativo **Apple II**. Se transmitía, mediante la copia y la reproducción de discos removibles o disquetes.

Un **virus** es un programa que puede reproducirse en forma automática haciendo copias de sí mismo. Su objetivo consiste en infectar la mayor cantidad posible de computadoras, distribuyéndose por redes o siendo transportado por los usuarios en medios de almacenamiento removibles o en e-mails (**Figura 2**).

LA PRIMERA VEZ QUE SE USÓ LA PALABRA VIRUS

En la novela de **David Gerrold**, **Cuando H.A.R.L.I.E. era una** *(When HARLIE Was One)*, se habla por primera vez de un programa de computadora denominado **Virus**, que actuaba de manera parecida a lo que ahora llamamos de la misma forma.

FIGURA 1. En el mundo web, un cliente (usuario con un navegador) y un servidor se relacionan mutuamente, utilizando el protocolo TCP/IP.

FIGURA 2.
La computadora Apple II fue el primer equipo cuyo sistema operativo se vio amenazado por un virus.
No contaba con firewalls, antivirus ni conexión a Internet.

El universo PC tuvo que esperar hasta **1986** para considerar las infecciones de virus como un riesgo importante. En ese año, dos hermanos programadores paquistaníes crearon el virus **Brain** para luchar con los actos de piratería contra el software que ellos mismos creaban.

HACKER

El **hacker** es un experto informático cuyo accionar aparece asociado al vandalismo. Muchos les temen, aunque los hackers no necesariamente son malvados. La etimología de la palabra, según el gurú informático **Richard Stallman**, se refiere a divertirse con el ingenio.

Infectaban copias pirata de sus productos para que circularan y se distribuyeran en las computadoras de los usuarios que no querían pagar por sus programas (**Figura 3**).

Con la llegada de los **BBS** (*Bulletin Board System*), y el comienzo de Internet a fines de los años ochenta y principios de los noventa, los virus se expandieron impensadamente, y el soporte preferido dejó de ser el medio removible para comenzar a ser la red de redes. Al mismo tiempo, surgieron los macro virus, virus creados en lenguajes menores y orientados a infectar, en especial, documentos de **Microsoft Office**.

Los virus son creados de manera deliberada por programadores humanos que ganan dinero a cambio de su producción. Algunas de esas creaciones (aquellas conocidas como **virus polimórficos**) pueden variar en su forma, aunque no es el fin de los virus

FIGURA 3. Richard Skrenta, creador del primer virus de la historia, tiene un website que podemos visitar en www.skrenta.com.

informáticos cambiar de estado o crear nuevas variantes de ellos mismos más que para escapar de los antivirus (**Figura 4**).

Además de las económicas, son muchas las razones por las cuales se crean los virus. Algunas veces, su aparición tiene que ver con investigaciones de laboratorio. Otras, resultan ser los llamados **hackers** los que los hacen para probar la vulnerabilidad de un sistema de seguridad. También los usan para expresar su descontento frente a las políticas comerciales de una empresa o las actitudes de un país u organización frente a un conflicto.

SEGURIDAD EN REDES WIFI

Cualquier red inalámbrica correctamente configurada y con sus opciones de seguridad activadas es tan segura o más que una red sin cables. Por ello, cualquier preocupación sobre intrusiones resulta innecesaria si la instalación y la configuración fue hecha a conciencia.

FIGURA 4.
Los interesados en estudiar la estructura informática de los virus pueden visitar www.hackpalace.com/virii/indexe.shtml, un sitio que guarda varios de ellos con fines estrictamente educativos.

Otras veces, quizás las menos, son puestos en marcha con fines de entretenimiento o por puro vandalismo. Incluso, algunos programadores de virus consideran sus creaciones como obras de arte.

Hace mucho tiempo, en las épocas de **DOS** y **Windows 3.1**, un antivirus residente actualizado (e incluso, en algunos casos, uno que nos permitiese escanear cada semana el equipo) era más que suficiente para que un usuario promedio sintiera que contaba con un equipo seguro. Y cabe aclarar que, en aquellos tiempos, el concepto **actualizado** significaba comprado en un negocio de venta de software en la última semana, lo que aseguraba que el archivo de definición de virus no tuviera más de dos meses de antigüedad.

Lejos de aquella situación, hoy en día, un antivirus residente que se actualiza en forma constante es, apenas, un componente del sistema de seguridad integral de una computadora.

De ese antivirus, además esperamos que controle, de manera automática, la presencia de **elementos maliciosos** en las unidades extraíbles que conectamos al equipo (pendrives, discos ópticos, disquetes y cualquier tarjeta de memoria) y en los **adjuntos** de correo electrónico. Algunos productos nos ofrecen, además, protección en sesiones de **mensajería instantánea** y hasta controlan que los **vínculos** que nos devuelva el buscador no nos lleven a sitios con contenidos potencialmente peligrosos o infectados con virus de cualquier tipo.

CENTROS DE DESCARGAS

En el sitio de descarga de archivos **Download** (**www.download.com**), de la red **Cnet**, podemos conseguir software gratuito para proteger nuestro equipo. Si lo que buscamos es software libre, el sitio recomendable es **SourceForge** (**http://web.sourceforge.com**).

AVG AntiVirus Free Edition (**Figura 5**) es una de las mejores opciones gratuitas del mercado. Esta aplicación cubre todas las expectativas posibles, con la ventaja de que resulta muy fácil de instalar, utilizar y configurar. Se puede descargar desde **http://free.avg.com**. Aprenderemos todo sobre él en el **capítulo 2**. También existen otras opciones como **Kaspersky Antivirus**, actualizado para ofrecer soporte a Windows 7.

FIGURA 5. AVG ofrece también una solución paga de antivirus. Con la versión gratuita y los consejos de este libro, estaremos protegidos.

Las ventajas del firewall

En la actualidad, el concepto de virus por sí solo resulta un tanto obsoleto. Como ya hemos dicho, hoy por hoy, las amenazas son muchísimas, y los virus o códigos maliciosos constituyen solo algunas de ellas. Por lo tanto, la tarea del antivirus, así como lo hemos adelantado, resulta insuficiente para establecer una política de protección global eficiente, en un equipo.

Por estas razones, resulta necesario instalar un **firewall**, cuyo funcionamiento veremos en detalle en el **capítulo 4**. Este elemento es el gran aliado de seguridad del antivirus desde hace ya unos años. El firewall (también llamado en castellano **cortafuegos**) establece una barrera entre el equipo e Internet, que impide que exista un tráfico de datos desde nuestro equipo y hacia él, si el usuario no lo ha pedido explícitamente (**Figura 6**).

De este modo, ninguna amenaza que viaje por la red local o por Internet logrará tomar el equipo, aunque tampoco podrán acceder a la computadora algunas aplicaciones deseables, como los clientes de redes **P2P** del estilo de **Ares** o **eMule**, a menos que el usuario los habilite.

La importancia de un firewall es tal que, sin tener esta aplicación activada, la computadora estaría tan amenazada que, quizás, luego de unos minutos de funcionamiento, se encontraría repleta de publicidades no deseadas, e infectada por varios programas maliciosos (**Figura 7**).

FIGURA 6.
COMODO Firewall **es una excelente alternativa al firewall de Windows Vista.**

FIGURA 7.
Después del virus Blaster, a los usuarios les quedó clara la importancia de contar con un firewall.

LA EXPERIENCIA BLASTER

Cuando **Windows XP RTM** era el estándar del mercado, un peligrosísimo virus causó estragos en la comunidad informática internacional: el **Blaster**, que aprovechaba un problema de seguridad de Windows para tomar el control del equipo y apagarlo.

Windows Vista incorpora un firewall muy efectivo y fácil de usar que asegura un nivel coherente de seguridad en la red local (**Figura 8**). Además, nos evita realizar molestas configuraciones e invertir en software de terceros. Los firewalls funcionan sobre la base de reglas. Las **reglas** son configuraciones que habilitan o no el tráfico entrante o saliente a través de la red. Vamos a estudiar con profundidad el funcionamiento del firewall y la creación de reglas en el **capítulo 4**.

A través del uso de reglas, podremos **proteger el equipo**, en tanto limitaremos el acceso de aplicaciones no autorizadas así como evitaremos, también, que la información saliente ponga en riesgo nuestra privacidad y haga circular datos que no nos interesa compartir con otros usuarios.

Las reglas bien configuradas nos permitirán, además, controlar los tiempos, horarios y aplicaciones que los usuarios utilicen en la red (**Figura 9**).

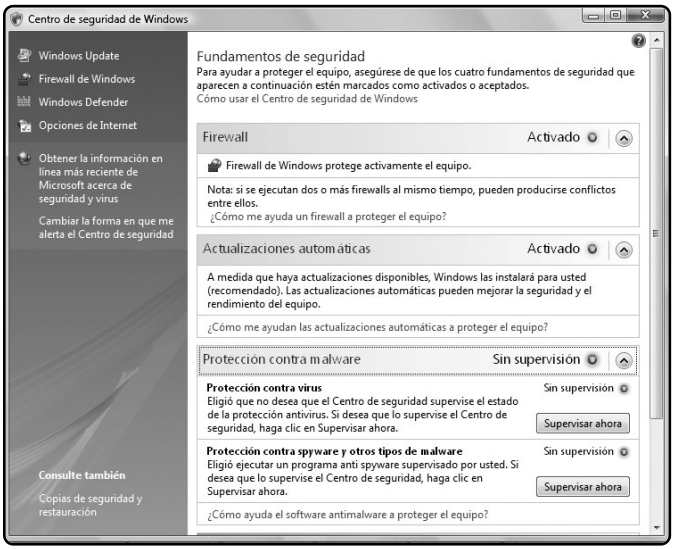


FIGURA 8.
Windows Vista, a pesar de las críticas que recibió, mejoró mucho en lo que a seguridad se refiere.

SOLUCIONES INTEGRALES

Algunas empresas, como **Symantec** con su **Norton 360** o **Comodo** con su **Internet Security**, ofrecen soluciones integrales de seguridad con paquetes que incluyen antivirus, firewalls y antispyware en una misma aplicación.

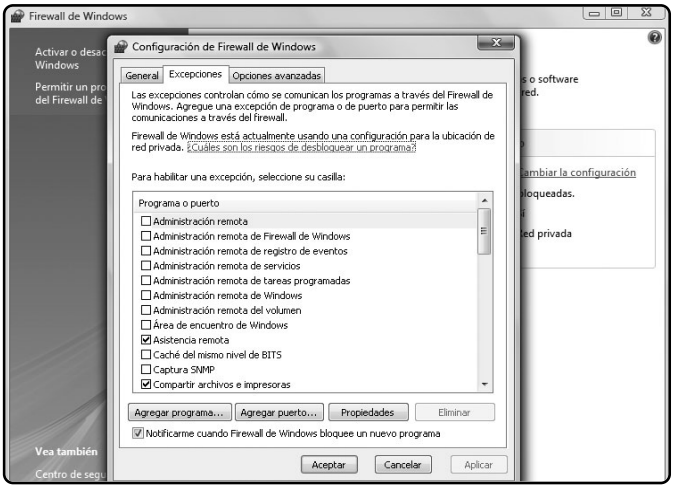
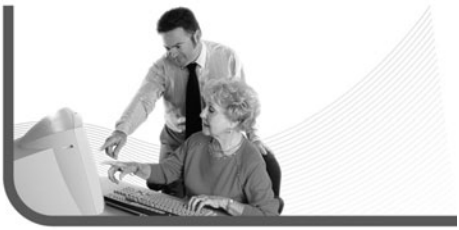


FIGURA 9.
En la solapa `Excepciones`**, de la ventana** `Configuración de Firewall de Windows`**, podemos ver qué aplicaciones están habilitadas para trabajar con la red y cuáles no. Se agregan o se quitan programas tildando las cajas correspondientes.**

En versiones anteriores del sistema operativo de Microsoft, el **Centro de seguridad** reunía opciones tales como la administración del firewall y las actualizaciones del sistema, entre otras. En Windows 7, el antiguo Centro de seguridad ha sido reemplazado por el **Centro de actividades**. Este apartado del sistema operativo nos permite acceder a **Windows Update**, seguridad de Internet, control de cuentas de usuario, y configuración del antispyware y firewall del sistema. Otra de sus ventajas es la posibilidad de ejecutar **solucionadores de problemas** frecuentes, y acceder a la configuración y mantenimiento de la computadora.

Para acceder al Centro de actividades de Windows 7, debemos hacer clic en **`Inicio`**/**`Panel de control`**/**`Sistema y seguridad`**/**`Centro de actividades`**.



FIREWALLS POR HARDWARE

En algunos entornos corporativos, se utilizan firewalls por **hardware**, dispositivos que administran la seguridad de una red antes de que los paquetes de datos lleguen a los equipos. En entornos hogareños, es posible encontrar firewalls por hardware en los routers.

¿DE QUIÉN NOS PROTEGE UN FIREWALL?

Como ya hemos dicho, un firewall nos protege en tanto controla el tráfico entrante y saliente de la red y evita que éste pueda poner en riesgo nuestra información. Sin embargo, y a través de la misma técnica, el firewall impide además que usuarios malintencionados accedan a nuestro equipo y lo controlen de manera remota o husmeen la información que contiene. Sin un firewall instalado en el equipo, sería muy fácil acceder a una computadora aun a pesar de que existen **políticas de red y recursos compartidos** que lo impiden. Imaginemos la siguiente situación: entramos a un bar y conectamos nuestra portátil a la red del lugar. Sin un firewall que nos proteja, cualquiera de los presentes podría acceder a nuestra carpeta **`Acceso público`** (**Figura 10**), que por defecto es visible y accesible por todos los usuarios de la red. Eso pondría en serio riesgo nuestro equipo y toda la información contenida en él.

Por añadidura, el firewall nos protege además de una de las más temidas amenazas de los últimos

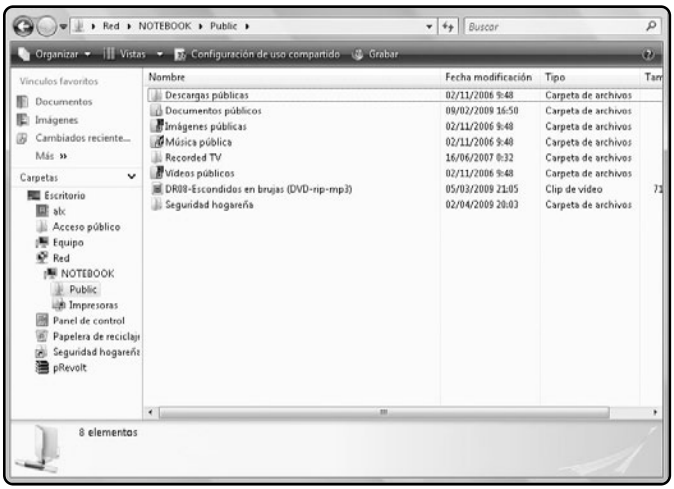


FIGURA 10.
La carpeta `Acceso público` es el espacio que Vista determina como el adecuado para compartir archivos.

CONFIGURACIÓN DEL FIREWALL

La configuración de un firewall exige el conocimiento de conceptos avanzados de seguridad informática. Un error mínimo en los parámetros de configuración podría generar un agujero de seguridad en el equipo. Por lo tanto, lo mejor es activar la configuración automática.

tiempos: los **adware** y **spyware**, un tipo de software malicioso que, sin autorización del usuario, utiliza la información de su perfil con fines estrictamente comerciales. Además, la instalación de aplicaciones de este tipo en computadoras personales suele tener efectos muy nocivos en el rendimiento general del equipo. El firewall nos protege de ellos, impidiendo que aplicaciones no autorizadas ingresen en la red o extraigan información de ella.

Acerca de adware y spyware

La nueva generación de amenazas informáticas incluye una de la que debemos aprender a cuidarnos con atención: los adware y spyware. Las máquinas infectadas por ellos suelen funcionar con lentitud. Además, la privacidad del usuario no está asegurada en los equipos infectados. Veamos en qué consisten estas amenazas, de las que aprenderemos a librarnos más adelante.

ADWARE

El término **adware** deriva de la conjunción de las palabras inglesas **advertisment** (**aviso publicitario**) y **software** (**Figura 11**). Los adware son programas cuyo objetivo consiste en mostrar, de manera continua, ventanas de publicidad en la computadora del usuario que lo instaló.

¿Por qué es éste un punto muy importante? Los adware son programas instalados con el consentimiento del usuario. Por supuesto, en la mayoría de los casos, el cibernauta instala adware sin saberlo. ¿Cómo? Junto con otros programas gratuitos que, para financiarse, incluyen este tipo de software, o al hacer clic en algún cuadro de

FIGURA 11.
El equipo se llenará de ventanas de publicidad si lo infectamos con adware y spyware.

descarga que la página abrió en forma automática y al cual el usuario no le prestó atención.

Los programas que incluyen adware consigo suelen generar controversia. Además, muchas veces los desarrolladores de adware crean aplicaciones que resultan muy llamativas para los navegantes más novatos, como juegos online o instaladores de smileys y papelería para e-mails, en busca de que los usuarios los instalen para así difundir más su adware.

Muchas descargas gratuitas se financian mediante la inclusión de un **banner** (un cartel de publicidad) en el programa mismo, y otros, más abiertamente, instalan un adware, cuyo fabricante paga por cada instalación de su producto. La inclusión de adware en los programas se está documentando y, si el usuario leyera el contrato de licencia completo cuando instala nuevos programas, descubriría el engaño del agregado de la aplicación publicitaria (**Figura 12**). Es lamentable, pero son pocos los usuarios que se toman el tiempo necesario para leer el **Contrato de Licencia de Usuario Final** (**CLUF**, o **EULA**, del inglés **End User License Agreement**).

El adware, una vez instalado, invade la privacidad del usuario y muestra en la computadora avisos cuya temática está basada en búsquedas que el cliente haya hecho en páginas de Internet y en el buscador de escritorio que utilice (**Figura 13**).

FIGURA 12.
El reproductor multimedia BSPlayer, en su versión gratuita, instala una buena cantidad de adware. Recomendamos, en su reemplazo, utilizar el excelente VLC Player (www.videolan.org).

ADWARE-SUPPORT

Existe una categoría de software conocida como **Adware-Support**. Este tipo de aplicaciones es desarrollado por programadores que buscan lucrar con la distribución de sus productos y cierran contratos con empresas de adware que les pagarán por cada descarga.

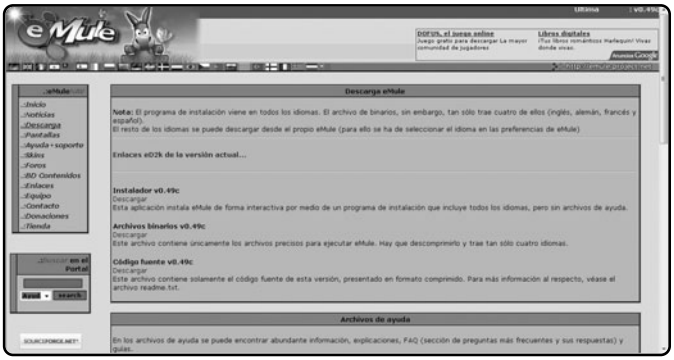


FIGURA 13.
Al pensar en algún programa de intercambio de archivos, eMule resulta sin duda la mejor opción. Además de ser un desarrollo libre y gratuito, es uno de los pocos programas de este tipo que no instala adware.

Los datos recolectados por el programa son enviados al servidor del adware con periodicidad. Este acto, cuando el navegante desconoce la situación, se plantea como una violación a la intimidad. Esta técnica es conocida en el mundo de la publicidad como **marketing contextual**.

SPYWARE

Es considerado **spyware** aquel software que envía información sobre los hábitos de navegación de un usuario al sitio web de su creador.

El spyware trabaja en conjunto con los adware y, por lo general, se instala también junto con ellos, al tiempo que el usuario instala un producto que promete ser gratis. Probablemente, en la licencia del software que esté infectado, se nos anoticie de esta situación y se nos explique qué datos va a recolectar el spyware.

El principal riesgo que suponen los spyware es la pérdida absoluta de la intimidad por parte del usuario. Aunque no siempre provocan mayor lentitud en el equipo ni generan un riesgo de pérdida

SERVICIOS PAGOS

La mayoría de los proveedores de Internet ofrecen servicios adicionales de protección contra amenazas informáticas. Es recomendable informarnos ya que, en muchas ocasiones, podremos obtener un filtro de spam o un antivirus directamente en el servidor por poco dinero.

de los datos, sí violan la privacidad del usuario (**Figura 14**). Esto supone un riesgo en tanto vuelve vulnerable un equipo en el que, casi siempre, contamos con información sensible, desde documentos hasta contraseñas de acceso a servicios de correo electrónico e, incluso, home banking.

Seguridad en la red local

Así como evitar una infección de adware y spyware es en gran parte responsabilidad del usuario, mantener un perfil de seguridad serio y eficiente en la red local está muy relacionado con las prácticas y políticas de navegación de cada usuario (**Figura 15**).

Sin embargo, contar con un **router** bien configurado, con una configuración de **seguridad inalámbrica** confiable y precisa, y con el **firewall por hardware** del dispositivo activado, son premisas centrales si pretendemos evitar una infección mayor.

En el **capítulo 5** de este libro, aprenderemos cómo configurar en detalle un router inalámbrico de modo que ningún apartado de seguridad quede olvidado. Porque es especialmente importante prestar atención a la forma en la que los usuarios se conectan a Internet en un hogar o en una pequeña oficina: de la precisión con la que esté establecida la configuración del router, depende la eficacia del perfil de seguridad (**Figura 16**).

FIGURA 14.
Los programas removedores de adware y spyware se han vuelto en los últimos tiempos tan importantes o más que los antivirus. Uno de los mejores exponentes en este rubro es Spybot Search & Destroy**.**

FIGURA 15. La actualización de los productos que defienden nuestro sistema es importante para que nuestra PC sea una fortaleza digital.

Cómo sentirse **seguro al navegar**

Para pensar en una navegación segura, lo primero por tener en cuenta es el cuidado de la información personal del propio usuario. Con el fin de no ser blanco de ningún tipo de ataque, hay que ser lo más anónimo posible. Es conveniente mantenernos alejados de cualquier servicio o aplicación interesada en conseguir información del navegante. Veremos en el **capítulo 7** de este libro de qué manera podemos proteger nuestra información personal.

La primera regla consiste en dar información personal solo en aquellos casos donde esta entrega se justifique y a aquellas empresas cuya reputación consideremos confiable o, como veremos más adelante, cuyos **certificados de seguridad** la validen como respetable.

FIGURA 16.
Cada vez más hogares y oficinas cuentan con dispositivos que brindan conectividad inalámbrica. Una configuración segura para el aparato es imprescindible para no poner en riesgo la computadora.

¿QUÉ ES UN ROUTER?

Un **router** o **enrutador** es un dispositivo que permite compartir la conexión a Internet de modo cableado y, a veces, de manera inalámbrica. Sirve para generar una **red local** (**LAN**) en tanto funciona como un servidor **DHCP**, es decir, asigna **direcciones IP** a los equipos de la red.

Datos útiles para tener en cuenta

NAVEGADOR ACTUALIZADO

Es importantísimo contar con un **navegador actualizado** para ayudar a prevenir el robo de cualquier información personal disponible en el equipo. Si usamos el navegador de **Microsoft**, recibiremos las actualizaciones de manera automática. Todos los navegadores, sin embargo, ofrecen este tipo de sistemas de actualización.

TELÉFONOS CELULARES

Los teléfonos celulares que ofrecen servicios **3G** y conexión a Internet de otros tipos (**GPRS** o **Edge**) no suelen ser blanco de los ataques de software malicioso. Sin embargo, no es una mala idea extremar las medidas de precaución y seguridad. Si su sistema operativo lo permite, es recomendable instalarle a nuestro gadget un antivirus.

CRUCE DE INFORMACIÓN

Quienes estén interesados en estudiar las causas y consecuencias del cruce de informaciones personales disponibles en la red, pueden leer el **capítulo 4** del excelente libro de Aníbal Ford, **La marca de la bestia**.

Lo más probable es que, al comprar algún producto en línea, resulte imprescindible entregar nuestra dirección para recibir el paquete, pero de ninguna manera será necesario dar una fecha de nacimiento. Ese dato no es importante y nada tiene que ver con el envío: si nos lo piden, están buscando de nosotros algo más (**Figura 17**).

La existencia de variados datos de una misma persona en el ciberespacio puede tener consecuencias inesperadas en tanto cualquier programa malintencionado posibilita cruzar **diferentes datos** disponibles sobre un usuario, con fines no deseados.

Para tomar un ejemplo en apariencia inofensivo, pensemos en un usuario que hubiese dado la fecha de nacimiento de su pequeño hijo a un sitio poco seguro: cualquier adware podría, con esa información, llenar de publicidades de juguetes su casilla de correo, o de ventanas publicitarias su navegador el día indicado (**Figura 18**).

FIGURA 17. Algunas instituciones, como BVQI, se encargan de verificar la precisión con la que las empresas manejan los datos confidenciales de sus clientes.

Los routers ofrecidos por los proveedores de Internet no tienen, activadas por defecto, funciones que mejoran el nivel de seguridad

FIGURA 18.
Los sitios más confiables tienen complicados (y algunas veces ineficientes) sistemas de recupero de contraseñas. Pero nunca preguntan información personal para restablecer datos secretos.

RESUMEN

En el primer capítulo de este libro, hemos aprendido las nociones básicas de seguridad informática y también hicimos una recorrida por las principales amenazas con las que podemos toparnos al interactuar con un equipo conectado a una red o a Internet.

Multiple **choice**

1 ¿En qué año se creó el primer virus esparcido fuera de laboratorio?

a- 1972
b- 1978
c- 1982
d- 1988

2 ¿Los programas contienen adware?

a- No.
b- Todos los programas contienen adware.
c- Sí, especialmente los descargados de Internet.
d- Solo los de sistemas Linux.

3 ¿Cuál fue la primera computadora cuyo sistema operativo fue afectada por un virus?

a- Apple II.
b- Pentium II.
c- IBM 286.
d- Ninguna de las anteriores.

4 ¿En qué época se extendieron los virus?

a- Finales de los sesenta.
b- Finales de los setenta.
c- Finales de los ochenta y principios de los noventa.
d- Finales de los noventa.

5 ¿Qué elementos favorecieron esa expansión de los virus?

a- La descarga ilegal de películas.
b- Los BBS y el uso masivo de Internet.
c- La aparición de la suite Office.
d- Ninguna de las anteriores.

6 ¿Existen los firewalls que actúan por hardware?

a- No, solo existe el de Windows.
b- Sí, se utilizan en algunos entornos corporativos.
c- Sí, por ejemplo Comodo Security.
d- Ninguna de las anteriores.

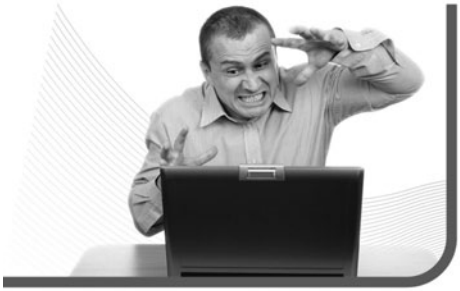
Respuestas: 1c, 2c, 3a, 4c, 5b y 6b.

Capítulo 2

Primer paso: instalar un antivirus

Conoceremos en detalle qué son los virus, para luego instalar un antivirus que nos mantenga a salvo de estas amenazas.

Una vez que conocimos las nociones básicas de protección, estamos listos para empezar con nuestra tarea de convertir nuestra computadora en el más seguro elemento de nuestra vida digital. Para comenzar, conoceremos en detalle qué son los virus, para luego instalar un antivirus que nos mantenga a salvo de estas amenazas que ponen en riesgo el sistema.



Virus, una antigua amenaza informática

Como hemos visto en el **capítulo 1**, los virus son la más antigua de las amenazas informáticas. Por eso, y porque son las que pueden traer las consecuencias más desagradables, ya que ponen en riesgo la existencia de nuestros datos y el funcionamiento del equipo, son las primeras de las que debemos protegernos. Además, con tantos años en el mercado, los productos antivirus han alcanzado un nivel de precisión y automatismo tal en su funcionamiento que le facilita la vida al usuario (**Figura 1**). Por esto, a menos que se encuentre con una infección repentina o que, en un descuido, se ejecute un archivo infectado, la razón más común de infecciones de virus en los últimos tiempos, es difícil que el usuario tenga que preocuparse por el antivirus.

Estas aplicaciones, incluso, se actualizan sin problemas y, solo llaman la atención del usuario en el momento en que, por algún motivo asociado a problemas de conexión, no cuentan con la última

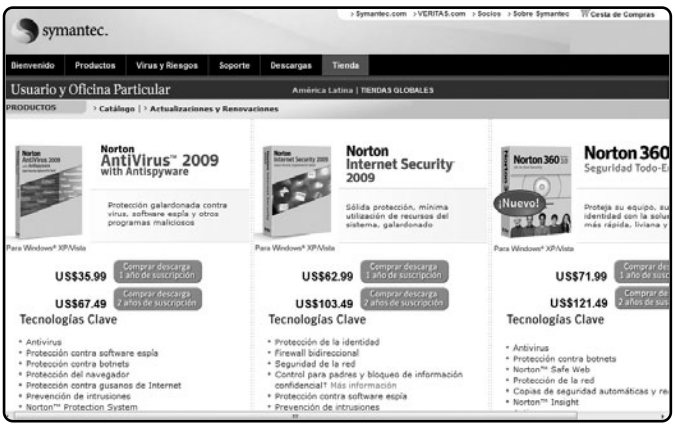


FIGURA 1.
Los productos históricos del sector, como el McAfee Antivirus y el Norton Antivirus, tienen más de 15 años de historia.

versión del archivo de definiciones de virus. Incluso, podemos implementar qué debe hacer el programa al encontrar un peligro y ni siquiera nos enteraremos de que halló una dificultad.

Tal es el grado de perfección y funcionalidad que alcanzaron en los últimos tiempos los antivirus que la amplia disponibilidad de opciones y productos dio lugar a que apareciera un **mercado de los antivirus gratuitos** (**Figura 2**). Éstos, ampliamente aceptados por el común de los usuarios, ganaron terrenos sobre las otras alternativas del mercado.

Con el correr de los años, los antivirus comerciales debieron ofrecer mayores niveles de protección al usuario y agregar a sus productos componentes de seguridad asociados, del estilo de antispyware, firewalls y sistemas de protección contra phishing y estafas informáticas de todo tipo. En la actualidad, las soluciones comerciales suelen venderse como **productos integrales de seguridad** y no como *antivirus stand alone*, es decir, que cumplen solo esa función.

Sin embargo, en este libro preferiremos utilizar un programa gratuito y que se limita a protegernos, en especial, de virus y de códigos maliciosos. Esto es así, porque a lo largo de este texto seleccionaremos las mejores herramientas para protegernos de cada

FIGURA 2. Las soluciones antivirus gratuitas ganaron mercado, respecto de las comerciales, en cuanto aparecieron los firewalls.

tipo de amenaza en particular y evitaremos entonces soluciones integradas que descuiden algún aspecto de la seguridad de nuestro equipo.

El antivirus que mostraremos, y sobre el cual profundizaremos en este capítulo, es **AVG AntiVirus Free Edition**, que se puede descargar desde el enlace **http://free.avg.com**. Este software también puede conseguirse en una versión comercial denominada **AVG Internet Security**.

Ahora que conocemos los antivirus, es un excelente momento para aprender más al respecto de los virus tecnológicos que estas herramientas combaten.

DOBLE PROTECCIÓN EN UNA SOLA APLICACIÓN

Para evitar instalar un antispyware de terceros, podemos utilizar AVG Internet Security (versión comercial de AVG), con protección avanzada contra estafas informáticas y un antispyware básico. **Spybot Search & Destroy** es mejor, pero AVG ofrece doble garantía en una sola aplicación.

Los virus **en acción**

Los **virus** son aplicaciones informáticas programadas por usuarios especializados que tienen algún interés particular en generar daños en sistemas, o crear pánico y controversia en la red. Para entender el modo en el que un virus se reproduce, debemos conocer la manera en la que ellos mismos actúan, razón por la cual los clasificaremos en dos grandes grupos: residentes y no residentes.

VIRUS NO RESIDENTES

Los virus **no residentes** (por lo general de **macro**) se alojan en un documento y sólo son ejecutados en el caso de que el archivo se abra. Por ejemplo, un macro virus en un archivo de **Microsoft Word** no estará residente en la memoria durante toda la sesión, sino que se ejecutará al momento de ser abierto el archivo infectado.

Los virus no residentes cuentan con un módulo **buscador** y un módulo **reproductor**. El módulo buscador selecciona nuevos archivos para infectar, mientras que el reproductor es el encargado de ejecutar la infección. A la hora de infectar un archivo, el módulo reproductor adosa el código del virus al punto inicial del archivo ejecutable de modo que, al abrir un archivo, el virus sea el primero en cargarse (**Figura 3**).

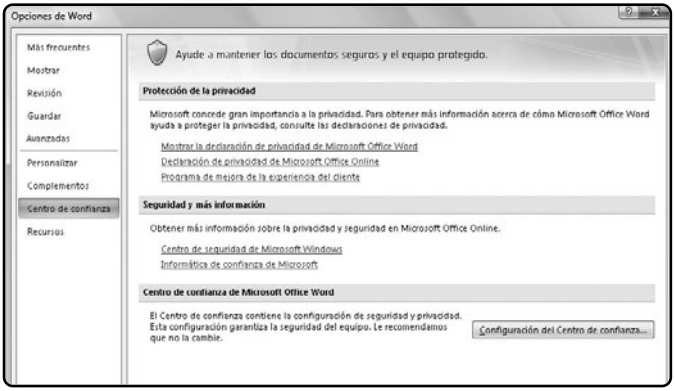


FIGURA 3.
El Centro de confianza de Office 2007 permite administrar el modo en el que se trabajará con macros para evitar infecciones.

APLICACIONES TSR

Un programa **TSR** (**residente en memoria**, del inglés **Terminate and Stay Resident**) es una aplicación que, al iniciarse, se mantiene funcionando en la memoria continuamente. Así funcionan los antivirus: inician con el equipo y quedan trabajando siempre en segundo plano.

También es importante destacar que los archivos **ejecutables** son los más propensos a ser atacados por un virus, así como también los documentos. Estos últimos (en particular aquellos creados con la suite de oficina de Microsoft) suelen ser objeto de virus no residentes y macrovirus, por lo que las aplicaciones que los abren deshabilitan las macros.

VIRUS RESIDENTES

Los **virus residentes** son aquellos que se ejecutan al inicio de la sesión de usuario en el sistema operativo y, durante el tiempo en que el equipo esté encendido, permanecen trabajando en la memoria. Estos elementos maliciosos emplean, para infectar archivos, un método similar al utilizado por los no residentes, con la diferencia de que no cuentan con un **módulo buscador**. Su carácter de residente hace que cualquier operación del sistema operativo sea analizada por el módulo reproductor del virus, que infectará todos los archivos y programas posibles de ser atacados.

Existen dos categorías de virus residentes, los llamados rápidos y los conocidos como lentos (**Figura 4**). Los **virus rápidos** tratan, en forma constante, de infectar nuevos archivos en el equipo elegido. Su accionar los hace demasiado peligrosos en tanto cada archivo que un programa trate de abrir será infectado. Esta efectividad a la hora de reproducirse conlleva un efecto muy negativo para el virus: este tipo de ataques son fácilmente detectables porque reducen de manera drástica la velocidad y los recursos del equipo infectado.

FIGURA 4.
Muchos residentes lentos insisten en el intento de infectar las unidades extraíbles en cuanto se las conecta. Si contamos con un buen antivirus, éste debería detener el ataque.

TAREAS PROGRAMADAS

Por defecto, el antivirus programa un análisis automático mensual. Sin embargo, es posible programar análisis quincenales, o semanales, si nuestro equipo está en constante riesgo. Los configuramos desde **`Análisis programados`**, del cuadro **`Configuración avanzada de AVG`**.

Los **virus residentes lentos**, en cambio, sólo infectan archivos en forma ocasional o en cierto contexto, por ejemplo, cuando un archivo es copiado. El usuario rara vez podrá descubrir la infección, aunque, por otra parte, el virus tampoco abarcará un gran número de archivos. A causa de este último problema, la mayoría de los virus suelen ser residentes rápidos.

LA VULNERABILIDAD DE LOS SISTEMAS OPERATIVOS

La cantidad de virus y la potencia con la que ellos actuarán sobre la computadora varía según el sistema operativo con el que cuenta el equipo amenazado. De hecho, hay sistemas operativos para los que no existen los virus, como **UNIX** y gran parte de las variantes de **Linux** (**Figura 5**).

Por motivos políticos, ideológicos y comerciales, **Windows**, el sistema operativo de Microsoft, está en la mira de los creadores de virus. Los programas de esta compañía, además, suelen ser muy criticados por la facilidad con la que pueden ser infectados y por los agujeros de seguridad con los que, por lo general, son lanzados al mercado.

FIGURA 5.
Los usuarios de Linux no deben preocuparse tanto como los de Windows por los virus. Casi no hay códigos maliciosos diseñados para atacarlo.

VIRUS EN LINUX

El primer virus para Linux (de nombre **Blizz**) fue lanzado al ciberespacio el 5 de febrero de 1997. Las principales empresas productoras de antivirus para Windows dijeron que era el principio de un mercado antivirus para Linux, cosa que hasta el momento, aún no ha ocurrido.

Más allá de las diferencias extratecnológicas, algunos sistemas operativos son, por la forma misma en la que funcionan, más factibles de ser infectables. Así, los sistemas operativos basados en UNIX, como hemos dicho, rara vez son atacados. Y aquí hay que aclarar que esto no se da sólo porque estos sistemas son de código abierto y, por ende, la comunidad de programadores apoya su desarrollo: estos sistemas trabajan de un modo en el que el usuario no puede ejecutar programas más allá de los límites que el sistema operativo le impone. De este modo, ningún virus podrá infectar nada más allá de la sesión del usuario, manteniendo intacto el **kernel** y sin la posibilidad de extenderse más allá de los límites de la sesión.

Los usuarios de Microsoft Windows, en cambio, suelen iniciar sus sesiones en modo **Administrador** y cuentan con acceso completo al sistema operativo. Si bien esto da la sensación de mejorar la experiencia del usuario, también permite que, cuando un virus logra infectar el sistema, tenga la máquina a su merced.

Como podemos ver, aquí no hay diferencias ideológicas, políticas ni comerciales: es una cuestión estrictamente técnica. El hecho de que la mayor parte de usuarios prefiera, por razones que no tiene sentido analizar aquí, el sistema operativo de Microsoft, habilita la existencia de una gran variedad de virus que, aprovechando las características técnicas del programa, se distribuyen entre los clientes.

La **prevención**

Es importantísimo repasar algunas estrategias para evitar infectarnos con cualquier virus que circule por Internet. Veamos qué se debe hacer y qué no, si queremos que nuestra vida en el ciberespacio sea segura y poco problemática (**Figura 6**).

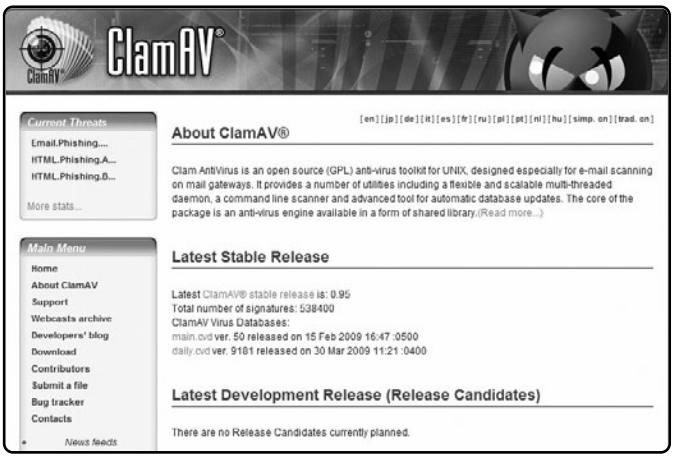


FIGURA 6.
Si buscamos una alternativa distinta de AVG, el antivirus ClamAV propone una muy buena solución para usuarios medios y avanzados. Además, es libre y gratuito.

En principio, cabe recordar que es imperativo tener instalado y actualizado a diario un programa antivirus. No hay siquiera que conectar el módem al equipo si el antivirus no está instalado y funcionando sin problemas. Las opciones son muchas, pagas y gratuitas, profesionales y hogareñas, y no hay ningún motivo por el cual no contemos con una completa suite antivirus. En este capítulo aprenderemos a instalar, configurar y utilizar **AVG AntiVirus Free Edition**.

Respecto de la actualización del antivirus (**Figura 7**), cabe aclarar que es un proceso sumamente simple que, en la mayoría de los casos, ni siquiera requiere intervención del usuario si se dispone de una **conexión permanente** a Internet.

Nunca está de más escanear cada tanto el disco duro de la PC en busca de virus. Si bien todos los antivirus cuentan con esta opción, si sospechamos de un ataque también podemos ejecutar el proceso en línea con un **antivirus web**. **Trend Micro** (**Figura 8**) ofrece uno gratuito cuya eficacia no es demasiado alta, pero alcanza para sacarnos de un apuro.

Al acceder a un medio extraíble en un equipo protegido por un antivirus cuya configuración sea la que propondremos en este capítulo, el medio será analizado de forma automática (**Figura 9**). Sin embargo, si el usuario quisiera volver a comprobar la unidad, también podría hacerlo de manera manual.

FIGURA 7.
Todos los antivirus tienen una alternativa de actualización manual, que nos permite descargar el último archivo de definiciones si la descarga no se pudo realizar en forma automática.

FIGURA 8. El antivirus en línea de Trend Micro está disponible en la dirección web http://housecall65.trendmicro.com.

Una última aclaración importante: de ninguna manera hay que abrir archivos adjuntos de remitentes desconocidos en mensajes de correo electrónico. Tampoco debemos hacer caso a aquellos de remitentes conocidos cuyo texto resulta raro u ofrece atractivos premios o imágenes provocativas. Sólo debemos, por regla general, abrir los adjuntos que esperábamos o aquellos a los que se hace referencia en el mensaje (**Figura 10**).

Frente a estos riesgos, la necesidad de una copia de respaldo de la información disponible en el equipo, siempre actualizada, es imprescindible (**Figura 11**).

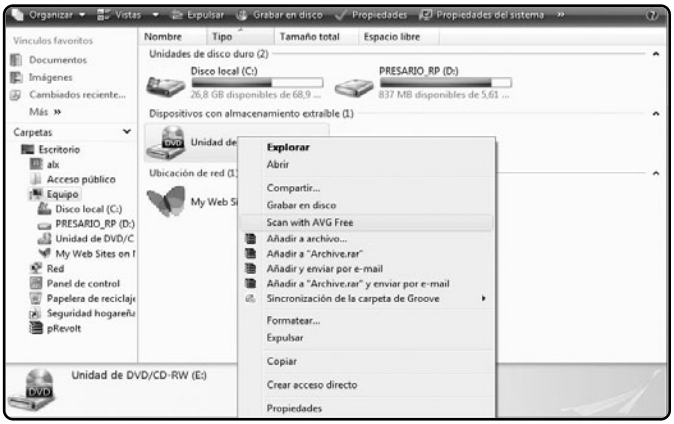


FIGURA 9. En el menú contextual de toda unidad extraíble, existe una opción para analizar el dispositivo antes de acceder a él. En la imagen, la herramienta del antivirus AVG.

ACTUALIZACIONES DE SEGURIDAD

Las fallas de seguridad inherentes al modo de funcionamiento de Windows pueden solucionarse instalando actualizaciones de seguridad. Activar las **actualizaciones automáticas** del sistema nos protege contra cualquier posible falla de seguridad.

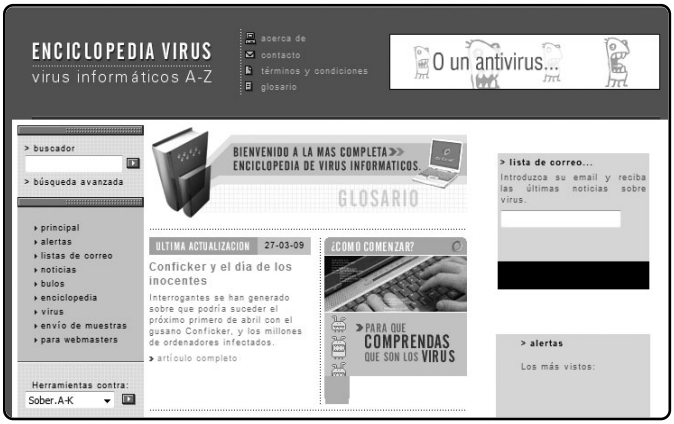


FIGURA 10.
El sitio Enciclopedia Virus**, al que se puede acceder ingresando en el enlace** www.enciclopediavirus.com**, actualiza a diario la información sobre nuevos virus y los modos de prevenirlos.**

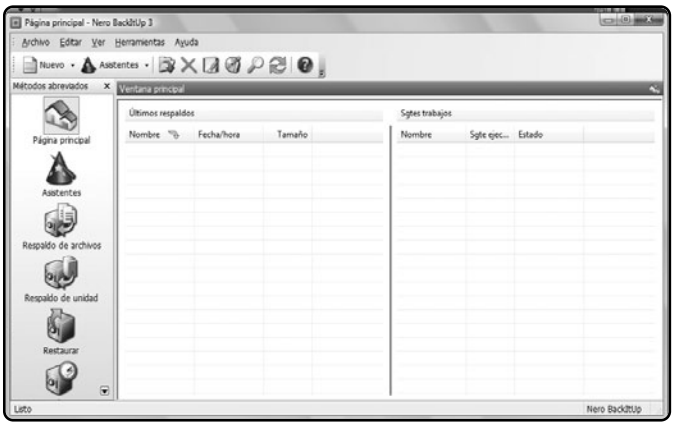


FIGURA 11.
La suite de grabación de CDs y DVDs Nero **incorpora** Nero BackItUp! 3**, una potente herramienta que mantendrá al día las copias de respaldo del equipo.**

INFORMACIÓN SOBRE ANÁLISIS

Aunque AVG detecte una infección en el equipo durante un análisis programado, el usuario no será alertado al respecto. Si deseamos saber el resultado de los diferentes tests automáticos, podemos consultarlo en **`Resultados del análisis`**, en el menú **`Historial`** del antivirus.

Las posibilidades de una infección son muchas aun para los usuarios más experimentados, y el riesgo de pérdida de datos es muy alto. Por lo tanto, resulta fundamental que tengamos una copia de seguridad de nuestros datos ante cualquier eventualidad.

Instalar un antivirus

Hemos recorrido en lo que va del capítulo los conceptos fundamentales acerca de las características de los virus y sus principales estrategias de infección, así como también los recaudos que los usuarios debemos tener para prevenirla.

Llegó el momento de poner manos a la obra y estudiar a fondo el funcionamiento de un antivirus desde su instalación hasta las más profesionales herramientas de protección. Para hacer esto, vamos a utilizar el antivirus gratuito AVG AntiVirus Free Edition, una versión reducida del antivirus de AVG que es absolutamente funcional y muy eficaz.

Para descargar este antivirus, ingresamos en **http://free.avg.com**. En el cuadro desplegable de idiomas, seleccionamos **`Latin America (Español)`**. Luego presionamos **`Descargar`**. En la nueva pantalla, pulsamos clic sobre el botón **`Descargar`** de la columna correspondiente a **`AVG Free`** (**Figura 12**).

FIGURA 12.
En la pantalla de descarga del producto, presionamos un clic sobre el botón Descargar AVG 8.5 gratuito**.**

BARRA AVG

La versión gratuita del antivirus de AVG ofrece la instalación automática de la **barra de seguridad AVG**, un buscador con fines comerciales que no aporta grandes mejoras de seguridad y hace más lento el funcionamiento del navegador.

En el siguiente paso, se nos pedirá una confirmación, que tendremos que aceptar haciendo clic en **Guardar**. Luego indicamos el destino del archivo (el escritorio puede ser una buena opción). A continuación, pulsamos clic en **Aceptar**, para que comience la descarga.

INSTALACIÓN

Al hacer doble clic sobre el archivo descargado, se iniciará el asistente para la instalación del antivirus AVG AntiVirus Free Edition. En la mayoría de los casos, la configuración predeterminada alcanza para proteger cualquier equipo, y el usuario no necesita cambiar ningún parámetro del programa.

AVG AntiVirus Free Edition no ofrece soporte técnico, aunque en los foros del sitio se pueden encontrar respuestas a las preguntas frecuentes. Aunque todos pueden leer las respuestas, sólo los usuarios registrados tienen la posibilidad de preguntar, por lo que es recomendable registrarse en **http://free.avg.com**.

Actualizar el antivirus

La actualización del antivirus es tan importante, o más, que la del sistema operativo. Si no contamos con una versión actualizada del archivo de definiciones de virus, el funcionamiento de la aplicación será pobre y no podrá detectar los últimos virus. Éstos resultan ser los más peligrosos, porque son aquellos contra los cuales el sistema tiene menos formas de defenderse.

El proceso de actualización del antivirus es automático, aunque hay actualizaciones secundarias y opcionales que siempre es recomendable instalar. Para forzar la búsqueda de actualizaciones, en el caso de AVG y de la mayoría de los antivirus, incluidos los pagos, alcanzará con presionar el botón derecho sobre el icono del antivirus en la zona de notificación de la Barra de tareas y seleccionar del menú contextual **Actualizar ahora** (**Figura 13**).

Al terminar la actualización, recibiremos la notificación. Presionamos **Ok** en el cuadro, y repetimos el proceso tantas veces como la cantidad de actualizaciones disponibles que haya.

PROBLEMAS DE ACTUALIZACIÓN

El problema con la actualización puede presentarse cuando no contamos con una conexión permanente a Internet o cuando se utiliza un **servidor proxy** de algún tipo, como suele ocurrir en redes corporativas o en ciertos servidores de Internet. Frente a situaciones de este tipo, puede ser conveniente la actualización manual del antivirus. En la versión 8.5 del antivirus de AVG, cuando hay un problema, el icono suma un signo de admiración, pero se mantiene de colores.

FIGURA 13. El área de notificación, con el icono del antivirus, está en la parte inferior derecha de la pantalla, en la barra de tareas de Windows.

PASO A PASO /1
Instalación de AVG AntiVirus Free Edition

1

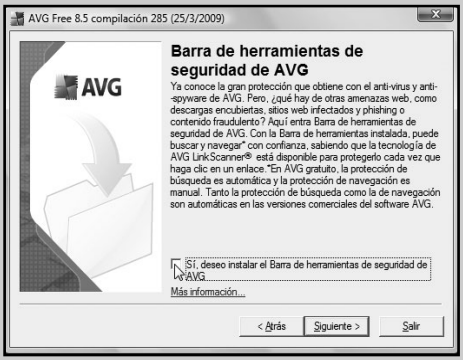
Haga doble clic sobre el archivo descargado. Al recibir una advertencia de seguridad, presione **Ejecutar**. En la pantalla de bienvenida del instalador del programa, seleccione el idioma **Español**.

2

Presione **Aceptar** en la Notificación de Aceptación y acepte el contrato de licencia con un clic en **Aceptar**. Una vez que el instalador verifique el sistema, se le preguntará por el tipo de instalación. Seleccione la opción **Instalación estándar** y, luego, presione **Siguiente**.

PASO A PASO /1 (cont.)

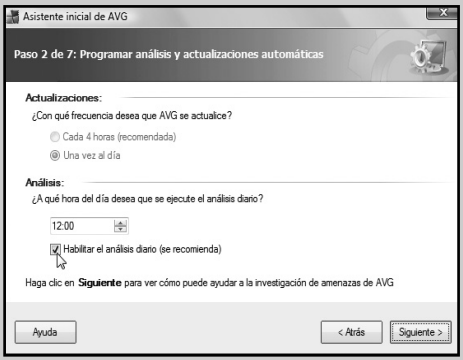
3



En el cuadro **`Activar su licencia de AVG Free`**, presione **`Siguiente`**.

Destilde **`Sí, deseo instalar la barra de herramientas de seguridad de AVG`** en el cuadro **`Barra de herramientas de seguridad de AVG`**.

4

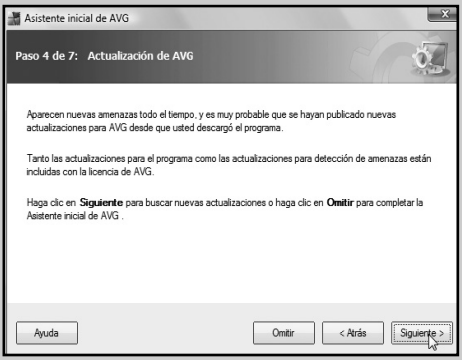


Pulse **`Finalizar`** en el cuadro **`Resumen de la instalación`**.

El programa copiará archivos en el sistema. En el paso 1 del **`Asistente inicial de AVG`**, presione **`Siguiente`**.

PASO A PASO /1 (cont.)

5



Si no cuenta con un equipo potente, destilde **Habilitar el análisis diario** en el paso 2, y presione **Siguiente**. Acepte las opciones por defecto del paso 3 y presione **Siguiente** en el paso 4 para que el sistema comience a actualizarse.

6

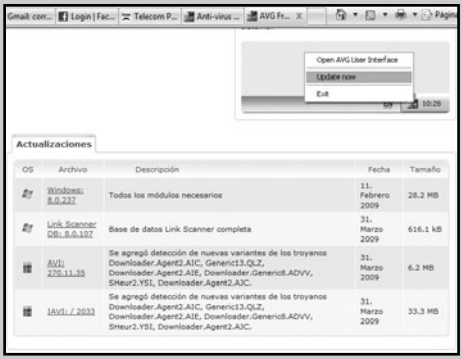
Puede registrar el antivirus presionando el botón **Registrar AVG Anti-Virus Free**. Presione **Siguiente**. Pulse **Finalizar** para terminar la instalación.

PASO A PASO /2
Actualización manual

1

Abra su navegador de Internet y conéctese a **http://free.avg.com**.
Cambie el idioma a **`Latin America (Español)`** y haga clic en el vínculo **`Descargar actualizaciones.`**

2



Haga clic sobre el nombre del archivo de la actualización más reciente.
Las puede discriminar por su fecha de emisión o tamaño. En la primera columna, aparece el nombre del archivo y, en la segunda, su descripción.

PASO A PASO /2 (cont.)

3

En este cuadro, presione **Guardar**. Seleccione como destino la ubicación del equipo en la que instaló el antivirus, por defecto **C:\Archivos de programa\AVG\AVG8.**

4

Una vez terminada la descarga, abra la interfaz del antivirus desde **Inicio/Todos los programas/AVG 8.5/AVG Free User Interface**.
EL programa se actualizará automáticamente al detectar el nuevo archivo de definiciones.

ACTUALIZACIÓN DESDE UNA CARPETA

Aunque la red en la que trabajemos no disponga de conexión a Internet, es imprescindible que todos los equipos cuenten con un antivirus y que ese antivirus esté actualizado. En situaciones así, más cómodo que copiar el archivo de definiciones a la carpeta de instalación de cada antivirus en cada equipo, es dejar una copia de este archivo en alguna carpeta de la red e indicar a cada copia de AVG que debe buscarla allí.

Para eso, luego de haber elegido para realizarlo una ubicación accesible a todos los equipos o de tenerle resguardo en alguna unidad extraíble con la que podamos visitar cada máquina, debemos abrir la pantalla principal del antivirus y allí optar por **`Herramientas/Actualizar desde directorio…`**

Seleccionaremos entonces la carpeta donde esté el archivo de definiciones, y el programa actualizará de manera automática su base de datos (**Figura 14**).

SERVIDORES PROXY

Si otra computadora de la red tiene una conexión permanente a Internet y la comparte mediante un servidor Proxy, será necesario configurar la opción correspondiente en AVG. En el **Paso a paso 3**, veremos cómo hacerlo. La información sobre el servidor proxy debe proveerla su administrador de red aunque, si ya tiene configurado un servidor proxy en un equipo, es posible que pueda encontrar estos datos en el cuadro **`Seguridad/Configuración LAN`** de las **`Opciones de Internet`** del Panel de Control de Windows.

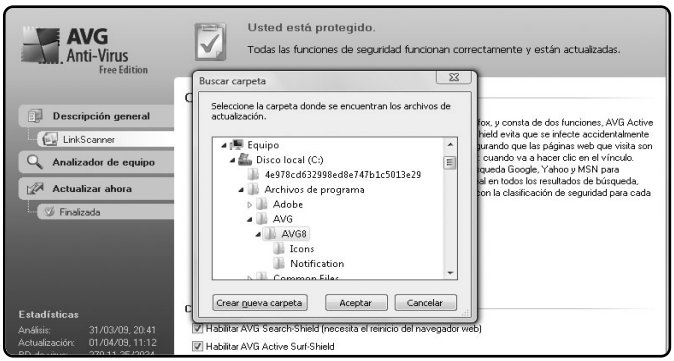


FIGURA 14.
Por defecto, el antivirus buscará las actualizaciones en la carpeta donde fue instalado, en cuyo caso el inicio de este proceso es automático.

PROBLEMA: ES POSIBLE NAVEGAR, PERO NO ACTUALIZAR

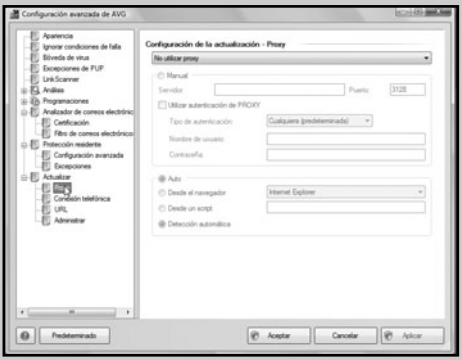
Si la conexión a Internet del equipo que usamos se da mediante un servidor proxy y no lo sabemos, ocurrirá que, aunque no tengamos problemas para navegar, el antivirus dirá que no se actualizó por no poder conectarse a Internet.

PASO A PASO /3
Cómo configurar el servidor proxy

1

Abra la ventana principal de AVG haciendo doble clic sobre el icono correspondiente en la zona de notificación de la Barra de tareas.

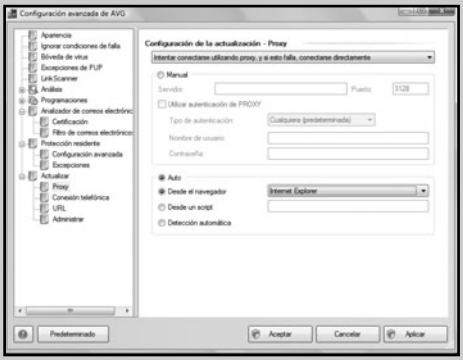
2



Una vez en la ventana principal, haga clic en el menú **Herramientas** y seleccione **Configuración avanzada**. En la nueva ventana, de la rama **Actualizar**, seleccione la subrama **Proxy**.

PASO A PASO /3 (cont.)

3



Del cuadro desplegable, seleccione **Intentar conectarse utilizando proxy, y si esto falla, conectarse directamente**. Del apartado **Auto**, seleccione la opción **Desde el navegador** y elija el explorador que utiliza en forma habitual.

4

Acepte todas las ventanas y, al volver a la pantalla principal, haga clic en el botón **Actualizar ahora** para contar con los nuevos archivos de definiciones.

CONEXIONES NO PERMANENTES

El comportamiento del antivirus en computadoras con conexiones a Internet que no son permanentes no requiere ninguna configuración específica ya que, en cuanto el programa detecte el establecimiento de la conexión, de manera automática comenzará el proceso de actualización.

Sin embargo, si no nos conectamos usualmente a Internet o trabajamos en redes donde sólo algunos equipos cuentan con una conexión propietaria a Internet, será una buena idea configurar las opciones necesarias para que el programa se conecte a la red, cuando lo requiera, del modo más automático posible.

Para acceder a la configuración avanzada del acceso telefónico, abrimos la ventana principal de AVG haciendo doble clic sobre el icono correspondiente en la zona de notificación de la Barra de tareas de Windows. Una vez en la ventana principal, pulsamos clic en el menú **Herramientas** y seleccionamos **Configuración avanzada**. En la nueva ventana, de la rama **Actualizar**, seleccionamos la subrama **Conexión telefónica** (**Figura 15**).

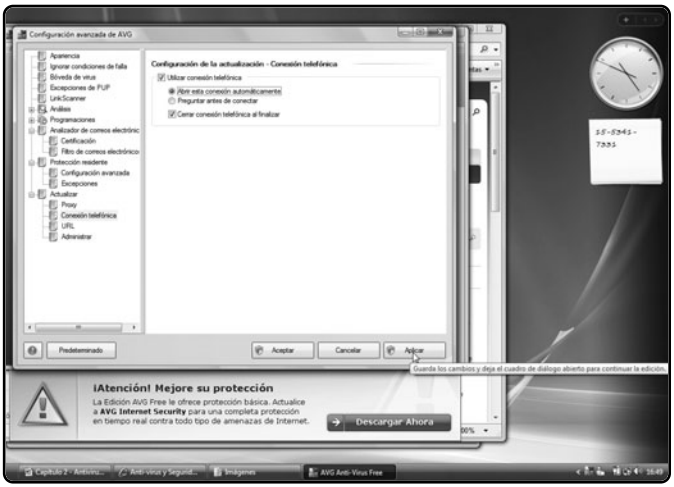
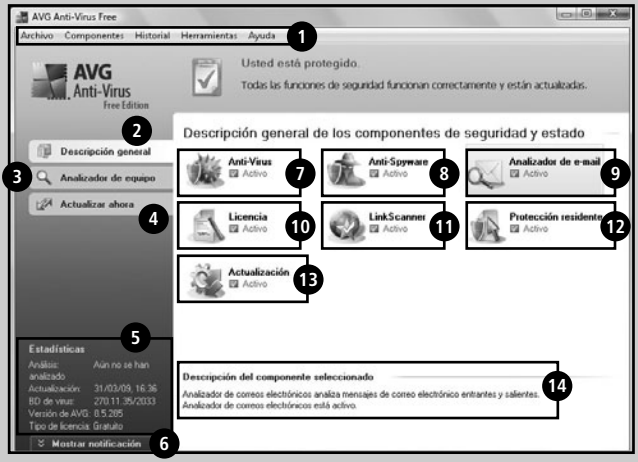


FIGURA 15.
Tildamos la opción `Utilizar conexión telefónica` **y seleccionamos** `Abrir esta conexión automáticamente`**. Luego hacemos clic en** `Aplicar`**.**

SERVIDORES PROXY

Un **servidor proxy** aumenta la seguridad y el control de una red. También puede dar acceso a Internet, previamente filtrado. Cualquier computadora puede funcionar como un servidor proxy, con el software correspondiente, como por ejemplo, **WinProxy 1.5** (**www.winproxy.net**).

GUÍA VISUAL /1
El Centro de Control de AVG Free



1. Barra de menús.
2. Muestra el estado de los componentes principales del antivirus.
3. Permite acceder a las opciones de análisis manual del sistema.
4. Busca actualizaciones del archivo de definiciones de virus.
5. Brinda información sobre el número de versión y la fecha de la aplicación; el archivo de definiciones y los últimos análisis del sistema.
6. Muestra u oculta opciones de mejoras ofrecidas por AVG.
7. Estado del módulo antivirus.
8. Estado del módulo antispyware, de funcionalidad limitada en la versión gratuita.
9. Estado del módulo de análisis de correo electrónico.
10. Estado de la activación de la licencia.
11. Estado del módulo analizador de vínculos.
12. Estado del módulo de protección residente, encargado de analizar los archivos por ejecutar y las acciones que llevará a cabo el usuario.
13. Estado del módulo de actualización automática.
14. Descripción del módulo seleccionado.

Si contamos con una **conexión ADSL** que, por alguna razón, no funciona continuamente, o aún tenemos conexiones de **acceso telefónico**, resulta imprescindible que utilicemos la configuración avanzada de este acceso, de modo que el antivirus esté siempre al día. Si no, es muy difícil que estemos bien protegidos.

El antivirus en acción

Con el antivirus instalado y con una configuración perfecta, estamos en condiciones de conectar el equipo a Internet sin riesgo de infecciones, siempre y cuando el sistema operativo que utilizamos cuente con un firewall coherente como el que incluye Windows Vista. Veamos entonces ahora cómo sacar el máximo provecho de AVG AntiVirus Free Edition y conozcamos a fondo todas sus funciones.

LA PANTALLA PRINCIPAL

Como sabemos, al hacer doble clic en el icono de la zona de notificación de la Barra de tareas, se abrirá el centro de control de antivirus de AVG. De las muchas ventajas que tiene este antivirus, sin duda, una de las más importantes es la velocidad con que su interfaz se carga, ya que en otros programas de este tipo el proceso de apertura de este componente puede durar bastante tiempo.

La pantalla principal del programa nos permitirá interactuar con todos los componentes del antivirus. Desde allí, ejecutaremos todas las herramientas y llevaremos a cabo los ajustes de configuración necesarios, relacionados con la protección. En la **Guía Visual 1**, pudimos estudiar los componentes de esta pantalla, para ubicarnos sin problemas en ella.

Para que el antivirus pueda comprobar la actualidad de sus definiciones, la fecha y la hora del sistema deben ser correctas. Si no es así, se nos notificará y deberemos corregir esta situación por medio de la sincronización automática con la hora de Internet de Windows.

RESUMEN

En este capítulo, hemos conocido las diferentes categorías de virus y sus características principales. Para defendernos de esta amenaza, hemos analizado cómo obtener y utilizar un antivirus gratuito y así, mantener a salvo nuestro sistema operativo.

Multiple **choice**

1 ¿Dónde se alojan los virus no residentes?

a- En los documentos.
b- En los archivos de sistema de Windows.
c- En las cookies.
d- Ninguna de las anteriores.

2 ¿Qué tipos de virus cuentan con un módulo buscador?

a- Solo los virus residentes.
b- Solo los virus no residentes.
c- Los virus residentes y no residentes.
d- Ninguna de las anteriores.

3 ¿En qué sistemas operativos no existe la posibilidad de virus?

a- En Windows.
b- En Windows 7.
c- En UNIX y gran parte de las variantes de LINUX.
d- Todos los sistemas operativos son vulnerables y pueden ser afectados por virus.

4 ¿Es importante actualizar el antivirus?

a- Siempre.
b- No es relevante.
c- Depende de nuestra versión de Windows.
d- Solo si nuestro equipo se conecta a una red.

5 ¿Cuál es el nombre del antivirus alternativo a AVG?

a- ClamAV.
b- Blackberry.
c- Zonealarm.
d- Thunderbird.

6 ¿Por qué es posible tener Internet, pero no poder actualizar el antivirus?

a- Por un problema del servidor.
b- Por el fabricante del módem.
c- Porque compartimos Internet con otra computadora y lo hacemos mediante un servidor proxy.
d- Ninguna de las anteriores.

Respuestas: 1a, 2b, 3c, 4a, 5a y 6c.

Capítulo 3

Segundo paso: protección contra adware, spyware y malware

Analizaremos la lucha con otras plagas, conocidas como adware, spyware y malware, y les daremos solución.

Así como en el capítulo anterior nos ocupamos a fondo de los virus, en éste, analizaremos la lucha con otras plagas, conocidas como adware, spyware y malware, y les daremos solución. Para esto, veremos en detalle el funcionamiento de estas amenazas y conoceremos a fondo todos los programas que nos ayudarán a combatirlas de manera eficaz.

La publicidad **no deseada**

Algunas veces, las amenazas tecnológicas suelen camuflarse en aplicaciones que proveen servicios personalizados para el cibernauta. En realidad, pretenden seducirlo para extraer información de su equipo.

Los adware y spyware son amenazas de este tipo, que roban datos personales del usuario para luego revenderlos a quienes le enviarán a éste publicidad con un perfil específico. Por lo general, se distribuyen con software gratuito que se financia con la inclusión de este tipo de programas, como podemos ver en la **Figura 1**.

FIGURA 1.
Los adware más peligrosos se distribuyen con programas básicos que prometen, por ejemplo, agregar fondos e imágenes a nuestros correos electrónicos.

SOFTWARE GRATUITO Y SOFTWARE LIBRE

Son muchos los programas que instalan consigo adware, y sobre ellos cabe hacer algunos comentarios. Aunque no sea el propósito de este libro profundizar en el tema, es importante diferenciar **software gratuito** de **software libre**. El software cuya descarga es gratuita no siempre es libre, y, en muchos casos, el hecho de que no le sea cobrado al usuario no supone que no tenga costo. De ese modo, muchas descargas gratuitas se financian mediante la inclusión de un **banner** (un cartel de publicidad) en el programa mismo, y otros, más directos, colocan un adware, instalación por la cual reciben un pago por parte del productor de la amenaza.

La inclusión de adware en los programas está siempre documentada, y, si el usuario lee el contrato de licencia, encontrará la información sobre el programa en cuestión. Desafortunadamente, son pocos los usuarios que se toman el tiempo necesario para leer el **Contrato de Licencia de Usuario Final** (**CLUF**, o **EULA** del inglés **End User License Agreement**). Si vamos a utilizar software gratuito, resulta fundamental que nos informemos sobre las condiciones en las que se distribuye el producto (**Figura 2**).

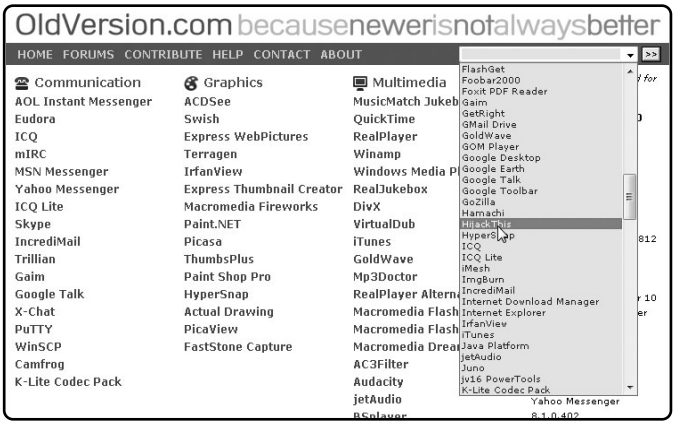


FIGURA 2.
En OldVersion, se pueden encontrar versiones antiguas, pero funcionales, de gran cantidad de software discontinuo sin adware.

PRECAUCIÓN CON JUEGOS ONLINE Y SMILEYS

Es muy importante tener cuidado al instalar **juegos online** o **instaladores de smileys** y **fondos** para e-mails, ya que muchas veces, están infectados con adware. Si deseamos usarlos, es necesario leer el contrato de licencia del producto y conocer los riesgos de utilización.

Una aplicación libre o de **código abierto**, en cambio, está sustentada por un marco filosófico que le impediría incluir adware u otras amenazas. Además, las aplicaciones creadas según este modo de distribución suelen compartir la licencia **GNU/GPL**, sobre la cual podemos encontrar más información en **www.gnu.org/licenses/licenses.es.html**. Por lo general, es posible utilizar sin mayores riesgos las aplicaciones libres (**Figura 3**).

Por otra parte, es posible encontrar en la red programas de dudosa utilidad que están creados, en última instancia, pura y exclusivamente para distribuir adware. Así, calendarios que se instalan en la zona de notificación de la barra de tareas o programas encargados de informar el estado del tiempo que ya ofrece el gadget de la **Windows Sidebar** podrían contener una importantísima cantidad de adware. Los paquetes de smileys (emoticones utilizados en los mensajeros instantáneos) son ejemplos clásicos de esta situación. En general, para poder utilizarlos, debemos aceptar la instalación de tres o cuatro servidores de adware.

Para terminar de entender el problema del adware y el spyware, es importante pensar una vez más en el tema de las licencias. No siempre hay que desconfiar de los productores: muchas veces en la licencia del software infectado con spyware se nos notifica de esta situación y nos explica qué datos

FIGURA 3. En las condiciones de la licencia GNU/GPL, en www.gnu.org/copyleft/ gpl.html**, vemos las ventajas de los sistemas de este tipo.**

FIGURA 4. Es posible ver la licencia de aquellos productos que ya estén instalados en nuestro equipo a la hora de adquirirlo.

¿QUÉ SON LOS ADS?

Para compatibilizar con el sistema de archivos **Mac**, Windows dispone de la característica **Alternate Data Strings** (**ADS**). El peligro de esta funcionalidad es que, a partir de una vulnerabilidad conocida, un usuario podría crear ADS y esconder un código malicioso en ellos.

va a recolectar el spyware. Pero, si no prestamos atención al contrato de licencia, difícilmente tomemos conocimiento de la instalación del software indeseado (**Figura 4**).

Adware y spyware **en funcionamiento**

La idea central del spyware es ayudar a focalizar promociones de ventas, al utilizar la información provista por la amenaza para individualizar el material. Mientras el spyware se encarga de clasificar los hábitos de consumo del usuario, el adware le acerca a éste los productos que probablemente quiera comprar (**Figura 5**).

Los productores de adware alegan que lo que ellos hacen es legal, ya que les ofrecen a los consumidores productos que, en realidad, podrían interesarles. Los instaladores de spyware se cubren diciendo que, en tanto los usuarios son tratados de forma **anónima** en la base de datos de la página, no hay violación a la privacidad. Estas posiciones son discutibles, y es una problemática para los consumidores decidir hasta qué punto el mercado puede, o no, entrometerse en sus vidas.

Por otra parte, algunos adware y spyware insisten en cambiar continuamente la página de inicio de los buscadores y muestran todo el tiempo avisos sin criterio aparente (**Figura 6 y 7**). Esta situación hace que los alegatos de los productores de este tipo de programas resulten aún más inverosímiles, y que los usuarios busquen una forma eficaz de eliminarlos de sus computadoras (**Figura 8**).

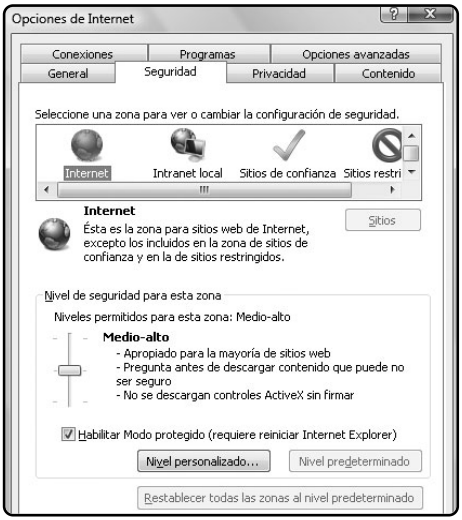


FIGURA 5. Algunos usuarios ni siquiera pueden navegar por los cambios de configuración que ciertos adware hacen en las zonas web.

ADWARE Y SPYWARE EN LINUX

Los adware y spyware no diferencian entre sistemas operativos y atacan indiscriminadamente a usuarios de Windows y Linux. Por eso, debemos contar con una buena protección contra ellos y un navegador seguro, para que los sitios poco confiables no arruinen el equipo.

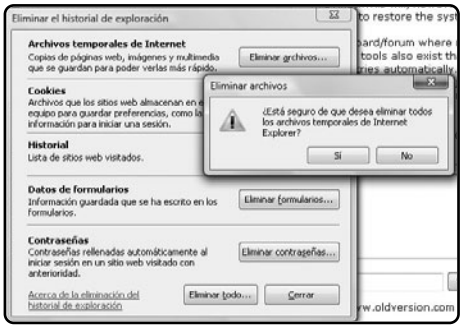


FIGURA 6. De no eliminar los archivos temporales, correríamos el riesgo de que todas las amenazas volvieran a instalarse.

FIGURA 7. Si deseamos buscar una alternativa a Internet Explorer, podemos probar las ventajas de seguridad de Mozilla Firefox.

FIGURA 8.
Los programas removedores de spyware se han vuelto, en los últimos tiempos, tanto o más importantes que los antivirus. Los analizadores en línea, por ejemplo, cobran por eliminar adware, pero no por limpiar virus.

DISCADORES

Los spyware pueden también crear ciertos fraudes conocidos como **discadores**. Estos fraudes representan un riesgo solo para aquellos usuarios que utilicen conexiones **dial-up**, y se encargan de crear una conexión telefónica con un número de larga distancia.

ADWARE Y SPYWARE EN AMÉRICA LATINA

A esta lógica de apertura de ventanas y avisos que tienen algunos adware, se le suma la imposibilidad de ciertos spyware de clasificar determinados datos. Con esto nos referimos, de manera específica, a lo siguiente: muchos adware y spyware están pensados para funcionar en mercados particulares con lógicas de articulación también muy específicas, como por ejemplo, el **norteamericano**, el **europeo** o algunos **asiáticos**.

Pero en los mercados más inestables o con consumos menos catalogables, como el **latinoamericano** o el de **Europa del Este**, las estrategias de focalización fallan, y no hay forma de enviar avisos muy específicos a los usuarios devenidos en consumidores. En ese caso, la estrategia de los adware y spyware es enviar avisos que consideran que pueden resultar interesantes a cualquier usuario. El criterio suele consistir en mostrar, de manera indiscriminada, publicidades de sitios asociados al juego y los casinos en línea, o directamente avisos de corte pornográfico (**Figura 9**).

DIFERENCIAS ENTRE ADWARE, SPYWARE Y VIRUS

En el **capítulo 2** de este libro, aprendimos que los adware y spyware no pueden ser considerados un tipo de virus. Mientras un virus es un pequeñísimo programa, o unas líneas de código adosadas a otro programa, y que puede reproducirse, lejos de eso,

FIGURA 9.
Los sitios ofrecidos por los spyware suelen intentar infectarnos con más spyware en cuanto los visitamos. Debemos evitarlos y contar con un navegador que resulte seguro.

EL ADWARE Y LOS MERCADOS

En los mercados desarrollados, son muchas las empresas dispuestas a invertir en adware, por lo que los productos que se ofrecen son variados. En los mercados emergentes, no son tantas las empresas dispuestas a invertir en este tipo de publicidad.

este nuevo tipo de amenaza (adware y spyware) tiene otro fin muy específico, ligado al lucro y la creación de nuevos mercados.

Sin embargo, hay muchas similitudes entre estas amenazas y los virus. De hecho, los adware y spyware siempre intentan esconderse de usuarios y programas removedores para poder seguir trabajando e introduciendo más y más publicidades, así como los virus intentan evitar ser eliminados.

Algunos tipos de malware, como los llamados **Caballos de Troya**, por ejemplo, usan ciertas técnicas para esconderse de las garras de removedores y antivirus que hace más evidente el parentesco entre virus y amenazas del tipo de los adware y spyware. Sin embargo, los programas para remover unos y otros ataques están claramente diferenciados, y solo algunas suites de aplicaciones los incluyen en un mismo paquete. AVG, por ejemplo, ofrece **AVG Internet Security**, una suite completa de protección antivirus y antispyware (**Figura 10**).

Limpiar y proteger el equipo

Si hemos seguido los consejos hasta aquí propuestos, es probable que nuestro equipo no esté infectado por adware y spyware. Sin embargo, si en un descuido fuimos atacados, debemos **limpiar el equipo**.

Además, aunque no hayamos sufrido ningún ataque, es necesario **instalar una protección** en la computadora, para que se encargue de vigilar que ninguna amenaza pueda afectar el rendimiento de nuestra PC, ni representar un riesgo de seguridad.

Es importante tener en cuenta que los adware y spyware, a diferencia de los virus, no están diseñados con propósitos de vandalismo. En muchos casos, es probable que se registren con normalidad en el sistema, como cualquier otro programa instalado y que, incluso, presenten un desinstalador en la lista de **`Programas y características`** de Windows.

FIGURA 10.
Norton 360 es la alternativa que ofrece Symantec como solución integral para mantener la seguridad contra virus y espías en la PC. Se puede descargar desde www.symantec.com/es/mx/norton/360.

Para saber si tenemos un espía instalado en nuestra PC, en primera instancia, abriremos la lista **Agregar y quitar programas** desde **Inicio/Panel de control/Programas y características**.

En ella, buscaremos la presencia de adware y demás amenazas conocidas (**Figura 11**). De no encontrar ningún espía ni elemento sospechoso allí, utilizaremos métodos más radicales, como por ejemplo, herramientas específicas para esta finalidad, tal es el caso de **Spybot Search & Destroy**.

Hace algunos años, la aplicación recomendada para eliminar adware y spyware de manera rápida y fácil era el programa **Lavasoft Ad-Aware**. Sin embargo, a partir de su versión 2007, la calidad del producto decayó notablemente, y su uso ya no es recomendado, al existir otras herramientas mucho más eficaces (**Figura 12**).

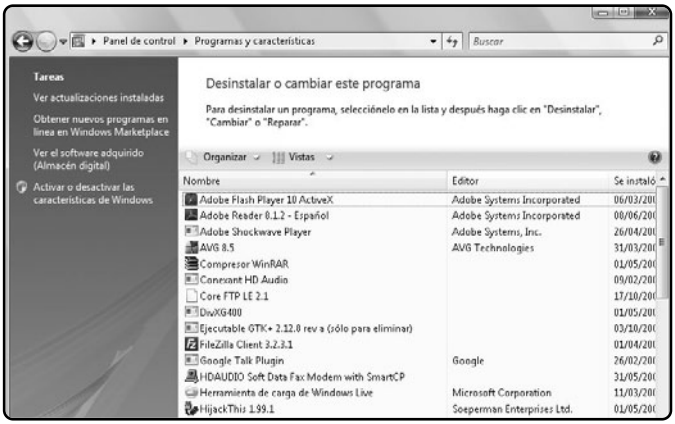


FIGURA 11.
Una importante cantidad de adware, además de presentarse en el contrato de licencia, también se registra para ser eliminado como cualquier otro programa, desde las opciones de Microsoft Windows para desinstalación.

CUIDADO AL DESINSTALAR

Cuando instalamos un programa **adware-supported**, en la lista de **Programas y características** del **Panel de control** suele sumarse el adware. Al desinstalar el programa, es necesario también desinstalar el adware, ya que de otro modo nuestro equipo seguirá infectado.

FIGURA 12.
El programa Ad-Aware ya no presenta la misma eficiencia que antes, pero quien desee protección en un producto muy fácil de usar, puede descargarlo desde www.lavasoft.com/products/ad_aware_free.php.

INSTALAR SPYBOT SEARCH & DESTROY

El programa que analizaremos en este apartado para proteger la PC de adware y spyware es Spybot Search & Destroy. Es una aplicación muy potente y tiene varios años de desarrollo, lo que nos asegura su confiabilidad y rendimiento. En primer lugar, lo que haremos será descargar la herramienta desde la página web de la empresa que la diseñó: **Safer Networking, Inc**. El enlace para acceder a ella es **www.safer-networking.org/es/mirrors/index.html**. Allí podremos cambiar el idioma de la página haciendo clic en la bandera española en el margen derecho de la pantalla.

Recomendamos descargar el software directamente desde un servidor de la empresa, para lo que haremos clic en el vínculo **`Servidor N.°1`** del apartado **`Hosted by Safer-Networking`**.

ATAQUES DoS

Los ataque *denial of service* (negación del servicio), también llamados DoS, direccionan los navegadores de varias computadoras a un mismo sitio web con el objetivo de colapsar el servidor. Esto impedirá que otros usuarios bienintencionados de ese sitio puedan acceder a él.

Siempre será bienvenida toda donación que queramos hacer para los programadores. El vínculo **Donación** nos permitirá colaborar con el equipo de desarrolladores de Spybot. El tamaño del archivo es de alrededor de 16 MB, y el tiempo de descarga dependerá de la conexión (**Figura 13**).

FIGURA 13. Debemos hacer clic en `Guardar` para disponer siempre del instalador de Spybot.

Instalación eficaz

La instalación de Spybot, aunque es muy simple, merece atención por parte del usuario en tanto algunos de los parámetros que allí se definen pueden hacer variar ostensiblemente el nivel de seguridad que ofrece el producto. De hecho, algunos aspectos de la configuración son muy complejos de modificar si no se llevan a cabo durante la instalación. Y para que ésta finalice de manera correcta, hay que contar con una conexión a Internet funcional, por lo que antes de ejecutar el archivo descargado, si no contamos con una conexión permanente, debemos conectarnos (**Figura 14**).

En el **Paso a paso 1**, veremos cómo completar de manera exitosa y eficaz la instalación del programa. Si hemos descargado el instalador del sitio

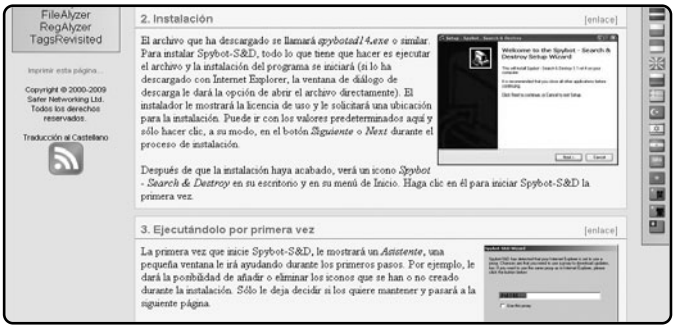


FIGURA 14. Aunque no está documentado en el sitio, la instalación de Spybot no puede concluir si la conexión a Internet no funciona.

TÉRMINOS DE USO

Las licencias de aquellos productos de tipo comercial producidos por grandes empresas son de carácter informativo y apuntan a evitar la piratería. Jamás deberíamos dejar de leer las licencias de programas de origen dudoso, o de descarga gratuita.

oficial, no debemos dudar en aceptar las advertencias de seguridad del software de terceros que pudiéramos tener instalado, ya que el archivo es seguro.

Al finalizar la instalación del programa, notaremos que un nuevo icono se ha instalado en la zona de notificación de la barra de tareas. Es el **componente residente** de Spybot. Si dejamos el mouse sobre él un segundo, veremos estadísticas de la cantidad de entradas de la base de datos de definiciones que se encuentran en ese momento. Un doble clic sobre él abrirá la ventana principal del programa y nos permitirá llevar adelante el análisis del sistema e inoculaciones. A continuación, aprenderemos a ejecutar todas estas tareas para que, junto con aquellas otras que ya aprendimos y con las que aprenderemos en los restantes capítulos, nos podamos convertir en auténticos expertos de la seguridad informática hogareña.

PRIMERA EJECUCIÓN

La primera vez que ejecutemos Spybot Search & Destroy, nos encontraremos con un asistente que nos ayudará a elevar el nivel de protección del sistema antes de analizarlo en busca de adware y spyware.

Completarlo es muy importante porque colaborará en la preparación del registro de modo que, si alguna vez sufrimos una infección, las consecuencias de ella sean mínimas (**Figura 15**).

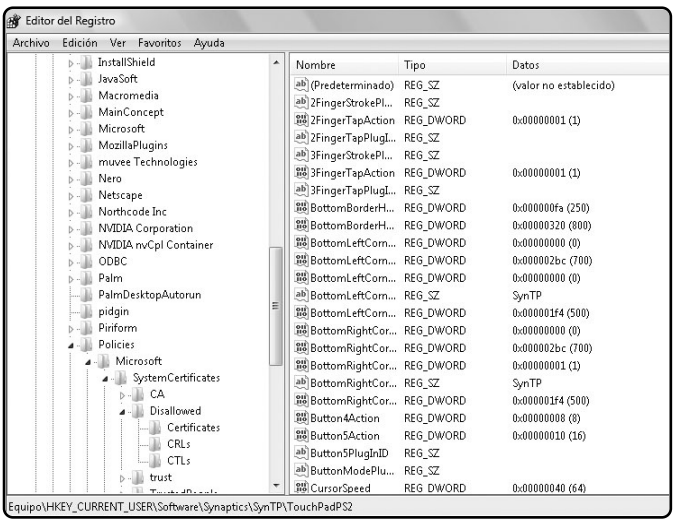
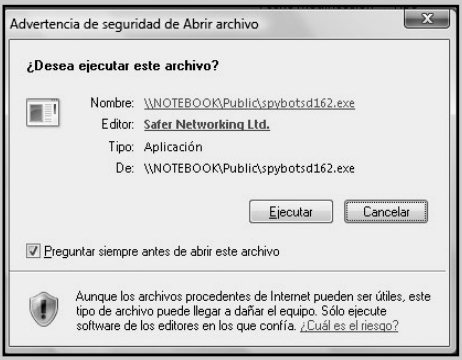


FIGURA 15.
El Registro de Windows es el primer componente del sistema atacado por los adware y spyware. Acorazarlo antes de sufrir un ataque es una buena idea.

PASO A PASO /1
Instalar Spybot S&D

1



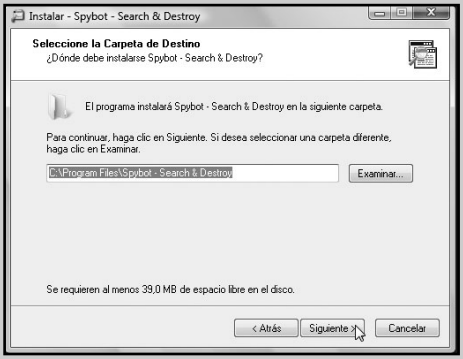
Ejecute el archivo que ha descargado previamente. Luego, haga clic en el botón que corresponde para confirmar la advertencia de seguridad de Windows.

2

Seleccione **`Español`** en el cuadro **`Seleccione el idioma de la Instalación`** y presione **`Aceptar`**. A continuación, pulse **`Siguiente`** en la pantalla de bienvenida de la instalación.

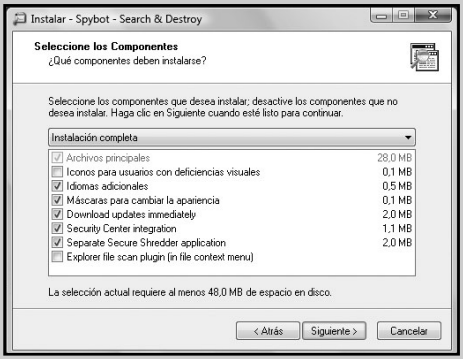
PASO A PASO /1 (cont.)

3



Luego de leerlo, seleccione **Acepto el acuerdo** y presione **Siguiente** para aceptar el contrato de licencia. Seleccione una carpeta de destino o acepte la predeterminada con **Siguiente**.

4



Acepte las opciones por defecto en el cuadro **Seleccione los componentes** presionando **Siguiente**. Luego pulse **Siguiente** en el cuadro **Seleccione la Carpeta del Menú Inicio**.

PASO A PASO /1 (cont.)

5

Para incrementar el nivel de protección del equipo, seleccione todas las opciones del cuadro **`Seleccione las Tareas Adicionales`**. En el siguiente cuadro, presione el botón **`Instalar`**.

6

Se iniciará la descarga de componentes actualizados. Una vez finalizada, seleccione todas las opciones de este cuadro para iniciar en forma automática el sistema de protección y, por último, presione **`Finalizar`**.

Primer paso:
crear una copia de seguridad del registro

El primer paso sugerido por el asistente consiste en crear una copia de seguridad del registro del sistema (**Figura 16**). Hacer esto nos permitirá sentirnos seguros ya que, si alguna vez algo sale mal, podremos simplemente reponer la copia de seguridad y todo volverá a la normalidad.

Para llevar a cabo esta copia, hacemos clic sobre el botón **Crear copia de seguridad del registro**. Luego presionamos **Siguiente**.

FIGURA 16. Hacer una copia de seguridad nos evitará reinstalar el sistema operativo ante un ataque certero.

Segundo paso:
conseguir nuevos archivos de definiciones

Contar con archivos actualizados de definiciones es central para que la búsqueda y remoción de adware y spyware resulte efectiva; por lo tanto, no podemos obviar este paso. Comenzaremos la búsqueda haciendo clic en **Buscar actualizaciones**; esto nos llevará a la ventana del actualizador automático. Allí presionamos **Continue**. De las opciones disponibles, además de las que el sistema eligió sin preguntarnos, podremos seleccionar todas aquellas que hagan referencia al idioma español en la sección **Other files**. Una vez que esté todo listo, presionamos **Download** y, ya descargadas las actualizaciones, volveremos al asistente con el botón **Exit** (**Figura 17**).

CENTRO DE SEGURIDAD DE WINDOWS

Si, como sugerimos, instalamos AVG AntiVirus antes que Spybot, en el Centro de seguridad de Windows, no se hará referencia a la segunda de las aplicaciones en la sección **Protección contra malware**. Sin embargo, el programa supervisará el funcionamiento del antispyware.

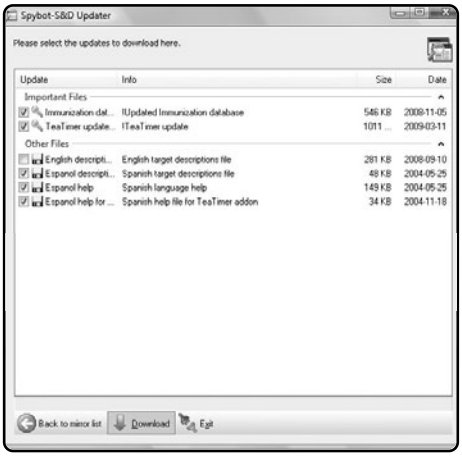


FIGURA 17. Los archivos de ayuda en español también pueden ser descargados al mismo tiempo que las actualizaciones de definiciones.

En equipos que corran Windows Vista, el asistente habrá terminado. Estamos ahora en condiciones de usar el programa, que incluso trabaja en conjunto con el Centro de seguridad de Windows para avisarnos si requiere una actualización o si hace demasiado tiempo que no se realiza un análisis completo del sistema.

No olvidemos que es recomendable siempre buscar un nuevo archivo de definiciones antes de cada análisis del sistema.

ANALIZAR EL SISTEMA

Cuando abramos Spybot S&D, veremos la pantalla principal del programa desde la cual ejecutaremos todas las tareas de seguridad. En la **Guía visual 1**, aprenderemos más sobre la pantalla principal y, en cuanto terminemos de leerla, presionemos el botón **`Analizar problemas`** para comprobar que nuestro equipo no esté infectado por algún adware o spyware.

El analizador del sistema

Al presionar el botón **`Analizar el sistema`** (**punto 2** de la **Guía visual 1**), de manera automática, Spybot buscará infecciones en el equipo, comparando las entradas disponibles en su base de datos de definiciones con las instaladas en el registro del equipo. Si se encontrase una importante cantidad de archivos temporales y cookies entre los archivos temporales de Internet, nos pedirá, en inglés, permiso para eliminarlos. Responderemos **`YES`**.

Durante el análisis, aparecerá la pantalla principal del analizador, desde la cual podemos llevar a cabo algunas acciones mientras analizamos el equipo. En la **Guía visual 2**, veremos cuáles.

En el estado extendido, podremos ver con precisión cuál de todas las amenazas de la base de datos de definiciones se está buscando en el momento.

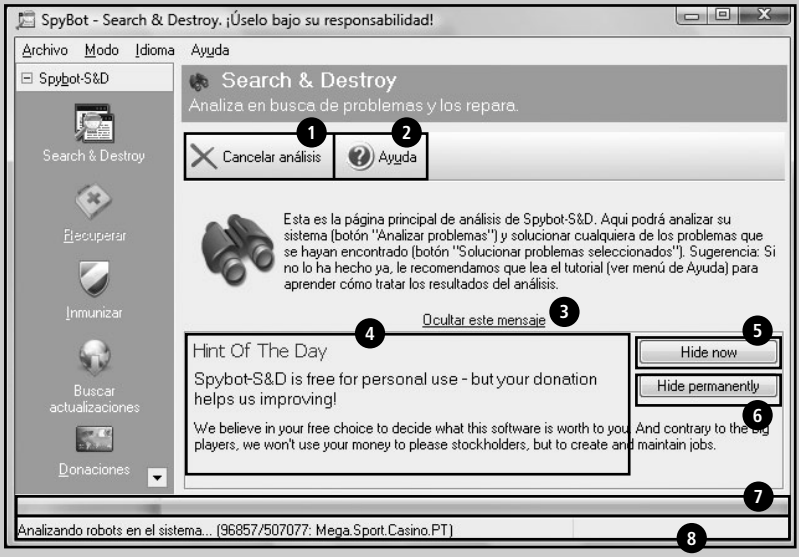
NAVEGADOR Y CLIENTE DE CORREO MOZILLA

Si los adware y spyware resultan un problema, podemos probar la suite **Mozilla**, que incluye el navegador **Firefox** y el cliente de correo **Thunderbird**. Esto puede ayudarnos en la lucha contra las amenazas tecnológicas. Se puede obtener desde **www.mozilla-europe.org/es**.

GUÍA VISUAL /1
La pantalla principal de Spybot S&D

1. Barra de menús.
2. Inicia el análisis en busca de problemas.
3. Inicia el gestor de recuperación del sistema, que vuelve el registro a estados anteriores si, luego de una desinfección, algo funciona mal.
4. Inicia el gestor de actualizaciones.
5. Abre la página web del fabricante de Spybot para recibir donaciones.
6. Inmuniza el registro del sistema contra ataques conocidos.
7. Muestra la pantalla principal del analizador de problemas del equipo.
8. Muestra la pantalla principal de Spybot S&D.

GUÍA VISUAL /2
La pantalla del analizador



1. Cancela el análisis en curso.
2. Muestra la ayuda sobre el análisis.
3. Oculta el mensaje descriptivo de la pantalla principal y muestra, en cambio, detalles útiles sobre las amenazas encontradas.
4. Ventana de consejos del día (solo disponible en idioma inglés).
5. Esconde los consejos del día.
6. Evita que se vuelvan a mostrar los consejos del día.
7. Muestra el progreso del análisis que, en algunos equipos, puede durar varias horas.
8. Muestra en tiempo real el estado extendido del análisis y la amenaza que se está buscando.

Desafortunadamente, por las características del motor de búsqueda de Spybot, mientras más componentes tiene la base de datos de definiciones, más tiempo toma el análisis, que en equipos inmunizados no debería demandar más de veinte minutos.

Terminada la revisión, el programa nos mostrará una pantalla con los resultados obtenidos. Las amenazas aparecerán en una tabla que indicará su nombre y su tipo. Por defecto, todas se mostrarán seleccionadas. Alcanzará con presionar el botón **Solucionar problemas seleccionados** (**Figura 18**) para eliminar todos los problemas del equipo en lo que a adware y spyware se refiere. Podemos también imprimir una lista de los problemas disponibles con el botón homónimo o volver a analizar el equipo con **Analizar problemas**.

Recuperar una reparación

Al ejecutar una reparación, algunos programas **adware-supported** pueden dejar de funcionar. Esto tiene que ver con que varias de estas aplicaciones, en tanto se financian con la inclusión de adware en sus instalaciones, por contrato no pueden funcionar si no está instalada también la aplicación de publicidad.

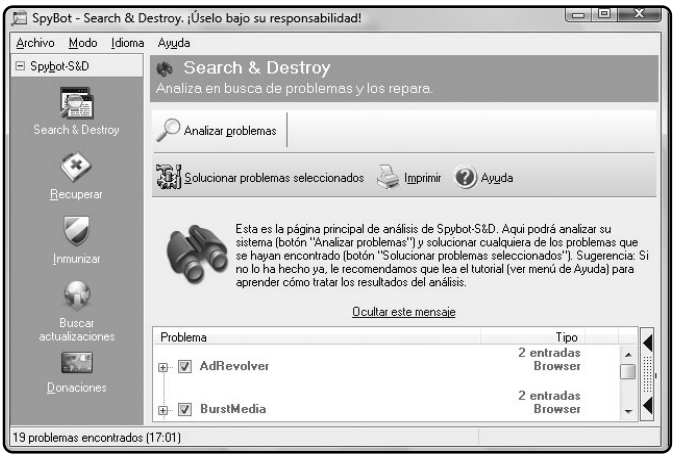


FIGURA 18.
La barra de estado indica la cantidad de amenazas encontradas y el tiempo que tomó el análisis.

CONSEJOS DE SPYBOT

Aunque se encuentran en inglés, los consejos de Spybot dan buenas ideas para utilizar el programa y evitar infecciones repentinas. Los lectores hispanohablantes encontrarán más información sobre el tema en **http://wiki.spybot.info/index.php/Main_Page**.

En el caso de que sea necesario seguir ejecutando la aplicación independientemente de la amenaza y, por lo tanto, haya que volver atrás la limpieza del sistema, podemos utilizar la herramienta **Recuperar** de Spybot. Con ella recuperaremos las claves de registro que el analizador del sistema eliminó en las últimas pasadas (**Figura 19**).

El proceso de recuperación es muy simple. Para llevarlo a cabo, en la pantalla principal de Spybot, presionamos el botón **Recuperar**, que nos llevará a la pantalla principal de **Recuperar**. Allí, encontraremos una lista de las amenazas eliminadas que pueden ser restauradas sin representar un riesgo importante para el equipo (**Figura 20)**. Debemos tildar cada una de las que queremos recuperar (si presionamos el signo **+** a la izquierda de cada una, podremos incluso seleccionar las claves componentes a ellas) y luego presionar **Recuperar los productos seleccionados**. De esa manera, tendremos solucionado muy rápido el problema generado por el analizador.

INMUNIZAR EL SISTEMA

La aplicación llamada Spybot Search & Destroy (**Figura 21**), ofrece una posibilidad muy interesante, la de **inmunizar** el sistema.

FIGURA 19.
La herramienta de recuperación funciona con claves de adware instalados por productos adware-supported. Para proteger el sistema, no permite recuperar instalaciones de spyware o adware instalados sin consentimiento del usuario.

REAPLICAR LA INMUNIZACIÓN

Es imprescindible volver a inmunizar el sistema luego de actualizar la base de datos de definiciones. En principio, porque las nuevas definiciones ofrecen un mayor nivel de protección, pero además porque, al utilizar el equipo, aumenta la cantidad de elementos por proteger.

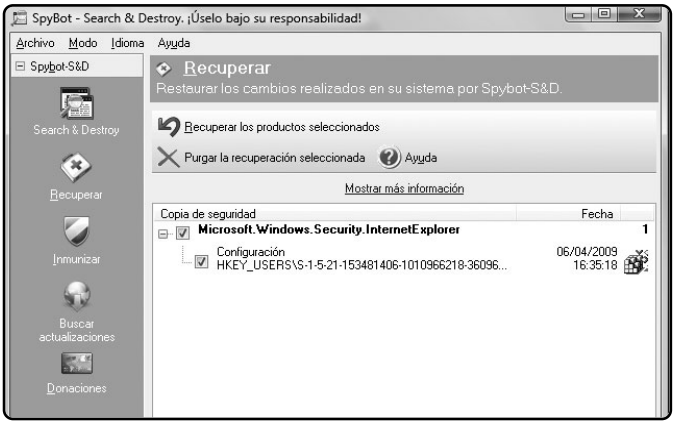


FIGURA 20. Si hacemos clic en el vínculo `Ocultar este mensaje`, tendremos mayor espacio para visualizar la lista de amenazas por recuperar. Volveremos a ver el mensaje si hacemos clic en `Mostrar más información`.

FIGURA 21. Mientras mayor sea el número de pasadas, tendremos más seguridad. El número por defecto (6), sin embargo, es suficiente.

La inmunización consiste en la modificación de algunos parámetros de configuración de los navegadores, que aseguren que las descargas por ellos llevadas a cabo y la instalación de plugins externos no represente un peligro para el equipo (**Figura 22**).

La inmunización protege en especial, tres aspectos de todo navegador. El primero es la instalación de controles **ActiveX** malignos. Luego de la inmunización, que debe repetirse cada vez que se actualiza el archivo de definiciones, ningún control ActiveX considerado maligno podrá ser instalado. El segundo corresponde a las descargas maliciosas.

SPYBOT ES UN PRODUCTO FREEWARE

Spybot Search & Destroy se distribuye bajo licencia **freeware**, lo que implica que el programa es gratuito y que el programador acepta donaciones. Sus productores apoyan el software libre, y su posición puede leerse en el apartado **`Licencia`**.

FIGURA 22.
Si utilizamos un equipo compartido, eliminar los registros de uso es una buena idea.

Cada archivo de definiciones incluye una lista de descargas peligrosas, que serán bloqueadas por el navegador si la inmunización ha sido aplicada. Por último, la inmunización evitará los cambios de ciertos aspectos puntuales del navegador, como el archivo de **hosts** en el cual se anotan los servidores seguros. Una vez inmunizado el sistema, la seguridad del navegador se habrá incrementado en forma considerable.

La primera vez que hagamos clic sobre **`Inmunizar`**, se nos recomendará cerrar todos los navegadores antes de continuar. Cerrados éstos, el inmunizador analizará el sistema y nos propondrá una serie de aspectos por proteger. A menos que sepamos que alguna aplicación requiere otra específica, aceptaremos las recomendaciones e iniciaremos la inmunización con el botón **`Inmunize`**. Si una vez aplicada la inmunización algo sale mal, podemos deshacer los cambios presionando el botón **`Undo`** del cuadro **`Inmunizar`**.

RESUMEN

En este capítulo, hemos aprendido algo fundamental en nuestra carrera por convertir a la computadora en una fortaleza: cómo protegerla de las más molestas y comunes amenazas, los adware y spyware. Para ello, utilizamos el software antiespías, Spybot Search & Destroy.

Multiple **choice**

1 ¿Cómo se llama el programa que envía publicidad no deseada?

a- Virus.
b- Spyware.
c- Adware.
d- Ninguna de las anteriores.

2 ¿En qué sitio podemos encontrar versiones anteriores y funcionales de software?

a- Smileys.
b- Oldversion.
c- GNU.
d- Ninguna de las anteriores.

3 ¿Cuál es la finalidad de la amenaza llamada spyware?

a- Acercar publicidad.
b- Ayudar a focalizar promociones de ventas.
c- Dañar el equipo.
d- Ninguna de las anteriores.

4 ¿El adware y spyware pueden atacar Linux?

a- Sí.
b- No.
c- Depende de la versión.
d- ¿Qué otra opción podría haber?

5 ¿Qué excelente alternativa existe a Internet Explorer?

a- Netscape.
b- Blackberry.
c- Mozilla.
d- Ninguna de las anteriores.

6 ¿Qué cliente de correo puede ayudarnos en la lucha contra las amenazas tecnológicas?

a- Netscape.
b- Blackberry.
c- Mozilla.
d- Thunderbird.

Respuestas: 1c, 2b, 3b, 4b, 5c, y 6d.

Capítulo 4

Tercer paso: blindar el equipo

Analizaremos en detalle
las distintas opciones y posibilidades
de configuración de firewall.

En los primeros capítulos de este libro, hemos visto la manera de protegernos de amenazas automatizadas, es decir, de aplicaciones programadas para atacar nuestro equipo.

Aprenderemos ahora a proteger la computadora no solo de ataques digitales, sino de usuarios malintencionados que intenten destruir la integridad de nuestros datos o acceder a ellos sin autorización. Para esto, analizaremos en detalle cómo incluir actualizaciones de sistema y las distintas opciones de configuración de firewall, que nos ayudarán a estar más seguros.

Protección **imprescindible**

Ha llegado el momento de elevar el nivel de la protección al punto donde no llega ni el antivirus ni cualquier removedor de spyware.

Podría decirse que más del 50% de las amenazas que rondan el ciberespacio son gusanos o programas maliciosos que intentan, en forma constante, de entrar en cuanta computadora les sea posible. En este sentido, tanto virus como adware, spyware y malware comparten una misma forma de trabajo: todos ellos buscan introducirse en la mayor cantidad de equipos. Si bien la efectividad de los antivirus, y de los removedores de adware y spyware está comprobada, la necesidad de alguna herramienta que frene (o reduzca) la posibilidad de ataques, antes de que tenga que actuar el antivirus u otro método de acción pasiva, se vuelve imprescindible (**Figura 1**).

Aquí es donde la instalación del **firewall** es indispensable: no podemos permitir que nuestro equipo esté expuesto a cualquier ataque si tenemos en cuenta la sensibilidad y cantidad de datos que alberga.

En otros tiempos, pensar en la posibilidad de que alguien se metiera en nuestro equipo era un

SITIOS PELIGROSOS

Muchos sitios de descargas ofrecen servidores de seguridad gratuitos y en apariencia muy fáciles de utilizar. Pero, en la mayoría de los casos, estos programas incluyen adware y spyware en el mismo firewall, lo que convierte a la aplicación en algo completamente inútil.

absurdo, o una problemática de paranoicos o ideas de aficionados a la **ciencia ficción**.

Hoy, esta posibilidad es real y efectiva si no se mantiene la computadora protegida de manera total. Y en este punto, no hay antivirus que resulte efectivo. La necesidad de una protección contra intrusos humanos y cibernéticos, en la computadora de la casa o de la oficina, está plenamente justificada frente a las posibles amenazas.

LAS ACTUALIZACIONES DE WINDOWS

Antes de pensar qué firewall utilizaremos y cómo debemos configurarlo para que su nivel de protección sea efectivo, debemos asegurarnos de contar con las últimas actualizaciones disponibles para el sistema operativo. Como ya vimos en capítulos anteriores, ninguna protección es efectiva si las diferentes **actualizaciones** del sistema no están instaladas como es debido.

FIGURA 1.
Antivirus y antispyware no son suficientes hoy en día: además de una constante actualización del software del equipo, es fundamental contar con otro método que limite los ataques.

FIREWALL POR HARDWARE EN EL HOGAR

Quienes quieran más protección que la sola instalación de un firewall personal, deben saber que, si disponen de un router en su casa para compartir la conexión a Internet, poseen también un firewall por hardware. En el próximo capítulo, aprenderemos a configurarlo.

Windows Update es el programa que nos ayudará a mantener actualizado el sistema. Accederemos a él haciendo clic en **`Inicio/Todos los programas/Windows Update`**. Si todo funciona bien y tenemos el sistema al día, el programa nos indicará que no hay nuevas actualizaciones por instalar. Si la opción **`Actualizaciones automáticas`** está activada de manera automática, las nuevas descargas de seguridad serán aplicadas. Sin embargo, podemos hacer clic en el vínculo **`Buscar actualizaciones`** de la pantalla principal del programa para eliminar cualquier duda al respecto (**Figura 2**).

LOS SERVICE PACKS

Un **service pack** es un paquete contenedor de una cantidad importante de actualizaciones. Si bien la teoría parece indicar que éstas pueden ser instaladas en forma, cuando una compañía lanza al mercado un service pack, suele ser necesaria su instalación completa ya que, por lo general se incluyen, junto con las actualizaciones acumulativas, mejoras globales para el sistema operativo.

Estos paquetes, entonces, además de contener todas las actualizaciones disponibles para el sistema

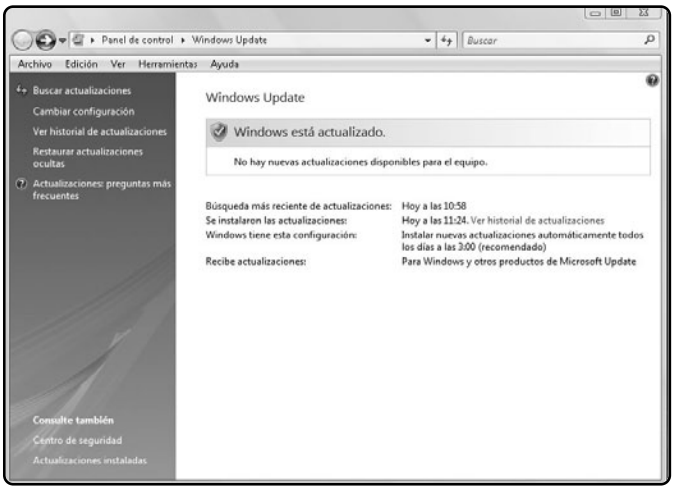


FIGURA 2.
Un sistema operativo actualizado es la base de cualquier protección frente a intrusiones. Windows Update **nos permite lograrlo de una manera simple con las** Actualizaciones automáticas**.**

PRIMERA VERSIÓN DE WINDOWS VISTA

La primera versión de Windows Vista tenía problemas de seguridad y una amplia gama de problemas de rendimiento. Éstos fueron solucionados en el paquete de actualizaciones **SP1** (que mejora el funcionamiento del sistema operativo). En mayo de 2009, se lanzó el **SP2**.

operativo al momento de su lanzamiento, incluyen mejoras de seguridad solo disponibles luego de su instalación. Es común que, después de transcurrido un tiempo de su lanzamiento, las actualizaciones posteriores solo puedan ser instaladas en equipos que dispongan de esas mejoras (**Figura 3**).

Si por alguna razón **Actualizaciones automáticas** está desactivado, es necesario descargar antes los paquetes de servicio para instalarlos en el equipo. Las copias de Windows compradas luego del lanzamiento de cada service pack los incluyen por defecto. Los instaladores de estos paquetes de servicio pueden descargarse de sitios como **Download** (**http://download.cnet.com/windows**) o, directamente, desde el sitio de descargas para Microsoft Windows, **http://update.microsoft.com**.

Una vez que hayamos confirmado, por los medios ya estudiados, que disponemos del último service pack y de las últimas actualizaciones, estaremos en condiciones de adentrarnos en la configuración del firewall.

EL FIREWALL

Con el equipo actualizado, nos encontramos en condiciones de configurar una protección contra intrusiones que nos brinde seguridad. En los días que corren es tan alto el nivel de ataques, que

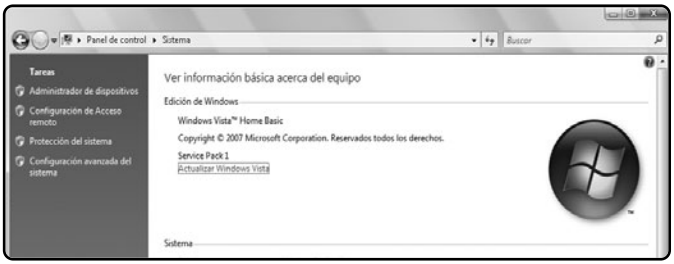


FIGURA 3.
En el ítem `Centro de Bienvenida` **del** `Panel de Control` **hacemos clic en** `Mostrar más detalles` **para conocer las actualizaciones.**

ZONEALARM

Entre los firewalls personales fabricados por terceros, **ZoneAlarm** es de los que gozan de mayor prestigio. Altamente confiable y de mediana complejidad en su uso, es una alternativa válida. Puede conseguirse en la sección de descargas de **www.zonealarm.com**.

resulta impensable ejecutar un sistema operativo **Windows** sin una protección de este tipo. Caer en una imprudencia tan grande podría derivar en una infección automática con virus, troyanos y millones de adware y spyware. Es aquí donde entra en juego el **firewall**, cuya importancia es tal que, aun aquellos sistemas operativos para los que casi no existen virus (como **Linux** o **BSD**), cuentan con uno por defecto (**Figura 4**).

Un firewall es un componente que tiene la función de prevenir comunicaciones y tráfico de datos. Existen por software, es decir, aplicaciones que controlan este tráfico; y por hardware, dispositivos dedicados al control. Su nombre es traducido al castellano como **pared de fuego** o **cortafuegos**.

Esta denominación, grafica claramente su accionar: un firewall actúa imponiendo un límite no traspasable entre dos o más equipos. En una computadora hogareña o de pequeña oficina, un firewall tiene la importantísima tarea de evitar que cualquier persona o código no autorizado tenga acceso a una computadora.

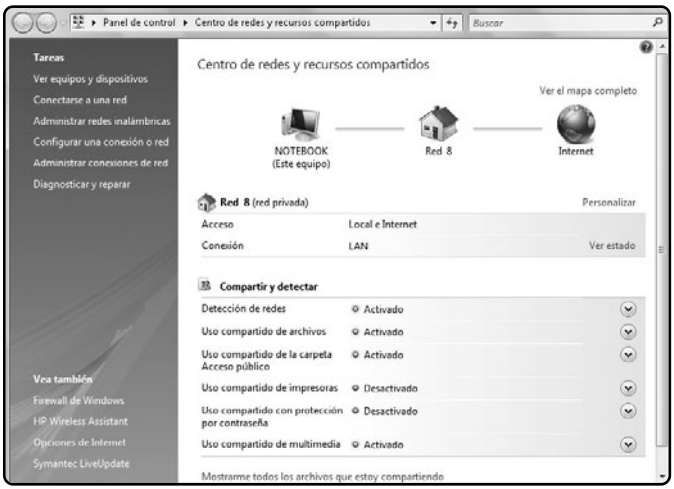


FIGURA 4.
Un firewall protege, además de los ataques vía Internet, la integridad y el acceso a la red local.

DESACTIVAR EL FIREWALL DE WINDOWS

Una PC debería tener por defecto el firewall activado, conocido como **servidor de seguridad.** El único caso en que un usuario podría querer desactivar el firewall de Windows se da cuando ha elegido otra opción para protegerse (como un firewall profesional o de otra compañía).

Existen varios tipos de firewall, desde simples programas hasta complejos dispositivos de hardware encargados de controlar la comunicación en una red. Para proteger el equipo de nuestro hogar, utilizaremos lo que se denomina **personal firewall** o **cortafuegos personal**. Es decir que instalaremos programas dedicados a la seguridad contra intrusiones, pero no dispositivos de hardware (**Figura 5**).

Un firewall tiene la tarea básica de controlar el tráfico entre equipos con diferentes zonas de seguridad. En una computadora conectada a una red, existen áreas con distintos niveles de seguridad y, como mínimo, se distingue la zona **Internet** (ampliamente insegura) y la zona de **red local**, de probada seguridad. Un firewall efectivo debería proveer conectividad absoluta entre todas las zonas filtrando los riesgos de seguridad propios de cada una.

El **service pack 1** de Windows Vista, **Windows XP SP2**, y las versiones posteriores incluyen un potente y configurable firewall activado por defecto en todas las conexiones de red. Cabe aclarar en este punto que, a partir de la versión XP de

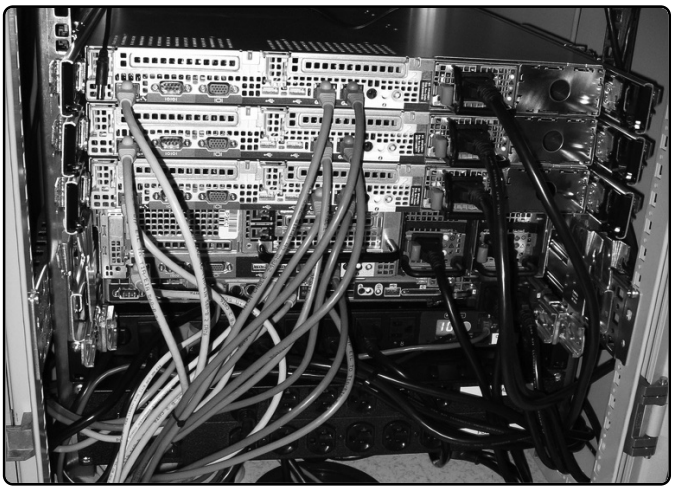


FIGURA 5.
Los firewalls por hardware se usan solo en grandes empresas. Sin embargo, los pequeños routers utilizados en casas y oficinas suelen incluir uno.

COMODO Y EL FIREWALL DE WINDOWS

Comodo Internet Security puede interactuar con el **firewall de Windows**, en cuanto está diseñado para convivir con él. Pero, cuando utilicemos Comodo, el firewall de Windows no interactuará con el usuario, ya que será administrado por el producto de terceros.

Windows, la seguridad contra intrusiones se aplica a cada conexión de red. Versiones de Windows anteriores incluían un firewall mucho menos potente y con mínimas opciones de configuración, que había que activar en forma manual. Una vez más: si disponemos de alguna de estas versiones de Windows, no podemos olvidar mantenernos actualizados (**Figura 6**).

Windows **Firewall**

El **firewall de Windows**, como dijimos, se activa y configura en forma automática con un nivel de seguridad importante para cada nueva conexión de red que establecemos. Sin embargo, recordemos siempre configurar los accesos a la red, de otro modo, cada vez que algún integrante del grupo de trabajo intente acceder a un documento alojado en nuestra computadora o pretenda utilizar la impresora compartida, el acceso le será denegado (**Figura 7**).

FIREWALL ACTIVADO

Desde la pantalla principal del Firewall de Windows (disponible en el ítem **`Firewall de Windows`** del **`Panel de Control`**), podremos activar o desactivar el servidor de seguridad así como también afectar o

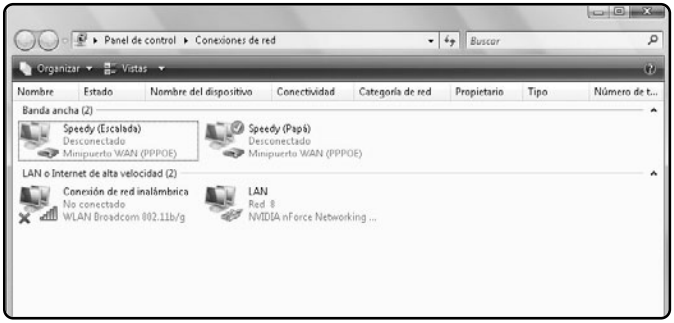


FIGURA 6.
Aunque ya no está el icono del candado, todas las conexiones de red por defecto funcionan con el firewall activado.

ASISTENTE PARA CONFIGURAR LA RED EN XP

Es fundamental para los usuarios de Windows XP, al momento de instalar un nuevo dispositivo de red (como una placa de red **WiFi**), ejecutar el **`Asistente para configuración de red`**, de modo que Windows acomode el firewall a la configuración necesaria de la red.

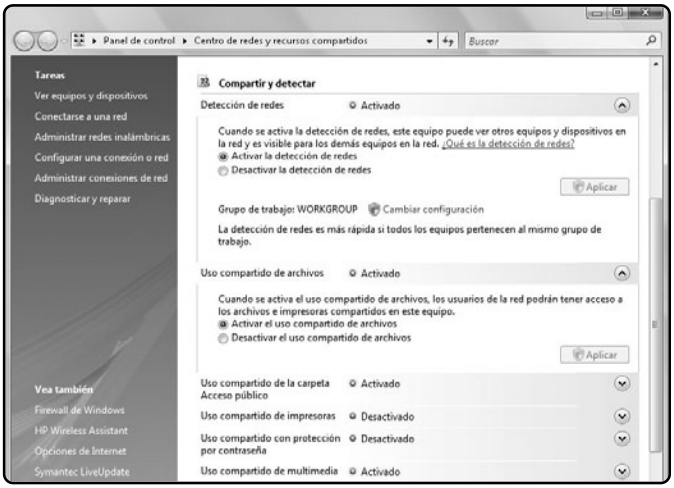


FIGURA 7.
El trabajo que antes hacía el `Asistente para configuración de red` **ahora se ejecuta desde el** `Centro de redes y recursos compartidos`**.**

desafectar el permiso para excepciones. Este último se maneja desde el vínculo **`Permitir un programa a través del Firewall de Windows`** (**Figura 8**).

Una excepción es un permiso otorgado a un programa o a un canal de transmisión de datos (puerto) para que las limitaciones impuestas por el firewall no se apliquen a él. Sin las excepciones, el nivel de seguridad del sistema podría volverse tan alto que el equipo perdería funcionalidad y no se podría ni siquiera, por ejemplo, transmitir archivos vía un mensajero instantáneo como puede ser **Windows Live Messenger**.

Las excepciones solo deben ser denegadas en casos de riesgo muy alto, como al estar conectados en redes públicas de hoteles o aeropuertos. Puede ocurrir también que quieran desactivarse las excepciones en redes donde ninguno de los programas

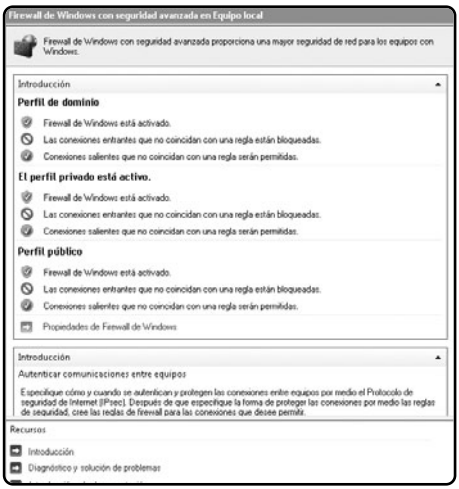


FIGURA 8. Las opciones avanzadas del firewall de Windows ayudan a mejorar el nivel de protección del equipo, aunque existen opciones más eficaces.

utilizados requiere conexión con Internet o con redes no seguras en las que es necesario mantener un nivel de seguridad superlativo (**Figura 9**).

En la **Guía Visual 1**, estudiaremos la ventana principal del firewall de Windows.

LAS EXCEPCIONES

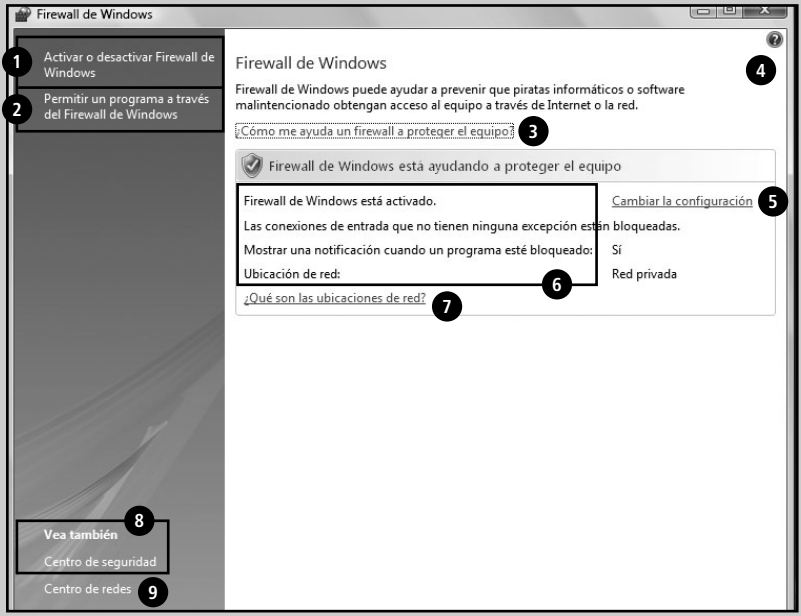
Al agregar un programa a la lista de excepciones, estaremos brindándole permiso total para manejar las conexiones entrantes y salientes con el exterior. Esto que a primera vista no parece deseable, se vuelve imprescindible en algunos programas cuya finalidad es, precisamente, manejar la entrada y salida de datos. Claro ejemplo de estos casos son los clientes de redes punto a punto como **eMule** o **Ares**, además de mensajeros con capacidad de transmisión de archivos o funcionalidades de voz como **Windows Live Messenger**, **Google Talk** o los mensajeros de **Yahoo!** y **Skype**.

Cada vez que un usuario ejecuta por primera vez en un equipo con el firewall de Windows activado un programa que intenta establecer una conexión no permitida, el servidor de seguridad muestra una advertencia y notifica el bloqueo. En esa misma ventana, el usuario puede agregar el programa a la lista de excepciones.

FIGURA 9. Al hacer clic sobre el vínculo `¿Cómo me ayuda un firewall a proteger el equipo?`, nos informaremos sobre el tema.

Ahora bien, no son solo programas los que pueden formar parte de la lista de excepciones. Ya dijimos antes que además podían desbloquearse puertos. ¿Qué es un puerto? Un **puerto** es una conexión mediante la cual los datos son enviados y recibidos. En un ambiente de red, los puertos son números que identifican un servicio en una red. Un puerto famoso y conocido por todos es el **80**, encargado de identificar el tráfico entre servidores web.

GUÍA VISUAL /1
Firewall de Windows

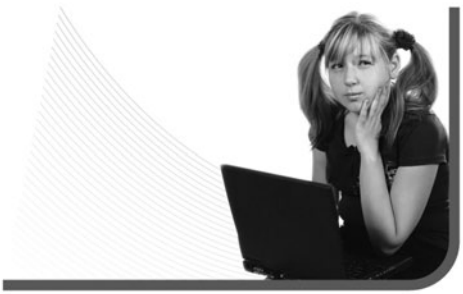


1. Abre la ventana de activación y desactivación del firewall.
2. Abre la ventana de configuración de excepciones.
3. Muestra una ventana de ayuda referida al funcionamiento básico de un firewall.
4. Abre la ayuda de Windows.
5. Cambia la configuración avanzada del firewall de Windows.
6. Muestra el estado básico de configuración del firewall.
7. Muestra una rápida explicación referida a las **`ubicaciones de red`**, un grupo de reglas preestablecidas para el firewall de Windows.
8. Abre el **`Centro de seguridad de Windows`**.
9. Abre el **`Centro de redes y recursos compartidos`**.

Esto quiere decir: siempre que visitemos páginas a través de un navegador, estaremos conectados mediante el puerto 80.

La relación entre los puertos y el servidor de seguridad es, entonces, clara: el firewall debe tener control absoluto de los puertos para poder administrar el tráfico que pasa a través de ellos. Por defecto, cualquier firewall bloquea todos los puertos a menos que el usuario decida lo contrario. Es posible definir la apertura de algunos puertos para que aquellos programas que los necesiten puedan funcionar. Con todos los puertos cerrados, una computadora no podría siquiera enviar e-mails.

Para administrar las excepciones de puertos y programas, es necesario acceder a la interfaz del firewall haciendo doble clic sobre el icono **Firewall de Windows** del **Panel de Control**. Allí deberemos hacer clic en **Permitir un programa a través del Firewall de Windows**, donde encontraremos la ventana analizada en la **Guía visual 2**.



AGREGAR EXCEPCIONES

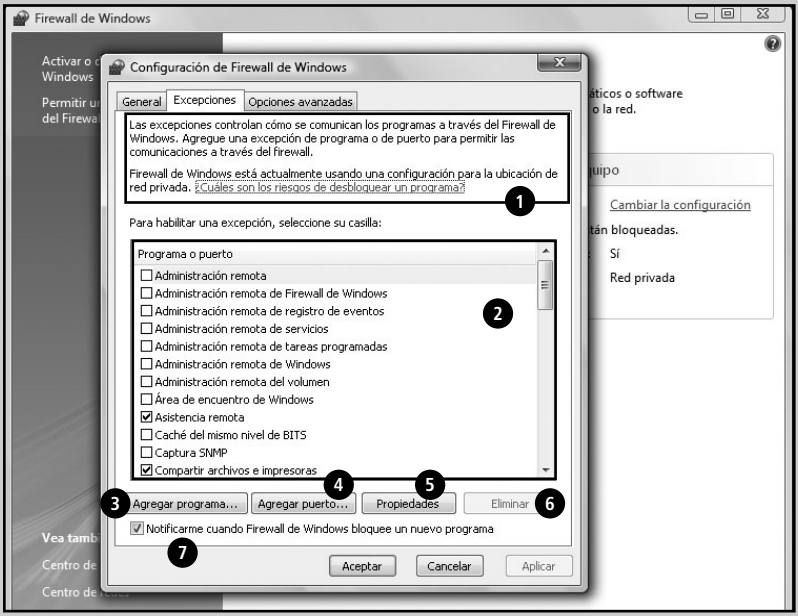
Una vez dentro de la ventana **Excepciones**, el proceso de agregar nuevos elementos es muy simple (**Figura 10**). No resulta tan sencillo, en cambio,

FIGURA 10. La configuración incorrecta de algún parámetro del firewall dejará nuestro equipo al descubierto.

PUERTOS VS. CONECTORES

Los puertos de los que hablamos cuando analizamos firewalls no son los conectores exteriores de la PC, también llamados puertos. No hay que confundir los puertos **USB** o **PS/2** con el puerto 80, que corresponde a los servidores web, o el 110, del correo saliente.

GUÍA VISUAL /2
Excepciones



1. Muestra una pantalla de ayuda respecto de la utilización de excepciones.
2. Lista de programas que ya fueron alguna vez agregados a la lista de excepciones. Aquellos no tildados no representan una excepción.
3. El botón **`Agregar programa`** permite definir un nuevo programa como excepción.
4. El botón **`Agregar puerto`** permite definir un nuevo puerto como excepción.
5. El botón **`Propiedades`** permite el acceso a modificar las condiciones de la excepción.
6. El botón **`Eliminar`** permite quitar una excepción de la lista de programas.
7. Una marca en esta casilla de verificación hará que, cada vez que un programa recién instalado intente acceder a la red, Windows nos permita bloquearlo o agregarlo a la lista de excepciones.

dimensionar con claridad qué estamos excluyendo y por qué. Es importante tener claro qué programa o puerto se va a excluir para no incurrir en un error y dejar, así, la seguridad de la máquina librada al azar.

Al agregar un programa a la lista de exclusiones, se le permite a esa aplicación que administre a su gusto el tráfico de datos desde Internet o desde las demás computadoras de la red, y hacia ellas. Esta concesión suele ser necesaria para juegos online o multiplayer y para programas de intercambio de archivos. Otras aplicaciones, por diferentes causas, podrían también necesitar tal libertad.

Es de sumo interés, por supuesto, tener siempre muy en claro qué es lo que va a hacer el programa con el permiso: de ninguna manera deberíamos abrir la puerta a un programa cuya utilidad no tenemos en claro.

Para agregar un programa a la lista de excepciones, en el cuadro **Excepciones** del Firewall de Windows, hay que hacer clic en **Agregar programa** y, luego, seleccionar el programa de la lista o presionar el botón **Examinar**. A continuación, debemos buscar en el disco el archivo ejecutable. Al presionar el botón **Aceptar**, el programa habrá empezado a formar parte de la lista de excepciones (**Figura 11**).

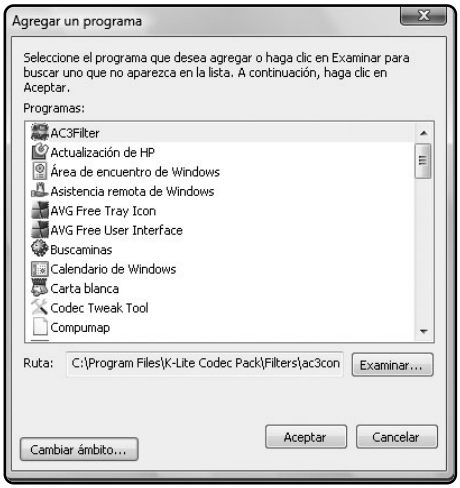


FIGURA 11. Nunca hay que agregar programas a la lista a menos que la necesidad haya sido declarada o el programa no funcione correctamente sin esta configuración.

FIREWALL POR HARDWARE O SOFTWARE

En computadoras hogareñas, se prefiere el firewall por software: programas encargados de monitorear y administrar el tráfico de la red. En entornos corporativos, se utilizan los firewalls por hardware: dispositivos dedicados que administran la seguridad de una red.

Cambiar ámbito

En el cuadro **Agregar programa**, hay un importantísimo botón que permite cambiar el ámbito donde la excepción tendrá lugar. De este modo, en el cuadro **Cambiar ámbito**, podremos definir si un programa será una excepción al comunicarse con Internet, con un equipo determinado de la red o con la Intranet completa y no Internet. Las opciones, entonces, son las siguientes:

- **Cualquier equipo**: la excepción podrá comunicarse bidireccionalmente con cualquier equipo de la red interna y de Internet. O sea, para ese programa, se aceptará todo el tráfico entrante y saliente.

- **Sólo mi red**: en este ámbito, las excepciones solo se harán con equipos que forman parte de una misma red de trabajo, pero no con los equipos de Internet o de otras redes. Esta configuración es la adecuada para, por ejemplo, mensajeros instantáneos diseñados para redes internas, caso en el cual no tiene ningún sentido dar acceso al programa también a Internet.

- **Lista personalizada**: esta opción permite determinar un rango de direcciones IP para que la comunicación esté reducida solo a aquellas computadoras cuya dirección aparezca en la lista.

Las direcciones del protocolo de Internet (**Internet Protocol** o **IP**) son cuatro números separados por puntos que identifican computadoras en una red (por ejemplo **192.168.0.1**). Una misma dirección no puede repetirse en una misma red (sí en otras), por lo que utilizar ese dato para identificar equipos es muy efectivo (**Figura 12**).

ABRIR PUERTOS

En el cuadro **Excepciones**, al presionar el botón **Agregar puerto**, accedemos al cuadro que nos permite definir los números de puerto que serán abiertos. Cabe aclarar que, como pasa con los

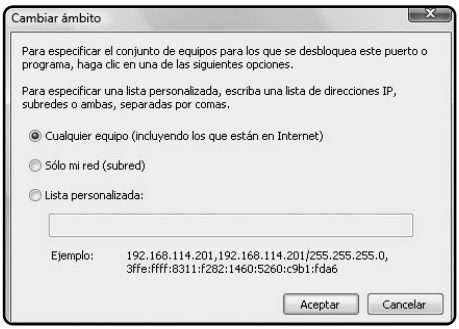


FIGURA 12. El cuadro `Cambiar ámbito` ayuda a definir con mayor exactitud el carácter de la excepción. Ningún programa debe tener más permisos de los que necesita.

CON UN SOLO FIREWALL ES SUFICIENTE

Un servidor de seguridad es suficiente como para no tener que poner a trabajar dos programas de este tipo en paralelo. Por eso, a menos que necesitemos un nivel de seguridad superior o mayor control sobre los puertos, bastará con el firewall de Windows.

programas, se pueden definir los ámbitos en los que un puerto estará abierto para evitar dejar alguno abierto innecesariamente. Los puertos abiertos son un riesgo de seguridad crítico en una red, por lo tanto, hay que evitar abrir aquellos que pueden mantenerse cerrados.

El cuadro de diálogo que nos permitirá abrir un puerto exige los siguientes datos:

• **Nombre**: es el nombre que queremos darle a la excepción. En el mundo de los firewalls, a la hora de definir un comportamiento para un programa o puerto (una excepción) se habla de reglas. Aquí se nos pregunta, entonces, el nombre descriptivo de la regla. Por ejemplo, **Puerto para compartir archivos**.

• **Número de puerto**: cuál es el número del puerto que queremos abrir; **4671**, por ejemplo.

• **TCP** o **UDP**: exige especificar si se trata de un puerto TCP o uno UDP (**Plaqueta TCP y UDP**).

• **Cambiar ámbito**: especifica el ámbito en el cual funcionará la regla. Esta opción actúa de la misma manera que al trabajar con programas.

• **¿Qué riesgo existe al abrir un puerto?**: Microsoft incluye una rápida e interesante guía sobre el riesgo de cambiar la configuración predeterminada de puertos (**Figura 13**).

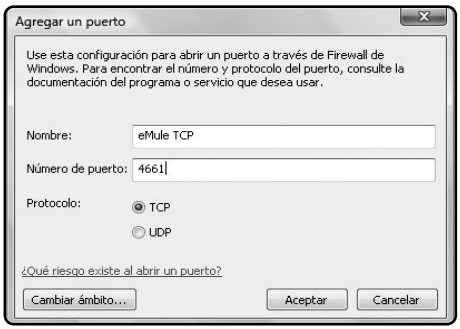


FIGURA 13. Un puerto abierto sin necesidad destruirá la protección de cualquier equipo. Este cuadro debe utilizarse en casos extremos.

TCP Y UDP

Transmission Control Protocol (TCP) y **User Datagram Protocol (UDP)** son componentes del protocolo **TCP/IP (Transmission Control Protocol/Internet Protocol)**. Mientras que UDP no necesita establecer una conexión segura para transmitir, TCP sí lo hace.

OPCIONES AVANZADAS

Las opciones avanzadas del firewall de Windows no se ocupan de ajustar la seguridad del sistema, sino que configuran variables de entorno del programa (**Figura 14**).

El recuadro **Configuración de conexión de red** permite establecer para qué conexiones activaremos el firewall. Como ya dijimos, Windows lo activa por defecto para todas, y no existe una razón válida por la cual desactivarlo (**Figura 15**).

Por último, el recuadro **Configuración predeterminada** contiene un botón (**Restaurar valores predeterminados**) que devolverá a la configuración del firewall los parámetros de la instalación. Este botón es muy útil en especial para aquellos usuarios que cambiaron la configuración de seguridad y luego desean restablecer los valores para cubrirse de un posible error (**Figura 16**).

Algunos sitios de Internet (que venden u ofrecen firewalls personales o por hardware) dan la posibilidad

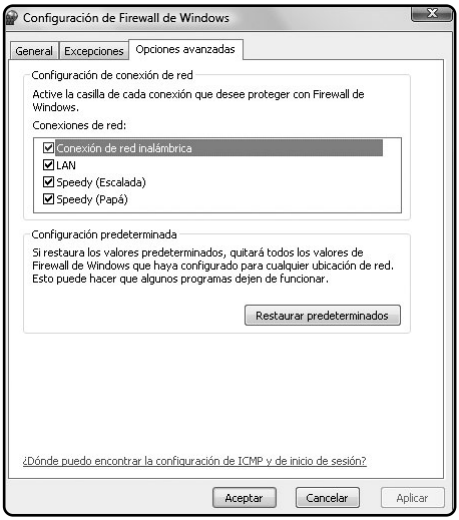


FIGURA 14. Las opciones avanzadas del firewall de Windows solo deberían ser cambiadas en casos muy necesarios o a la hora de restaurar la configuración a su punto inicial.

FIGURA 15. Es importante buscar las alternativas que nos permitan disminuir los riesgos ante posibles amenazas.

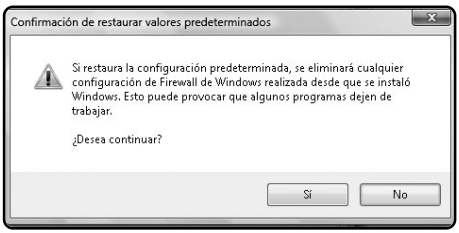


FIGURA 16. Si hicimos algún cambio de cuya consecuencia no estamos seguros, podemos restablecer la configuración del firewall a su estado anterior.

de realizar une test online del funcionamiento del firewall instalado en el equipo. Por practicidad y facilidad de uso, vamos a utilizar para nuestra prueba el servicio de la empresa Symantec, desarrolladora de los productos de seguridad de la línea **Norton**.

Para hacer la prueba, abrimos nuestro navegador e ingresamos en **http://security.symantec.com/sscv6**. Allí presionamos el botón **`Continue to Symantec Security Check`**. Iniciamos la prueba al pulsar el botón **`Start`**, ubicado debajo del título **`Security Scan`** (**Figura 17**).

El centro de seguridad

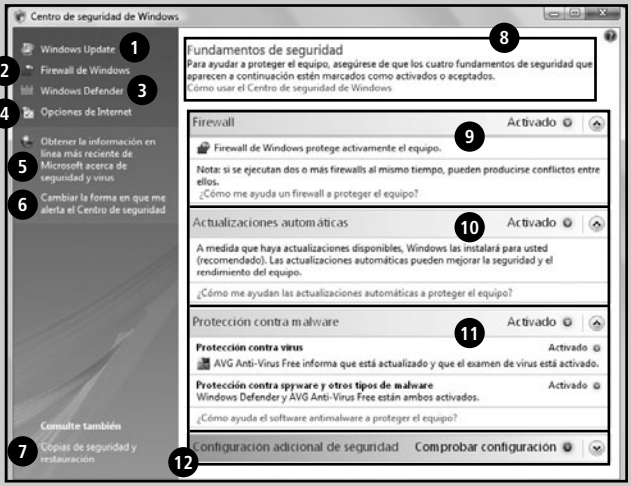
Una buena herramienta para monitorear el funcionamiento de las herramientas de seguridad y de otras, como el antivirus y el antispyware, es el **Centro de seguridad**. El **`Centro de seguridad`** se encuentra en el **`Panel de control`** y, ante la falla de alguno de los componentes básicos de seguridad del sistema, instala un icono en la zona de notificación de la barra de tareas informando sobre el problema.

FIGURA 17.
Las pruebas online no son 100% efectivas, pero nos darán una idea acabada de si el firewall instalado en el equipo reacciona en forma correcta frente a un ataque.

RESUMEN

En este capítulo vimos la importancia que tienen las actualizaciones del sistema en los aspectos relacionados con seguridad. Aprendimos a manejar el firewall de Windows. Además, conocimos cómo configurarlo para extremar los niveles de protección del equipo.

GUÍA VISUAL /3
Centro de seguridad



1. Abre **`Windows Update`** para comprobar la actualización del sistema operativo.
2. Abre la pantalla principal del firewall de Windows
3. Abre la pantalla principal del software antispyware **`Windows Defender`**.
4. Abre el cuadro **`Opciones de Internet`**.
5. Conecta con el sitio de Microsoft de información sobre virus, adware, spyware y malware.
6. Permite definir cuándo y de qué modo el **`Centro de seguridad`** debe alertar al usuario al respecto de las falencias de seguridad del equipo.
7. Abre la herramienta **`Copias de seguridad y restauración`** para efectuar una copia de respaldo de los datos disponibles en el equipo.
8. Muestra la ayuda del **`Centro de seguridad`**.
9. Muestra información y estado inmediato sobre el firewall del sistema.
10. Indica el estado y la configuración de las actualizaciones automáticas.
11. Muestra el estado de las diferentes herramientas antimalware disponibles en el equipo.
12. Muestra el estado del **`Control de cuentas de usuario`** y la protección antiphishing.

Multiple **choice**

1 ¿Qué es un service pack?

a- Un paquete contenedor de una cantidad importante de actualizaciones.
b- Un navegador.
c- Un antivirus.
d- Un antimalware.

2 ¿Qué aplicación protege nuestro equipo contra intrusiones?

a- El service pack.
b- La suite Office.
c- El firewall.
d- Ninguna de las anteriores.

3 ¿Cuál de las siguientes opciones corresponde a uno de los mejores firewalls fabricado por empresas ajenas a Windows?

a- Netscape.
b- Blackberry.
c- Zonealarm.
d- Thunderbird.

4 ¿Qué más protege un firewall, además de resguarar los ataques vía Internet?

a- La integridad y el acceso a la red local.
b- Las actualizaciones de Windows.
c- La criptografía de los mensajes.
d- Ninguna de las anteriores.

5 ¿Comodo Internet Security puede interactuar con el firewall de Windows?

a- No.
b- Solo en Windows 7.
c- Sí, pero cuando lo utilicemos, éste administrará el firewall de Windows y no nos permitirá modificarlo.
d- Ninguna de las anteriores.

6 ¿Se pueden agregar excepciones al firewall de Windows?

a- No.
b- Solo en Windows 7.
c- Solo en Windows XP.
d- Ninguna de las anteriores.

Respuestas: 1a, 2c, 3c, 4c, 5c y 6d.

Capítulo 5

Cuarto paso: configuración segura de la red Wi-Fi

Estudiaremos cómo encargarnos de que la red inalámbrica Wi-Fi esté configurada de manera segura.

En la actualidad, es posible tener una red inalámbrica en el hogar a bajo costo. Desafortunadamente, para los usuarios poco cuidadosos, una red inalámbrica puede ser muy insegura si no está configurada de manera eficiente. Estudiaremos, en este capítulo, cómo encargarnos de que este apartado de nuestra infraestructura informática esté cuidado. Aprendamos la forma de utilizar una red inalámbrica sin que esto signifique un riesgo importantísimo para los datos.

Redes inalámbricas y seguras

En los últimos tiempos, las redes inalámbricas (**Figura 1**) se hicieron cada vez más y más comunes, en parte gracias a la disminución de sus precios y también porque el avance de los dispositivos portables y su interacción con las computadoras convirtió a las redes cableadas en algo estrictamente asociado al mundo corporativo.

Las interfaces de conexión inalámbricas dejaron de ser un opcional en cualquier equipo portátil, y la diferencia económica entre un router regular y uno que incorpore conexión **Wi-Fi** es cada vez menor. Sin embargo, muchas veces la incorporación de dispositivos inalámbricos a una red cableada atenta contra la seguridad del grupo de trabajo, en tanto muchos usuarios creen que alcanza con conectar un **punto de acceso inalámbrico** para empezar a usarlo (**Figura 2**).

Las redes inalámbricas plantean, en principio, una serie de problemas de seguridad que no se aplican (por una cuestión estructural) a las redes cableadas. Estos problemas están asociados, básicamente, a la visibilidad de las redes inalámbricas y a la fragilidad de las claves que se utilizan para autenticar los diferentes equipos (**Figura 3**).

Esto, sumado a una falta de conocimiento bastante generalizada por buena parte de instaladores y usuarios sobre las posibles consecuencias de seguridad, que deben ser consideradas a la hora de montar

FIGURA 1.
Redes inalámbricas según su alcance y protocolos relacionados.

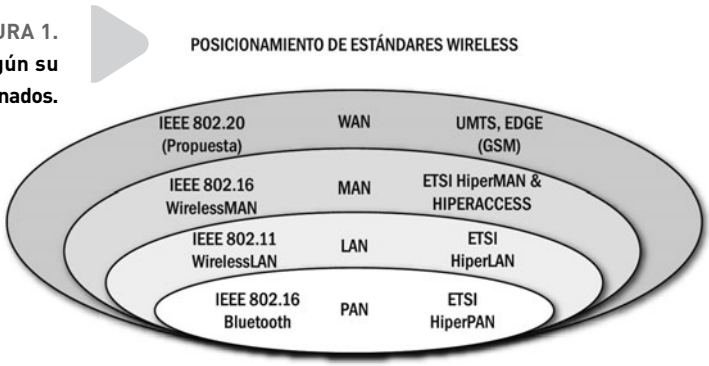


FIGURA 2.
En su apariencia exterior, un router cableado y uno inalámbrico, por lo general, solo difieren por la antena.

una red sin cables, hace que el panorama del mundo Wi-Fi esté bastante comprometido. La necesidad de una instalación seria de cualquier dispositivo inalámbrico es imprescindible para no tirar por la borda todo el esfuerzo que hemos hecho hasta ahora para convertir el equipo en una fortaleza digital. También, para evitar ofrecer al mundo la totalidad de nuestros archivos.

EL PROBLEMAS DE LAS CONTRASEÑAS

Hay una diferencia sustancial al momento de pensar en los problemas de seguridad que puede acarrear el uso de una red inalámbrica respecto de una infraestructura cableada. Y esa diferencia tiene que ver con el **medio de transporte** que es utilizado.

Una red cableada requiere una conexión física con los equipos. Esto hace que una persona que no esté conectada mediante un cable UTP con un conector RJ45 no tenga posibilidad de entrar en la red. A menos, claro, que lo haga por medio de un agujero de seguridad en la conexión a Internet.

El carácter más difuso y no tangible del transporte aéreo de datos hace que una red inalámbrica, paradójicamente, sea en principio más accesible por terceros, ya que no requiere que el equipo desconocido esté conectado a ningún concentrador (**Figura 4**).

Más allá de los problemas lógicos que pueden planteársele a un atacante para acceder a los datos de

FIGURA 3. Siempre que podamos, es fundamental cambiar el nombre de usuario del router, además de la contraseña.

un equipo que forme parte de un grupo de trabajo, la conexión física, como decíamos antes, es una característica que se vuelve imperativa.

En una red inalámbrica mal configurada, cualquier atacante podrá acceder muy rápido al grupo de trabajo, y el acceso a los datos de los usuarios solo estará limitado por la correcta configuración de un firewall. Por lo tanto, es primordial tomarnos unos minutos para configurar los valores de seguridad del router inalámbrico o del **Access Point** (punto de acceso) antes de empezar a utilizarlo (**Figura 5**).

Más adelante, veremos algunos conceptos básicos de seguridad y administración de la red, pero es fundamental tener en cuenta que resulta **inseguro** utilizar una red inalámbrica con los valores de configuración predeterminados que traen de fábrica los dispositivos que la componen (**Figura 6**).

Un segundo problema, no menor, de las redes inalámbricas tiene que ver con el modo mediante el

cual los diferentes dispositivos inalámbricos se autentican para acceder a un **grupo de trabajo** o red de área local (**LAN**). Cuando una red inalámbrica está asegurada de manera correcta, el usuario debe conocer una clave de seguridad para acceder a ella. Sin embargo, hay varios tipos de claves que pueden utilizarse, que ofrecen distintos niveles de seguridad en cada uno de ellos. Elegir un tipo de **encriptación** para la clave que no sea el adecuado puede significar exponer una red a que un usuario malintencionado que intente atacarla no encuentre mayores problemas para quebrar su seguridad (**Figura 7**).

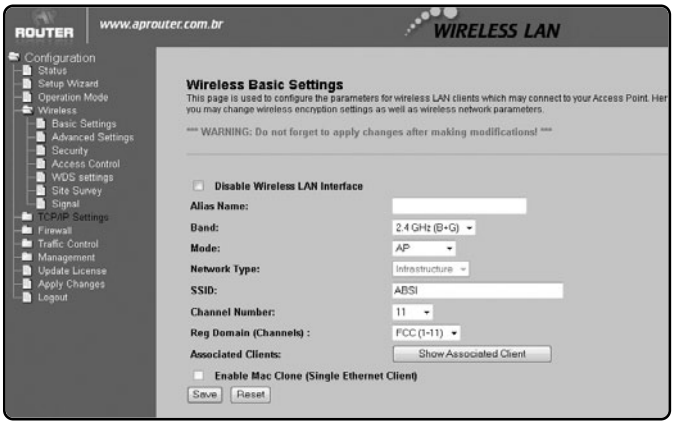


FIGURA 4.
El botón Show Associated Client nos permitirá saber qué equipos están conectados a la red Wi-Fi en ese momento.

FIGURA 5.
Según el fabricante del router que utilizamos en la red, podemos encontrar diferentes Access Point.

Desde su aparición, se han establecido una serie de mecanismos que apuntan a mejorar la seguridad en las redes inalámbricas, en tanto éstas, por los motivos que hemos explicitado antes, deben ser consideradas a priori inseguras. Estos mecanismos consisten en proteger el acceso a la red mediante el uso de contraseñas y complejas técnicas de autenticación que validen al usuario.

El primero de éstos fue **WEP**, cuya excesiva debilidad lo dejó rápidamente fuera de competencia. A pesar de esto, algunos usuarios aún lo utilizan para mantener compatibilidad con sus viejos dispositivos que no son compatibles con métodos de autenticación más modernos. El reemplazo de WEP, que tuvo algunos problemas en sus primeras versiones, se llama **WPA**. Por sus características, aumenta en mayor grado la seguridad de las redes sin cables.

FIGURA 6.
Una red inalámbrica mal configurada puede ser vista por cualquier dispositivo inalámbrico, y alcanzaría un pequeño adaptador Wi-Fi para vulnerarla.

IMPORTANCIA DE LA SEGURIDAD EN UNA RED WI-FI

Hablar de seguridad en una red Wi-Fi significa cuidar la integridad de nuestros datos y proteger el acceso a la información sensible. Un router bien configurado, en conjunto con un firewall personal, harán del grupo de trabajo un entorno realmente seguro.

FIGURA 7. No es recomendable tildar la casilla de verificación `Recordar contraseña` **para el acceso al router inalámbrico ni en ningún otro dispositivo de red.**

Como primera medida, utiliza contraseñas más complejas (en muchos casos, solo acepta números hexadecimales de 10 dígitos) y algoritmos de encriptación que elevan el nivel de seguridad de las redes Wi-Fi a estándares muy aceptables. A continuación, veremos los principios de ambos protocolos para que se pueda entender por qué es necesario tomar las mayores medidas de seguridad posibles cuando de redes inalámbricas se trata. Por supuesto, existen otros métodos de autenticación en redes inalámbricas, como por ejemplo, el estándar **Radius**, pero que no resultan funcionales para pequeñas redes (**Figura 8**).

WEP

WEP es el acrónimo de **Wired Equivalent Privacy** o, en castellano, **privacidad equivalente al cableado**. Los objetivos de este algoritmo de seguridad consisten en proporcionar confidencialidad, autenticación y control de acceso en conexiones inalámbricas.

FIGURA 8. En el sitio de la compañía Cisco (www.cisco.com), podremos encontrar una interesante cantidad de información acerca de Radius.

WEP Y WPA EN ROUTERS

Si bien la mayoría de los routers y dispositivos de conectividad inalámbricos de la actualidad son compatibles con WEP y WPA, ninguno activa por defecto estos protocolos de seguridad. Es decir, que no plantean mecanismos de seguridad para acceder a la red inalámbrica.

Para esto, WEP utiliza una clave de seguridad idéntica en todos los equipos y puntos de acceso de la red. Esta clave es creada e introducida en forma manual en cada equipo, y no existe un sistema de automatización de las contraseñas, lo que hace que esta clave pierda muy pronto su fuerza (**Figura 9**). En primer lugar porque, al estar ingresada en todas las terminales, la posibilidad de ser corrompida es bastante alta. Y en segundo término porque, al ser una clave que debe estar en todas las terminales, es conocida por varias personas. Esto también redunda en que la clave no sea actualizada casi nunca, ya que su actualización resulta bastante incómoda en tanto debe ser repuesta en cada uno de los equipos.

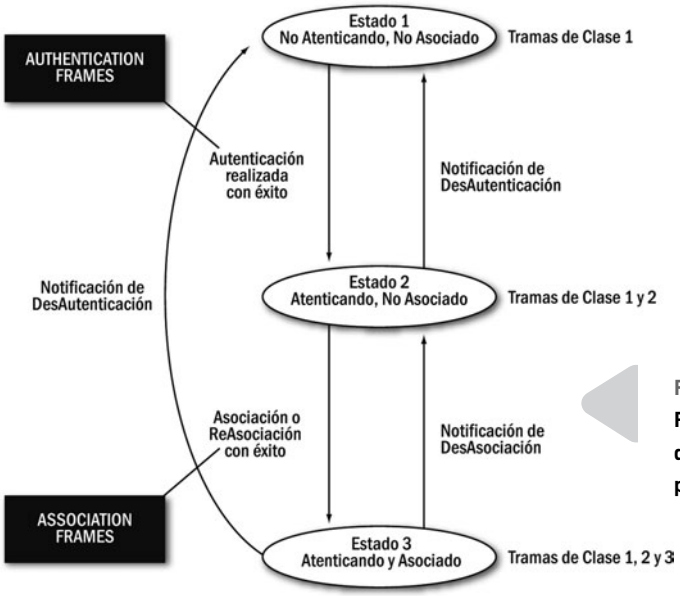


FIGURA 9.
Representación del proceso de autenticación y asociación para el sistema WEP.

CALIDAD DE LOS DISPOSITIVOS

Mientras más avanzado y de mejor calidad sea el dispositivo de acceso inalámbrico que compremos, más herramientas de seguridad y administración pondrá a nuestro alcance. Si apuntamos a elevar el nivel de protección de la red, es buena idea comprar productos mejores.

Además, algunas debilidades serias en el funcionamiento técnico del algoritmo y una serie de desprolijidades a la hora de implementar la norma hicieron que WEP se volviera casi inservible en poco tiempo. Sus objetivos, entonces, quedaron frustrados y, en nuestros días, aporta un nivel de seguridad que no nos alcanzará si pretendemos que nuestro equipo resulte inviolable de verdad.

WPA

WPA (**Wi-FI Protected Access**, o en castellano **acceso a Wi-Fi protegido**) es un protocolo de seguridad que pretendía mejorar las características de WEP mientras el consorcio Wi-Fi terminaba el nuevo algoritmo de protección de datos **WPA2**, también conocido como **802.11i** (**Figura 10**).

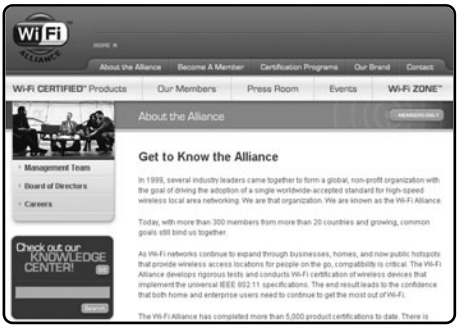


FIGURA 10. El consorcio Wi-Fi (www.wi-fi.org) define los estándares para que los dispositivos inalámbricos funcionen en conjunto.

WPA mejora las debilidades de WEP e introduce nuevos mecanismos para asegurar los datos transmitidos. De esta forma, puede ser considerado más que suficiente para una red de hogar y de pequeña oficina, y no debemos dudar de su eficacia ni temer el uso de las redes Wi-Fi si nos basamos en una protección de este tipo. Aun cuando todavía requiere, en uno de sus modos, una clave compartida por el router y todos los equipos, esa clave es utilizada en WPA solo para la autenticación inicial de los usuarios. Luego, este protocolo genera claves dinámicas para proteger el transporte de datos, a diferencia de WEP que, aun en esos casos, continúa utilizando la clave conocida por todos los usuarios de la red.

WEP O WPA

Siempre que los dispositivos inalámbricos con los que estemos trabajando sean compatibles con el protocolo de seguridad **WPA**, ésta es la opción que debemos utilizar por sobre **WEP**. No hay razón para usar un algoritmo menos seguro, ni motivos para tener una red desprotegida.

FIGURA 11.
Todos los dispositivos de conectividad inalámbrica modernos son compatibles con WPA. En la actualidad, este estándar es considerado seguro y elimina todas las debilidades de WEP.

La única debilidad de WPA reside en que, para funcionar, requiere un pequeño servidor de seguridad, que muchas veces suele estar incorporado en el router inalámbrico. Sin embargo, de no contar con un router compatible con WPA, será imposible utilizar el estándar, y el nivel de seguridad de la red no podrá mejorarse respecto de WEP. En estos casos, la recomendación es actualizar la infraestructura de la red (**Figura 11**).

Adquirir un router **Wi-Fi**

Comprar un router de acceso inalámbrico suele ser una tarea sencilla si tenemos en cuenta ciertos aspectos del producto. Pero, si en cambio, no prestamos la debida atención a la compra y volvemos a casa con un producto inapropiado, nos lamentaremos por mucho tiempo.

También debemos tener en cuenta todos los detalles cuando recibimos un dispositivo provisto por un proveedor de Internet. Aunque la mayoría de los **ISP** en la actualidad ofrecen a sus clientes módems con conexión **Ethernet**, es decir, que se conectan a la computadora vía puerto de red, es imprescindible que verifiquemos que contamos con uno de este tipo, porque los módems **USB** solo pueden ser conectados a routers provistos por el proveedor.

Es importe aclarar que todos los routers, además de ofrecer capacidades inalámbricas, pueden también conectar un mínimo de **cuatro** equipos vía Ethernet,

CONFIGURACIÓN PREDETERMINADA INSEGURA

Los dispositivos de conexión inalámbrica vienen configurados de modo predeterminado para hacer más fácil su instalación. Sin embargo, esa configuración es la más insegura de todas las posibles y deja la red en su totalidad al descubierto, por lo que no debemos utilizarla.

FIGURA 12.
A diferencia de un router, un switch no asigna direcciones IP a los equipos que tiene conectados.

es decir, por cable. El número se eleva a **256** dispositivos si utilizamos switches para aumentar la cantidad de bocas (**Figura 12**).

Cuando decidimos adquirir un router en un comercio especializado, el primer aspecto por tener en cuenta al momento de comprar es que el producto sea de buena calidad general y que el software controlador sea realmente eficaz y amigable.

Por lo general, los routers de mala calidad suelen tener problemas físicos que van desde fuentes insuficientes o de durabilidad reducida a problemas de temperatura en el procesador y los componentes principales, lo que redunda en reinicios intempestivos del equipo.

El tema del software es central para poder acceder al dispositivo y configurarlo. Un router, cuya interfaz a la que nos conectaremos vía navegador web es poco amigable o que no ofrece la cantidad de opciones que el aparato puede manejar, complicará bastante nuestra tarea de configuración y nos traerá más de un problema. Aunque por lo general es posible actualizar el software, solo los productos de buena calidad ofrecen actualizaciones que mejoran los **bugs** (errores o defectos de software) de las versiones anteriores.

RECOMENDACIONES WI-FI

En **www.virusprot.com/Whitepap1.html**, encontraremos una completa guía con consejos de seguridad para usuarios de redes inalámbricas. Además, este sitio cuenta con un completo glosario de términos asociados, recomendable para quienes deseen saber más del tema.

FIGURA 13.
Si necesitamos más alcance en nuestra red Wi-Fi, es posible agregar antenas más potentes y pigtails que mejoren el alcance.

Los aparatos de marcas reconocidas nos aseguran calidad y pocos problemas. Además, los mejores routers son aquellos que ofrecen un mayor rango de acción. En éstos, las especificaciones del fabricante suelen ser más precisas y nos ofrecen una mayor gama de opciones a la hora de decidir qué producto debemos llevarnos a casa cuando definimos la compra (**Figura 13**).

Si compramos productos con norma **G** (aunque no es la especificación más nueva), encontraremos un resultado suficiente para el uso hogareño. Esta alternativa representa la mejor relación precio/producto. Además, ofrece compatibilidad con los viejos aparatos norma **B**, y cualquier adaptador compatible con el borrador de la nueva norma **N** podrá conectarse a nuestro equipo sin problemas (**Figura 14**).

Si, en cambio, lo que necesitamos es un router muy potente, porque deseamos cubrir un rango bastante amplio, la recomendación es adquirir un producto con la norma más moderna, que en la teoría cuadriplica el accionar de su predecesora. En la práctica, claro, los resultados no son tan espectaculares. Pero en cualquier caso, el alcance del router será de todas formas mayor. En algunos productos, la mejora resulta superior al 50%.

También, se pueden utilizar dos routers para cubrir una distancia más amplia, pero debemos tener en cuenta algunas especificaciones.

WDS

Si vamos a utilizar Wi-Fi en un espacio muy amplio, es aconsejable comprar enrutadores que soporten **WDS** (**Wireless Data Distribution** o **distribución inalámbrica de datos**). Esta característica nos permitirá conectar dos routers, entre sí, sin cables.

FIGURA 14.
Los routers norma N ofrecen el mayor rendimiento del mercado. Su rango es sumamente amplio y, si buscamos potencia y fiabilidad, no nos sentiremos defraudados.

Configuración básica del router

Como ya hemos mencionado, la correcta configuración del router depende directamente de la seguridad de la red inalámbrica y, por ende, la seguridad de la red en general y de nuestro equipo en particular. Por lo tanto, el tiempo que dediquemos para hacer de nuestro punto de acceso inalámbrico uno bien seguro es tiempo ganado (**Figura 15**).

Además, en cualquier caso, tardaremos menos tiempo en configurar correctamente el acceso Wi-Fi que en limpiar una infección de la red, por no pensar en las horas y el dinero que nos tomaría recuperar los datos perdidos. En este capítulo, trabajaremos con un **router genérico**, de bajo costo, pero que, a su vez, cuenta con todas las características que recomendamos antes.

La conexión física del router es similar en todos los dispositivos. A continuación conoceremos el detalle. Al desembalar el aparato, debemos en principio atornillar la antena al router y ubicar éste en un lugar visible, y dentro de las posibilidades, a una altura superior a **2 metros**. Amurarlo es siempre una buena idea, ya que nos permitirá dejarlo fijo y evitar que el movimiento cambie la orientación de las antenas, característica fundamental en algunos casos para que el aparato resulte por demás eficiente. Todos los routers incluyen, junto con un juego de topes de goma para el aparato, los tornillos y tarugos necesarios para colgar el dispositivo.

CONTRASEÑAS

Al momento de establecer una contraseña en un entorno de trabajo inalámbrico, debemos tener especial cuidado para elegirla. Por sus características, en este tipo de ambiente es necesario crear una contraseña realmente segura.

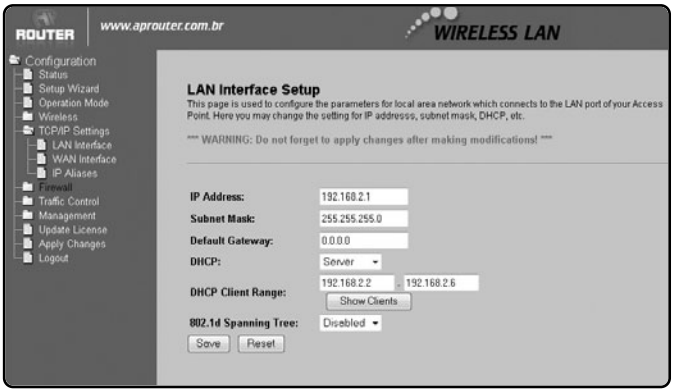


FIGURA 15.
Por defecto, ninguno de estos valores, salvo el del rango de direcciones IP, debe ser cambiado.

Luego, solo nos restará enchufar la fuente de alimentación a la corriente eléctrica y al router; y el cable UTP provisto por el fabricante, al módem y al conector indicado como **WAN** o **1** en el router. Las computadoras que se conecten a la red local vía Ethernet deben ser conectadas en este momento al resto de los puertos disponibles en el enrutador. Lo que falta del trabajo lo haremos vía software desde la computadora (**Figura 16**).

CONFIGURACIÓN INICIAL

En primer lugar, lo que debemos hacer es realizar la configuración inicial del router, que nos permitirá establecer una contraseña para el acceso al dispositivo,

FIGURA 16.
Los routers de mejor calidad suelen incluir buenos manuales que nos ayudarán durante el proceso de configuración, mientras que los demás, solo incluyen una guía de inicio rápido.

una clave de acceso WEP para acceder a la red y otros valores menos importantes, como el servidor de fecha y hora que nos ayudará a precisar las alertas administrativas. En esta configuración inicial, definiremos el modo en el que el router debe conectarse a Internet y estableceremos la conexión por primera vez. Por defecto, los usuarios de conexiones que no requieren nombres de usuario y contraseña, como aquellos que utilizan servicios de **cablemodem**, podrán conectarse a Internet en forma directa sin llevar a cabo ninguna configuración inicial, pero, en ese caso, estarán dejando de lado el apartado de seguridad.

Muchos routers incluyen un CD con un asistente para realizar esta configuración inicial. Si bien puede ser una buena idea ejecutar desde aquí el asistente, nosotros, que no nos conformamos con un nivel básico de seguridad, sino que buscamos sistemas de protección con más opciones, nos inclinaremos por utilizar, en forma directa, la **interfaz web** del router.

Si ya hemos instalado el router utilizando el CD, no debemos preocuparnos: todos los parámetros de seguridad pueden configurarse otra vez vía web.

Acceder al router

Para acceder al router, visitaremos su interfaz web. A ésta se accede utilizando la **dirección IP** del dispositivo o una dirección web del estilo de **www.modelodelrouter.com**. Lograremos averiguar la dirección IP por defecto o la dirección web que nos permitirá acceder a la interfaz leyendo el manual o la guía rápida del usuario.

Algunos dispositivos tienen una etiqueta pegada en su parte inferior con esa información, y el nombre de usuario y contraseña por defecto. Si nuestro dispositivo no la incluye, es una buena idea escribir esos datos en el aparato, para estar prevenidos en el caso de que extraviemos el manual del producto.

Una vez que contemos con la información necesaria, abriremos el navegador web y escribiremos la dirección correcta en la barra de direcciones. Luego de presionar **Enter**, alcanzará con escribir el nombre

CREAR RED INALÁMBRICA

En el foro del sitio Trucos Windows (**www.trucoswindows.net/foro**), encontraremos varios tutoriales para crear una red inalámbrica desde el principio, para sistemas Windows. Allí se ofrecen los componentes por elegir y las configuraciones de seguridad más adecuadas.

de usuario y contraseña por defecto del dispositivo para entrar en la interfaz (**Figura 17**).

El asistente para la configuración inicial

En la mayoría de los dispositivos, la configuración inicial puede llevarse a cabo con la ayuda de un asistente o **Lizard**, que nos guiará en el proceso. Esto es importante, sobre todo porque la interfaz de los dispositivos suele estar en inglés y, además, puede contener términos cuyo significado desconocemos.

En el **Paso a paso 1**, veremos cómo completar con éxito el proceso de configuración inicial.

Una vez concluido el proceso, es probable que, según el dispositivo que utilicemos, debamos hacer clic en el botón **Apply changes**. Una vez que hayamos hecho esto, el router se reiniciará, y los equipos que accedan a él vía Wi-Fi deberán reconectarse a la red utilizando el nuevo SSID y la contraseña de acceso que acabamos de definir.

FIGURA 17.
En el sitio www.adslzone.net, podremos encontrar información y manuales de los routers más populares del mercado.

FIRMWARE

El **firmware** es un programa grabado en una memoria no volátil (**EEPROM** o **Flash**) que controla los circuitos electrónicos de un aparato. Está integrado en la electrónica del dispositivo, y se lo considera un elemento de hardware, pero puede ser actualizado vía software.

PASO A PASO /1
Configuración inicial del router

1

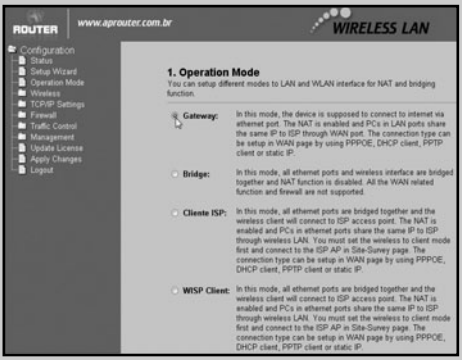
Abra su navegador web y conéctese a la dirección IP o web del router.
Escriba su nombre de usuario y contraseña; haga clic en **`Aceptar`**.
En algunos dispositivos, este botón puede llamarse **`Log in`** o **`Submit`**.

2

Haga clic en el vínculo **`Setup wizard`** (u opción similar en su modelo) y, en la pantalla de bienvenida, presione **`Next`**.

PASO A PASO /1 (cont.)

3



Seleccione **Gateway** como modo de operación y, si esa opción no está disponible, deje la predeterminada. Luego, pulse **Next**.

4

Seleccione su zona horaria y elija el servidor de horario correspondiente a su región o país en el menú desplegable pertinente. Luego, presione **Next**.

PASO A PASO /1 (cont.)

5

Deje las direcciones predeterminadas para el dispositivo en lo que a configuración LAN respecta, a menos que su administrador de red le indique lo contrario. Luego, presione **Next**. Seleccione el tipo de conexión a Internet que utiliza. Si es **ADSL**, complete el nombre de usuario y contraseña del servicio. Luego, pulse **Next**.

6

Deje las opciones por defecto para la red inalámbrica. Pero defina un nombre para su red en la línea **SSID** y marque la casilla **Enable Mac Clone** si usa una única computadora vía puerto **Ethernet**, independientemente de los equipos inalámbricos. Luego, presione **Next**.

PASO A PASO /1 (cont.)

7

Seleccione el tipo de seguridad **WPA** si ésta se encuentra disponible. Seleccione el formato **Passphrase** siempre que pueda y defina, por último, una clave en la línea correspondiente. Use cualquier número y letras de la **A** a la **F**. Presione **Finish** para terminar.

RESUMEN

En este capítulo, hemos aprendido a configurar los elementos más importantes de la seguridad de una red inalámbrica. Conocimos los aspectos por tener en cuenta al adquirir un router. Además, vimos cómo realizar una configuración básica de un router.

Multiple **choice**

1 ¿Qué significa WEP?

a- Privacidad equivalente al cableado.
b- Acceso a WI-FI protegido.
c- Ethernet.
d- Ninguna de las anteriores.

2 ¿Qué significa WPA?

a- Privacidad equivalente al cableado.
b- Acceso a WI-FI protegido.
c- Ethernet.
d- Ninguna de las anteriores.

3 ¿Cuál es más conveniente: WEP o WPA?

a- WEP.
b- WPA.
c- Proveen la misma seguridad.
d- Según el router.

4 ¿Se puede mejorar el alcance de nuestra red WI-FI?

a- No.
b- Sí, al agregar otro módem.
c- Sí, con antenas y pigtails.
d- Ninguna de las anteriores.

5 ¿Qué es el firmware?

a- Un paquete con actualizaciones.
b- Un navegador.
c- Un antivirus.
d- Un programa grabado en la memoria no volátil con los circuitos electrónicos de un programa.

6 ¿Qué diferencia física presenta un router cableado de uno inalámbrico?

a- El tamaño.
b- El color.
c- La presencia de una antena.
d- Ninguna de las anteriores.

Respuestas: 1a, 2b, 3b, 4c, 5d y 6c.

Capítulo 6

Quinto paso: establecer políticas de seguridad y privacidad en la red local

Conoceremos aplicaciones
que permiten encriptar información
para que no puedan acceder otros usuarios.

Ahora que todos los equipos y dispositivos de nuestro hogar o pequeña oficina se encuentran perfectamente protegidos y configurados, en este capítulo aprenderemos a asegurar nuestra información en la red local. Además de conocer cómo se diseña una red segura, veremos aplicaciones que permiten encriptar información para que no pueda ser accedida por otros usuarios. También conoceremos aspectos de seguridad en mensajería interna y la importancia de configurar el control parental para proteger a menores.

Una red **segura**

Veremos ahora cómo configurar las diferentes computadoras para poder intercambiar información y recursos. Además, aprenderemos lo que debemos hacer para que ello no ponga en riesgo la fortaleza que, con mucho esfuerzo, fuimos armando a lo largo de los primeros capítulos de este libro (**Figura 1**).

CONCEPTOS BÁSICOS ANTES DE ARMAR LA RED

Antes de pensar en armar la red y asegurarla, repasaremos un poco ciertos conceptos básicos que es necesario manejar para entender de qué se trata cuando pensamos en una red.

Cuando en informática hablamos de **redes** (**networks**), nos referimos a una serie de computadoras interconectadas entre sí por un **concentrador**. Este concentrador puede ser un router, un switch o un hub, aunque estos dos últimos están en la actualidad casi extintos. Planteada la interconexión, estas computadoras pueden compartir infinidad de recursos: archivos, impresoras, conexiones a Internet, reproductores de medios y otros tantos dispositivos compatibles.

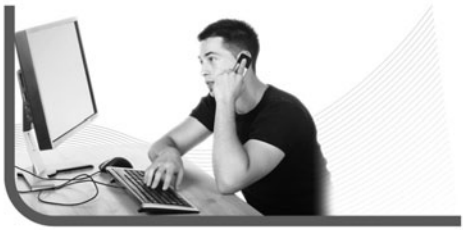
FIGURA 1.
Las redes de área local permiten compartir documentos, acceso a Internet y otros recursos, como impresoras.

NUESTRA INFORMACIÓN EN LA RED LOCAL

Es muy importante asegurar nuestra información en la red local, la red que usamos todo el tiempo para interactuar con los equipos cercanos. Luego de poner en práctica estos consejos, nadie podrá acceder a información o medios a los que no esté autorizado.

Existen dos tipos básicos de red: las **LAN** y las **WAN**. Las redes LAN (**Local Area Networks** o redes de área local) son aquellas que interconectan computadoras separadas por menos de 100 metros, a través de cableado estructural o de antenas inalámbricas (**Figura 2**). Las redes WAN (**Wide Area Networks** o redes de área extensa), en cambio, son dos o más redes de área local conectadas a través de Internet (**Figura 3**).

En este capítulo, nos vamos a centrar en el trabajo sobre redes de área local. Éstas cobraron especial importancia en los últimos años ya que, debido a su bajísimo costo, cualquier usuario que disponga de dos o más computadoras en un perímetro bastante reducido no dudará en armar una.



Antes de pensar en el nivel de seguridad de una red LAN, por supuesto, hay que tener en cuenta la seguridad de cada equipo que va a formar parte de ella. Cada computadora que integre la red deberá estar perfectamente configurada y asegurada igual que lo estaría si fuera un equipo único (**stand-alone**) conectado a Internet.

FIGURA 2.
Las redes LAN se pueden establecer tanto mediante cables como con acceso Wi-Fi de manera simple y económica.

MATERIAL PARA EDUCAR

Son cada vez más los docentes que instruyen a sus alumnos con presentaciones interactivas. En **www.segu-kids.org/material/** encontraremos un completo listado de presentaciones, videos, informes y cursos para padres y alumnos.

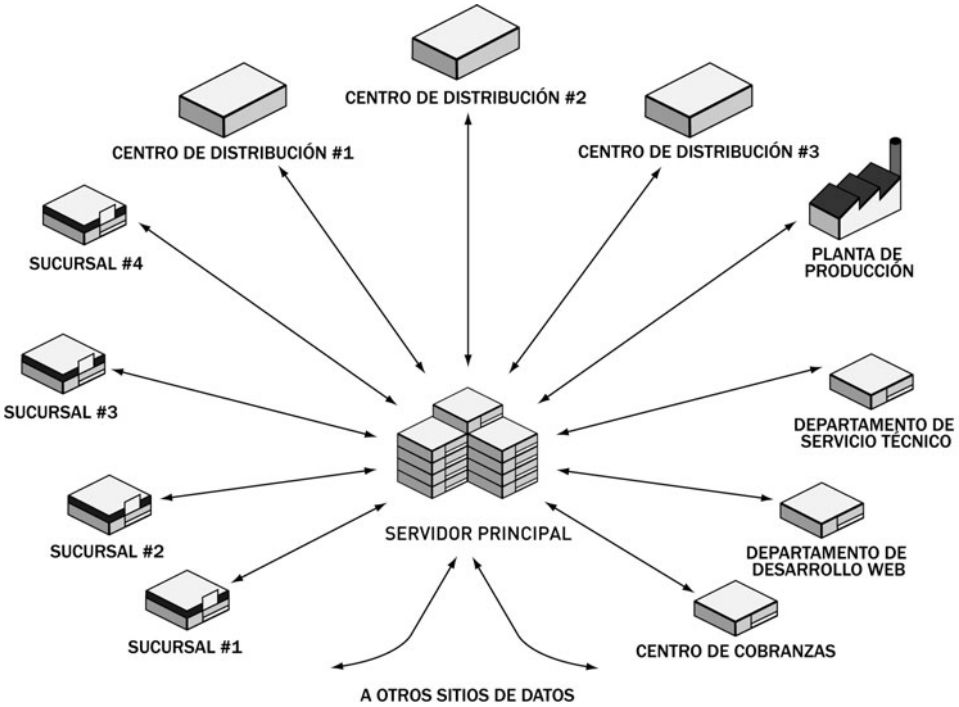


FIGURA 3.Una red WAN suele ser usada en ámbitos corporativos para conectar, por ejemplo, las redes LAN de dos sucursales distintas de una misma empresa.

DOCUMENTOS PRIVADOS

Muchas veces ocurre que, al margen de la existencia de la red, una misma computadora puede ser utilizada por varios usuarios. Si bien la configuración de seguridad de la red establece restricciones a los usuarios para el acceso a los datos disponibles en una computadora, éstos permanecen visibles para cualquiera que utilice el equipo a menos que definamos de manera explícita lo contrario.

Determinar diferentes usuarios para un mismo equipo nos da la posibilidad de que distintas personas mantengan sus datos completamente privados e invisibles para las otras personas que puedan acceder al equipo. La protección estará definida por una contraseña y un nombre de usuario que será pedido en cada inicio de sesión, y así podrá identificarse a qué documentos tendrá acceso cada usuario (**Figura 4**).

Si nuestra computadora no tiene aún una contraseña que restrinja el acceso a ella, podemos crearla desde el icono **`Cuentas de usuario`** del **`Panel de control`**. En **Paso a paso1**, veremos el proceso que nos permitirá hacerlo.

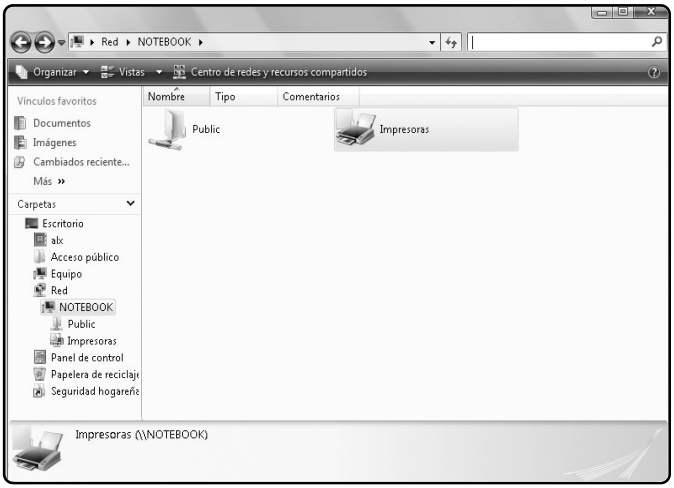


FIGURA 4.
Un cable verde y gris en el extremo inferior izquierdo indica que la carpeta `Acceso público` **puede ser utilizada por cualquier usuario de la red.**

Cuentas de usuario

Cuando varias personas utilizan el mismo equipo, es necesario crear tantas **cuentas de usuario** como usuarios existan. Cada cuenta puede estar protegida por una contraseña y, posteriormente, puede ser borrada.

La existencia de diferentes cuentas permitirá que los datos de cada usuario se conviertan en privados y que cada uno configure el equipo en general y cada aplicación en particular de la manera que le resulte más eficiente. Así, cada uno tendrá su propio grupo de favoritos, sus cookies y sus cuentas de correo. En el **Paso a paso 2**, veremos cómo crear nuevas cuentas de usuario.

Una vez creada la cuenta, el usuario podrá iniciar sesión en ella al reiniciar el equipo o al presionar la combinación de teclas **`WINDOWS+L`** y pulsar el botón **`Cambiar de usuario`**.

Aumentar la seguridad con un sensor biométrico

Para aumentar el nivel de protección y privacidad, en lugar de una contraseña para iniciar sesión, es posible emplear un **sensor biométrico**, que solo permita arrancar el equipo si las huellas dactilares del propietario son correctamente leídas. Algunas notebooks incorporan un sensor de fábrica. Si contamos con uno de estos equipos, no necesitaremos comprar un dispositivo dedicado para utilizar esta funcionalidad.

PASO A PASO /1
Convertir datos en privados

1

Haga doble clic sobre el icono **Cuentas de Usuario** del **Panel de control**. Si no ve la opción, haga clic en el vínculo **Vista clásica**.

2

Haga clic en el vínculo **Crear una contraseña para la cuenta**.
Una vez finalizado el proceso, siempre que inicie el equipo, se le pedirá la clave que creará.

3

Complete los campos **Nueva contraseña** y **Confirmar contraseña nueva**, con la contraseña que desee instalar en el equipo. En la línea **Escriba un indicio de contraseña**, puede escribir una palabra o frase que le sirva de recordatorio por si olvidara su contraseña. Presione **Crear Contraseña**.

PASO A PASO /2
Cómo crear nuevas cuentas de usuario

1

Haga doble clic sobre el icono **Cuentas de Usuario** del **Panel de control**. Luego, pulse clic en el vínculo **Administrar otra cuenta**.

2

El segundo paso es hacer clic en el vínculo **Crear una nueva cuenta** para crear una nueva cuenta de usuario de Windows.

PASO A PASO /2 (cont.)

3

Escriba un nombre para la cuenta creada en la línea **Nombre de la nueva cuenta**. Seleccione **Usuario estándar** y luego, haga clic en **Crear cuenta**.

4

La cuenta ha sido creada. Puede hacer clic sobre ella y, luego, sobre el vínculo **Crear contraseña** para establecer una nueva clave de acceso.

FIGURA 5.
Un mouse con sensor biométrico puede conseguirse en América Latina por un poco más del doble de dinero de lo que sale un dispositivo de este tipo de gama media-alta.

Por lo general, la primera vez que pasamos la huella dactilar por el lector se inicia el asistente para reemplazar el inicio con contraseña por el inicio vía lectura biométrica. Si nuestro equipo no cuenta con uno, deberemos hacer una pequeña inversión. Incluso existen algunos modelos de mouse con un sensor integrado, lo que nos ahorrará portar otro dispositivo (**Figura 5**).

Crear **la red**

Aunque muchos usuarios sintieron que la desaparición del **Asistente para la configuración de red** complicaba las cosas, la verdad es que establecer una red de hogar y pequeña oficina en Windows Vista resulta una tarea bastante sencilla.

Si usamos un concentrador cableado y conectamos el cable UTP a la placa de red, en forma automática, Windows detectará la conexión y nos ofrecerá elegir un perfil de protección predeterminado. Lo mismo ocurrirá si, en lugar de utilizar una opción cableada, nos conectamos vía Wi-Fi. Las opciones en ambos casos serán las siguientes:

- **Hogar**: la conexión para hogares permite el acceso a Internet y configura el firewall para que todas las conexiones de área local sean aceptadas. Se activa por defecto la detección de redes y se habilita el uso de la carpeta **Acceso público**.

- **Trabajo**: funciona del mismo modo que **Hogar**, establece la posibilidad de trabajar en una red LAN.

- **Pública**: esta opción es la indicada cuando utilizamos la conexión para ingresar directo en Internet (por ejemplo, si en el otro extremo del cable hay un

REDES CON XP Y VISTA

Los usuarios de Windows XP, en redes donde hay equipos con Windows Vista, pueden interactuar sin problemas. Deben asegurarse de que el **grupo de trabajo** utilice el mismo nombre que los equipos que corren en Vista.

módem) si estamos conectados a un concentrador público. Un ejemplo de esto podría darse en el caso de conectarnos desde un restaurante o un aeropuerto (**Figura 6**).

Una vez conectado el adaptador a cada uno de los equipos, para establecer la red, solo debemos configurar valores similares en el **Centro de redes y recursos compartidos** de Windows Vista. Para esto, todos deben haber establecido el tipo de ubicación como **Privada**. Quienes hayan hecho lo contrario, deberán abrir el **Centro de redes y recursos compartidos** desde el **Panel de control** y hacer clic en el vínculo **Personalizar** para poder elegir el tipo de ubicación correcta.

En el **Paso a paso 3**, veremos cómo configurar todas las variables sin problemas.

Aquellas redes que se encuentren montadas sobre un router, que administra la conexión a Internet, no pueden utilizar un proxy

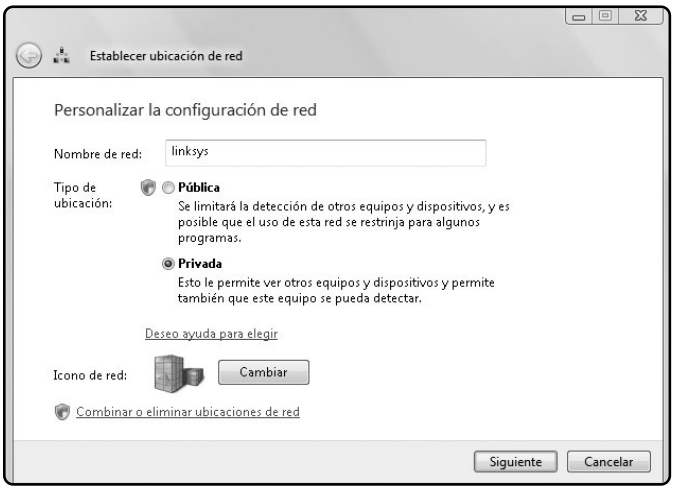


FIGURA 6. Hasta tal punto las opciones de `Hogar` y `Trabajo` son similares que, en la configuración personalizada de Windows, son tratadas como ubicación `Privada`.

PASO A PASO /3
Configurar una red en Windows Vista

1

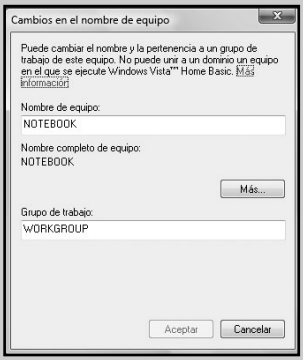
Haga clic en **`Inicio/Panel de Control`**. Luego pulse doble clic sobre el icono **`Centro de redes y recursos compartidos`**. Si no ve la opción, haga clic en el vínculo **`Vista clásica`**.

2

Despliegue el menú **`Detección de redes`**. Seleccione la opción **`Activar la detección de redes`**. Presione **`Aplicar`**.

PASO A PASO /3 (cont.)

3



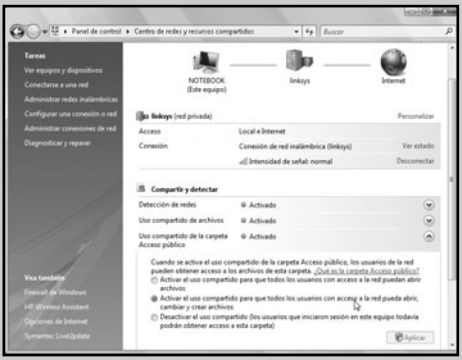
Confirme que, luego de la leyenda **Grupo de trabajo**, se indique el mismo grupo de trabajo que utilizan los demás equipos. De no ser así, presione **Cambiar configuración** y luego el botón **Cambiar…** para escribir en la línea **Grupo de trabajo** el nombre correcto.

4

Despliegue el menú **Uso compartido de archivos**. Seleccione el vínculo **Activar uso compartido de archivos**. Presione **Aplicar**. Repita el procedimiento con el menú **Uso compartido de impresoras**.

PASO A PASO /3 (cont.)

5



Despliegue el menú **Uso compartido de la carpeta Acceso público**. Seleccione el vínculo **Activar el uso compartido para que todos los usuarios con acceso a la red puedan abrir, cambiar y crear los archivos**. Haga clic en **Aplicar**.

6

Asegúrese de que el **Uso compartido con protección por contraseña** aparezca como **Desactivado**. De otro modo, despliegue el menú y seleccione la opción **Desactivar uso compartido con protección por contraseña**. Haga clic en **Aplicar** y cierre el **Centro de redes y recursos compartidos**.

Encriptación de datos

En este apartado, aprenderemos a utilizar una aplicación que nos permitirá mantener ocultos los datos, incluso para las personas que conozcan los datos de inicio de nuestra propia sesión (**Figura 7**).

Puede ocurrir que, en la oficina (o aun en algunos hogares), por determinada razón, todas las personas que comparten un mismo equipo utilicen el mismo usuario. Si bien esto no es recomendado en lo más mínimo, en la práctica es común verlo y resulta necesario buscar un método alternativo al momento de convertir los datos de un usuario en privados.

El método que recomendamos es la encriptación de datos. La **encriptación** es una tecnología que permite cifrar los datos seleccionados de modo que solo quienes conozcan la clave para su desencriptación puedan accederlos.

FIGURA 7.
Folder Lock **es una de las mejores aplicaciones de cifrado de datos y una de las pocas que se consigue en español.**

PARA SABER MÁS SOBRE ENCRIPTACIÓN

La **criptología** es el estudio de los sistemas que ofrecen medios seguros de transmisión de datos. Visitar el artículo publicado sobre este tema en la enciclopedia colaborativa en línea **Wikipedia** (**es.wikipedia.org/wiki/Criptolog%C3%ADa**), nos brindará más información.

Al cifrar una carpeta, lo que hacemos es ocultar su contenido para cualquier usuario que no posea la llave para volverla visible.

FOLDER LOCK 5.3.5

Existen en el mercado muchísimos programas dedicados a la encriptación de datos y a la administración de la información protegida. Por practicidad y facilidad de uso, trabajaremos en este momento con el programa **Folder Lock 5.3.5.**

Instalación

Para instalar el programa es necesario primero descargar el archivo de instalación, lo que podemos llevar a cabo de manera gratuita desde el sitio de descargas **CNet Download.com** (**www.download.com**) o de cualquier otra fuente de descarga como **Tucows** (**www.tucows.com**). También es posible, aunque a una velocidad bastante baja, descargarlo del sitio oficial, disponible en **www.newsoftwares.net/folderlock/spanish/**. Allí alcanzará con hacer clic sobre el vínculo **Descargar en español** y seleccionar un destino para la descarga (de aproximadamente 2 MB). En el **Paso a paso 4**, aprenderemos cómo instalar el producto.

Al ejecutar por primera vez el programa, necesitaremos tomar unos minutos para configurarlo. Lo primero será, inevitablemente, establecer una contraseña para su uso (**Figura 8**).

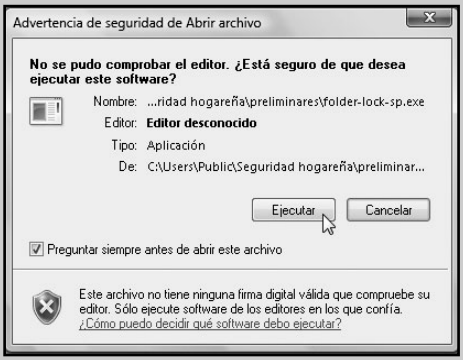
FIGURA 8. Al ejecutar por primera vez Folder Lock, se nos invitará a crear la contraseña. Debemos presionar `Ok` **en esta ventana.**

USO DE PROXY Y CONFIGURACIÓN DE PROGRAMAS

Una vez instalado un servidor proxy, los programas del equipo que se conecten a Internet necesitan actualizar su configuración. Esto resulta incómodo, pero refuerza la seguridad del equipo. Muchos programas toman los parámetros de configuración de Internet Explorer.

PASO A PASO /4
Instalar Folder Lock

1



Una vez completada la descarga del instalador, haga doble clic sobre el archivo descargado. En la advertencia de seguridad, presione la opción **Ejecutar**.

2

En la pantalla de bienvenida, pulse **Siguiente**. Seleccione **Acepto el acuerdo** y, luego, presione **Siguiente** en la ventana **Acuerdo de licencia**.

PASO A PASO /4 (cont.)

3

El programa le informará en qué carpeta va a ser instalado. Presione **Siguiente** para aceptar la opción predeterminada. Repita la acción en la ventana **Seleccionar el folder del menú Inicio**. Desactive la casilla de verificación **Create a Quick Launch icon** si no desea crear un acceso en la barra **Inicio rápido**.

4

Haga clic en **Instalar** para iniciar la copia de archivos. Pulse clic en **Finalizar** para ejecutar la aplicación.

Control parental

NAVEGADOR ACTUALIZADO

Muchos padres se preocupan por el consumo de Internet de sus hijos y recurren a aplicaciones de terceros para limitar el uso de juegos violentos, y la visualización de imágenes pornográficas o inapropiadas.

En el sitio **www.segu-kids.org/padres/control-parental-aplicaciones.html**, encontraremos una lista de los sitios y aplicaciones más recomendados.

MICROSOFT PRIVATE FOLDER

Si Folder Lock no resulta una opción adecuada para nuestras necesidades, podemos buscar otras alternativas. En el caso de contar con Windows XP como sistema operativo, una opción que es posible elegir para conocer sus funcionalidades, consiste en un software de Microsoft, que encripta carpetas, y cuyo nombre es **Private Folder**.

Nos permite establecer una contraseña para la carpeta **`My Private Folder`**. La mayor desventaja de este software es que si perdemos el password, no hay manera de recuperar los datos.

Usar el locker

Cada vez que el programa sea abierto y la clave introducida, automáticamente se abrirá el **locker**. El locker no es más que una carpeta donde arrastraremos los archivos que mantendremos encriptados. Para desencriptar un archivo, bastará entonces con sacarlo del locker (arrastrándolo y soltándolo en cualquier otra carpeta) para que otra vez pueda ser accedido por cualquiera que esté en condiciones de verlo. Mientras el programa se encuentre abierto, el locker estará desprotegido y, si lo cerramos, podremos volver a acceder a él, en la ruta **`C:\Program Files\Folder Lock\Locker`**.

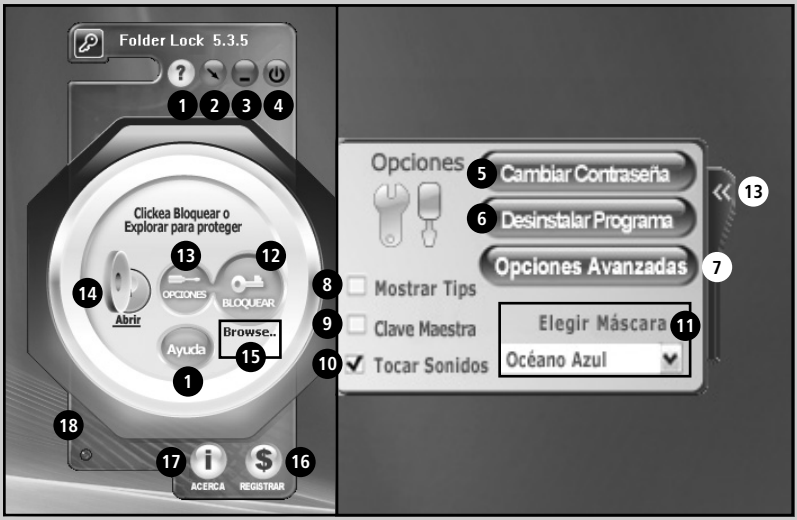
Cuando cerremos el programa, el locker será protegido y automáticamente cerrado. Para volver a acceder a él, deberemos ejecutar de nuevo el programa.

Desinstalación

Para evitar que otros usuarios administradores del equipo puedan desinstalar el programa, Folder Lock no puede ser removido desde la lista de **`Programas y características`** del **`Panel de control`**. En cambio, es necesario ingresar en el programa, abrir el **`Cuadro de Opciones`** y presionar el botón **`Desinstalar Programa`** para acceder al desinstalador. El proceso de desinstalación puede resultar un poco confuso, y será analizado en el **Paso a paso 5**.

Al momento de elegir el motivo de la desinstalación, los creadores de Folder Lock nos ofrecen información sobre el programa, una lista de preguntas frecuentes por si no entendimos su funcionamiento e, incluso, un descuento si consideramos que el precio es muy alto. Con estas opciones, los creadores del software intentan que sigamos usando su producto.

GUÍA VISUAL /1
Folder Lock XP



1. Abre la ayuda del programa.
2. Minimiza el programa a la zona de notificación de la barra de tareas.
3. Minimiza el programa.
4. Cierra el programa y lo bloquea.
5. Permite cambiar la contraseña de acceso al programa y, por ende, al locker.
6. Inicia el proceso de desinstalación.
7. Muestra las **`Opciones avanzadas`**.
8. Muestra consejos sobre el programa.
9. Habilita o deshabilita el uso de una clave para recuperar la contraseña del programa (solo en la versión registrada).
10. Habilita o deshabilita la ejecución de sonidos al presionar un botón del programa.
11. Permite elegir una máscara (**skin**) para cambiar la apariencia del programa.
12. Protege el contenido del locker.
13. Muestra u oculta el cuadro de opciones.
14. Abre el locker.
15. Permite seleccionar el bloqueo y desbloqueo de unidades y mover la carpeta de instalación del programa y el locker a un disco removible.
16. Opciones de registro del programa.
17. Muestra el cuadro **`Acerca de...`**.
18. Cuando destella, indica que se trata de una versión de prueba del programa.

PASO A PASO /5
Desinstalar Folder Lock

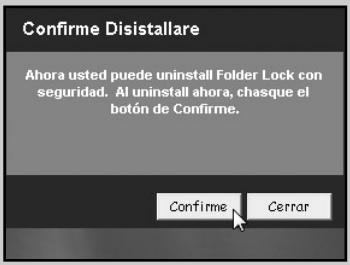
1

Abra el programa e ingrese su clave.

2

Cierre el locker y abra el **Cuadro de Opciones**. Haga clic en **Desinstalar programa** y, luego, en **Desinstalar**.

3



Presione el botón **Confirme** para comenzar el proceso de desinstalación.

PASO A PASO /5 (cont.)

4

Presione **My Locker** para mover los archivos del locker a su ubicación original.
Una vez movidos todos los archivos, pulse **OK**.

5

Necesita reiniciar el equipo para completar la desinstalación. Presione **Later** si planea reiniciar el equipo más tarde o **Reboot** para reiniciarlo en forma automática.

RESUMEN

Además de conocer los secretos para establecer y configurar una red confiable, en este capítulo hemos aprendido cómo hacer que la red local, fuente constante de amenazas, sea un espacio seguro. Ya sabemos cómo lograr que nuestros datos se conviertan en privados.

Multiple **choice**

1 **¿Qué es una red LAN?**

a- Una colección de redes pequeñas, dispersas en el área de un campus.
b- Dos o más redes de área local conectadas entre sí.
c- Una red que interconecta computadoras separadas por menos de 100 m.
d- Ninguna de las anteriores.

2 **¿Qué es una red WAN?**

a- Una colección de redes pequeñas, dispersas en el área de un campus.
b- Dos o más redes de área local conectadas entre sí.
c- Una red que interconecta computadoras separadas por menos de 100 m.
d- Ninguna de las anteriores.

3 **¿Las redes LAN se pueden establecer mediante cables o con acceso WI-FI?**

a- Solo con cables.
b- Solo con acceso WI-FI.
c- Las dos opciones son válidas.
d- Ninguna de las anteriores.

4 **¿Cuál de las siguientes opciones de perfil de red no corresponde a una predeterminada de Windows?**

a- Hogar.
b- Pública.
c- Trabajo.
d- Educación.

5 **¿Las redes que se encuentran montadas sobre un router que administra la conexión a Internet pueden utilizar un proxy?**

a- Siempre.
b- Nunca.
c- Depende del sistema operativo.
d- Depende de la marca del router.

6 **¿Podemos mantener los datos de inicio de sesión ocultos?**

a- No.
b- Sí, con la encriptación de datos.
c- Sí, con un firewall apropiado.
d- Ninguna de las anteriores.

Respuestas: 1a, 2c, 3c, 4d, 5b y 6b.

Capítulo 7

Sexto paso: navegar de forma segura

Analizaremos las prácticas básicas para resguardar la privacidad y la integridad de los datos.

RedUSERS.com

Luego de aprender a proteger la red y el equipo local en los capítulos anteriores, ahora iremos un paso más allá. Analizaremos qué prácticas hay que tener en cuenta para resguardar la privacidad y la integridad de los datos al navegar por Internet.

La **privacidad**

Las prácticas de navegación del usuario tienen una importancia central al momento de mantener el equipo libre de toda amenaza informática y, además, al intentar proteger la integridad de los datos y nuestra propia privacidad. En la mayoría de los casos, las prácticas que hacen a mantener la privacidad ayudan también a que el equipo se encuentre libre de virus y lejos de amenazas comunes. En este capítulo, aprenderemos cómo un usuario debe manejar sus datos para evitar la entrega de más información de la necesaria a proveedores que podrían usar ese contenido con fines malintencionados (**Figura 1**).

DATOS PERSONALES

Para pensar en una navegación segura, lo primero por tener en cuenta es el cuidado de la información

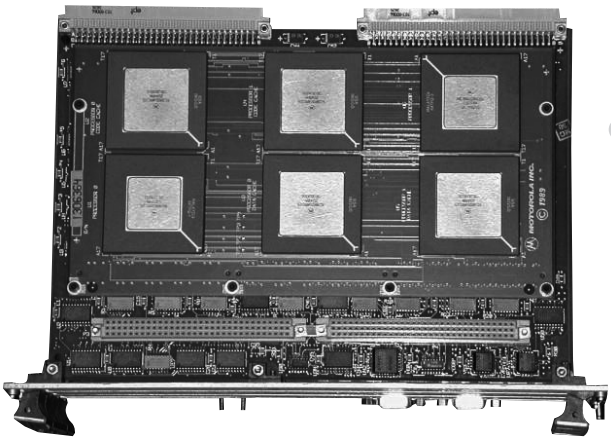


FIGURA 1.
Algunas empresas, como Motorola e IBM, comercializan chips encargados de proteger la seguridad del usuario, pero, si seguimos las pautas de este capítulo, será posible sentirnos seguros de una forma más económica.

RECOMENDACIONES PARA UNA NAVEGACIÓN SEGURA

En **www.vsantivirus.com/guia-de-supervivencia.htm**, encontramos un resumen de lo que se entiende por navegación segura. Este sitio nombra los comportamientos que hay que tener para navegar sin poner en riesgo nuestros datos ni nuestra información personal

personal del propio usuario. Las razones de esta medida son simples: mientras menos datos tengan los servidores remotos, menos en cuenta tendrán al equipo local. O sea que, para no ser blanco de ningún tipo de ataque, hay que ser lo más **anónimo** posible.

La primera regla, y tal vez la más importante de todas, es dar información personal solo en aquellos casos donde esta entrega se justifique. Además, debemos proporcionar datos a aquellas empresas cuya reputación consideremos confiable (**Figura 2**).

Muchos sitios cuentan con estrategias avanzadas para obtener la mayor cantidad de información personal del usuario, sin que éste tenga conciencia, de que están extrayéndole estos datos. Si bien la mayoría de los sitios que requieren un inicio de sesión ofrecen a sus visitantes la posibilidad de responder una pregunta secreta para recuperar la contraseña, algunos ofrecen preguntas cuyas respuestas pueden ser utilizadas para averiguar información personal como "¿Cuál es el apellido de soltera de mi mujer?" (**Figura 3**).

FIGURA 2.
No es una buena idea completar formularios exhaustivos para poder descargar aplicaciones sencillas.

NO PASAR POR ALTO LAS ADVERTENCIAS

Los servicios de correo electrónico web suelen incluir efectivos antivirus que protegen los datos adjuntos que recibimos. Sin embargo, si no prestamos atención a las advertencias de estos servicios, de cualquier modo nos infectaremos.

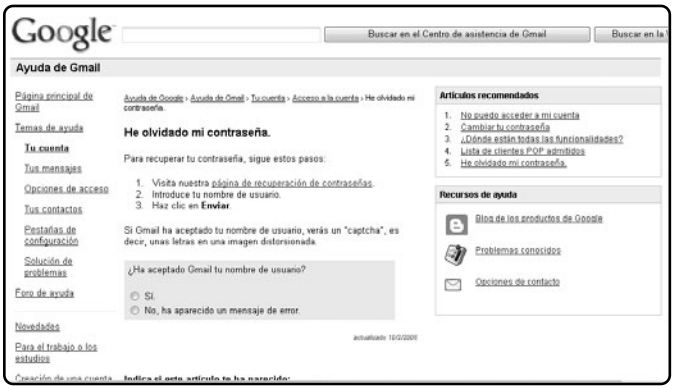


FIGURA 3. Los sitios más confiables tienen complicados sistemas de recupero de contraseñas. Pero no preguntan información personal para restablecer datos secretos.

Hay que **desestimar** el uso de ese tipo de preguntas para resguardar la privacidad y, en lo posible, mantenerse alejado de sitios que utilicen estas prácticas **fraudulentas**.

Por último, es importante recordar que las computadoras de **uso público** son aquellas en las que hay que tener mayor cuidado. Esta regla, tan básica, es muchas veces pasada por alto por una importante cantidad de usuarios de computadoras compartidas o públicas. Siempre que se utilice un equipo que luego puede ser usado por otra persona, resulta imprescindible desconectarse de los servicios a los que nos hubiésemos conectado. También es indispensable cerrar navegadores web y, en lo posible, reiniciar o pedir al encargado del lugar que reinicie el equipo. En los últimos tiempos, la mayoría de los locales que ofrecen servicio de Internet al público (conocidos como CiberCafés o CiberCentros) han incorporado sistemas de control que reinician los equipos y limpian la información personal de manera automática al recibir el pago del cliente (**Figura 4**).

ENCRIPTACIÓN

Al momento de cerrar una transacción electrónica y de brindar información crítica, como números de tarjeta de crédito o débito, es fundamental asegurarse de que el sitio con el que estamos tratando utilice la tecnología **Secure Socket Layer** o

CENTRO DE PROTECCIÓN

Microsoft ofrece a los usuarios del sistema operativo Windows, en **www.microsoft.com/latam/ athome/security/default.mspx**, el **Centro de Protección**. Este sitio es recomendable para todos los que quieran probar sus conocimientos sobre la protección de sus datos.

FIGURA 4.
Los programas de gestión para CiberCafés o CiberCentros permiten a los encargados reiniciar los equipos de los usuarios después de cada sesión.

Secure Electronic Transaction. Estas tecnologías (la última diseñada en especial para encriptar números de tarjetas de crédito) se encargan de proteger los datos enviados al sitio web para que nadie pueda verlos o hacerse de ellos.

Secure Socket Layer (**SSL**) es utilizada para validar la identidad de un sitio web a la vez que crea conexiones seguras que habiliten el envío de datos críticos. Secure Electronic Transaction (**SET**) es un protocolo creado por Visa y MasterCard para transmitir los números de las tarjetas de créditos mediante encriptación. Este método se conoce también como **criptografía**. Al utilizar técnicas criptológicas, el mensaje es descompuesto según una tabla criptológica, y su contenido (en este caso, los números de la tarjeta) se convierte en ininteligible. En cuanto el receptor, que es certificado mediante una firma digital, demuestra su identidad, recibe la tabla criptográfica y está en condiciones de leer o desencriptar su mensaje.

LA IMPORTANCIA DEL NAVEGADOR ACTUALIZADO

En lo que se refiere a seguridad, es de gran importancia contar con un navegador actualizado para prevenir el robo de cualquier información personal disponible en nuestro equipo. Aunque es el más usado, Internet Explorer resulta, más inseguro que otras alternativas.

Muchos sitios, para asegurar las identidades del emisor y del receptor, utilizan también técnicas esteganográficas. La **esteganografía** es una técnica utilizada para ocultar un mensaje o un dato (en este caso, la identidad del emisor y del receptor) en un canal puro de información distinto al original del mensaje, por ejemplo, ocultando texto en una imagen. Así, algunas páginas web nos obligan a escribir texto desparramado en una imagen para confirmar que somos quienes decimos ser y no un equipo remoto probando combinaciones (**Figura 5**).

Para saber si un sitio cuenta o no con estas tecnologías, existen dos indicadores visuales en la pantalla, a saber, el **icono de un candado** en la barra de estado del navegador y el encabezado **https** en la dirección del sitio web (**Figura 6**).

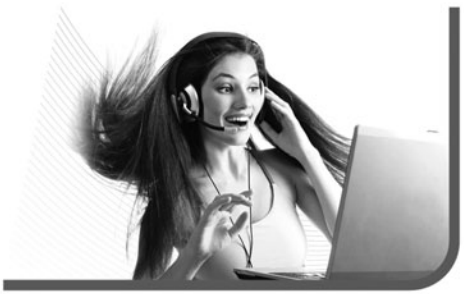


FIGURA 5. Los sitios de descargas en línea utilizan muy seguido técnicas esteganográficas para evitar abuso en las descargas.

Si pulsamos clic sobre el icono del candado, tendremos acceso a información acerca del tipo de conexión propuesta por el sitio, así como también de quién certifica su seguridad.

Además, desde el menú desplegable, podremos acceder al certificado de seguridad si hacemos clic en **`Ver certificados`**. Allí encontraremos detalles de la entidad emisora y sus fechas de emisión y vencimiento (**Figura 7**).

FALTA DE DECLARACIÓN DE PRIVACIDAD

Si el sitio que visitamos no exhibe su declaración de privacidad, es posible escribir al administrador del sitio pidiendo este documento. Todas las páginas que manejen información personal cuentan con una declaración y deberían dejarla al alcance de cualquier cibernauta.

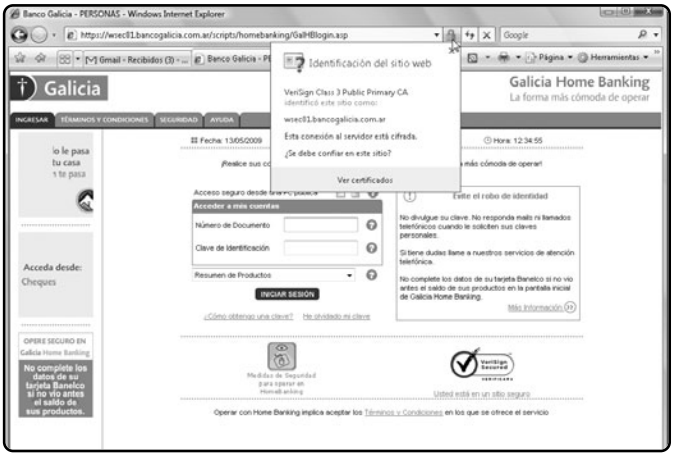


FIGURA 6. Independientemente del navegador que utilicemos, el icono del candado indicará que estamos en un sitio seguro. Al hacer clic sobre él, veremos más información de seguridad.

FIGURA 7. Este certificado corresponde a una entidad bancaria. En `Declaración del emisor`, hallaremos datos de contacto de la entidad que otorgó el certificado.

INTERNET EXPLORER SEGURO

Muchas veces hemos hablado en este libro sobre las conocidas falencias de seguridad del explorador de Internet de Microsoft. A pesar de sus problemas, este programa sigue siendo el navegador que más usuarios utilizan en el mundo, por lo que quienes lo usen deberán extremar las medidas de seguridad para correr la menor cantidad posible de riesgos.

Uno de los puntos críticos asociados a la privacidad del usuario es la administración de cookies. Los sitios de Internet colectan de manera continua información sobre los visitantes mediante el uso de estos documentos. Además de analizar qué ha hecho un sitio con la información que tomó del equipo visitante es posible definir el modo en el que Internet Explorer (**Figura 8**) administrará las cookies para compartir la menor cantidad posible de información o, incluso, prohibir su uso. Hay que tener cuidado con esta última opción porque muchos sitios no funcionan sin las cookies habilitadas.

FIGURA 8.
Para contar con un navegador actualizado, la versión 8 de Internet Explorer puede descargarse del sitio oficial www.microsoft.com/latam/windows/internet-explorer/default.aspx.

¿Qué es una cookie?

Una **cookie** es un pequeño archivo de texto que los sitios web pueden crear en el equipo del visitante para guardar información personal que el usuario haya decidido compartir así como también datos sobre qué hizo en el sitio, qué links visitó, configuraciones personales y otra información. También los anunciantes del sitio pueden crear cookies en el equipo, conocidas como **cookies de terceros**.

La utilización de cookies permite que un sitio identifique a una computadora y, por lo tanto, a un usuario. De este modo, el sitio podrá ofrecer un servicio por demás personalizado para el navegante, y hasta incluso guardar su nombre de usuario y contraseña (**Figura 9**).

El uso de cookies hace de la navegación una actividad más cómoda y dinámica, y permite a su vez que los cibernautas puedan personalizar a su gusto los sitios para hacer de las tareas rutinarias algo más automático. Asimismo, las cookies ahorran tiempo y ancho de banda en tanto evitan el tráfico redundante de información que ya fue descargada alguna vez.

Además, permiten mostrar solo aquellos datos que son importantes para el usuario. Sin embargo, los sitios pueden utilizar la información recolectada

SPYBOT SEARCH & DESTROY Y LAS COOKIES

Spybot Search & Destroy, nos ayudará muchísimo en la protección contra agujeros de privacidad causados por el mal uso de las cookies. Con este software, podremos eliminar todas las cookies que pongan en riesgo la seguridad del equipo y los datos.

en las cookies con fines comerciales o de otro tipo no deseados por el usuario. Así, si alguien visita en forma constante en el sitio web de un periódico la sección deportiva, el administrador web podría mostrar directamente esa sección en la portada, pero también podría ofrecer publicidad de indumentaria futbolística o espectáculos relacionados que el usuario no pidió. Por este motivo, hay que administrar correctamente el uso de cookies para controlar qué utilidad se le da a la información que el sitio tiene de cada uno de nosotros.

Administrar cookies con Internet Explorer

Es posible configurar cualquier navegador de Internet de modo que acepte solo la creación de las cookies que el usuario considere **necesarias**. Es importante destacar que cuantas menos cookies sean aceptadas más incómoda resultará la navegación, ya que los sitios web siempre se verán como la primera vez que los visitamos. Incluso, algunas páginas requieren que las cookies estén activadas para funcionar y, sin ellas, no son mostradas. Este punto representa un aspecto fundamental para considerar en este caso.

Internet Explorer llama **`Control de privacidad`** al control de cookies y configura por defecto un nivel de privacidad **`Medio`**, que permite una navegación funcional y bloquea ciertas cookies de terceros para reducir la publicidad no deseada. Si queremos cambiar el nivel de privacidad, debemos hacer clic en el

FIGURA 9.
Los sitios que permiten recordar nombres de usuario y contraseña, así como otras configuraciones personalizables, requieren del uso de cookies para funcionar de manera correcta.

USO DE LA TARJETA DE CRÉDITO EN INTERNET

Los usuarios que quisieran saber más sobre lo seguro que resulta utilizar la tarjeta de crédito en compras en línea pueden leer el informe de **www.vsantivirus.com/20-05-02.htm**. La seguridad es, en Internet, directamente proporcional al nivel de responsabilidad del usuario.

menú **Herramientas/Opciones de Internet** de Internet Explorer; allí seleccionamos la solapa **Privacidad**. Luego deslizamos la barra hasta encontrar el nivel que más se adapte a nuestras necesidades (**Figura 10**).

Los predeterminados de privacidad son los siguientes:

• **Aceptar todas las cookies**: permite que cualquier sitio utilice con cualquier fin cookies en el equipo local. No es recomendado de ninguna manera.

• **Baja**: ofrece un altísimo nivel de funcionalidad en la navegación, en tanto solo evita las cookies de terceros, pero permite administrar información personal de cualquier tipo por cualquier sitio. Si bien supone una importante mejora en el nivel de funcionalidad de la navegación, resulta peligroso a menos que se utilice un gestor de cookies de terceros.

FIGURA 10. El botón `Importar`, nos permitirá agregar niveles de seguridad creados por el administrador de nuestra red.

• **Media**: es el nivel predeterminado, y ofrece la mejor relación entre seguridad y funcionalidad. Además de bloquear cookies de terceros, evita que se guarde información personal sensible que podría ser utilizada con fines comerciales.

• **Media Alta**: aumenta el nivel de seguridad en relación con el punto anterior en tanto tampoco permite guardar cookies originarias del sitio (y no de sus auspiciantes) que incluyan información personal.

• **Alta**: bloquea todas las cookies que pretendan ser creadas sin el consentimiento explícito del

MICROSOFT Y LOS SITIOS DE SUBASTA

Microsoft tiene su visión de la seguridad en las subastas en línea. En **www.microsoft.com/latam/athome/security/online/auctionsell.mspx** presenta un artículo recomendado para todos los que utilicen asiduamente estos sitios y para los que aún no se hayan animado.

usuario. Algunos sitios no pueden funcionar con este nivel de seguridad.

• **Bloquear todas las cookies**: se bloquean todas las cookies, y los sitios web que anteriormente hubiesen generado cookies en el equipo no pueden tampoco acceder a ellas. El nivel de funcionalidad en la navegación se reduce de manera drástica, factor que debemos considerar en especial, si nos inclinamos por esta alternativa (**Figura 11**).

Al margen de la directiva de privacidad general, es posible definir sitios donde el uso de cookies esté permitido y sitios donde esté bloqueado en su totalidad. Para ello, habrá que presionar el botón **Sitios** de la solapa **Privacidad** de las **Opciones de Internet** del navegador y, luego de escribir la dirección del sitio, presionar **Bloquear** o **Permitir**.

Esto es muy recomendable, en tanto nos permite utilizar un nivel **Medio** de seguridad sin riesgo de infectar el equipo. Las actualizaciones de Windows actúan sobre la lista de sitios bloqueados cada vez que se descarga una nueva actualización para **Windows Defender** (**Figura 12**).

A veces, es posible pasar por alto la directiva de privacidad del sistema y administrar las cookies de un modo manual. Con el botón **Avanzada** de la solapa

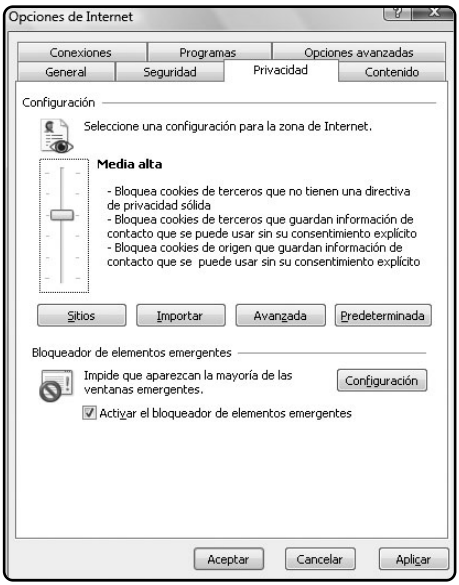


FIGURA 11. El botón `Predeterminada` nos permitirá regresar al nivel de privacidad por defecto, si la navegación perdiera funcionalidad, luego de algún cambio.

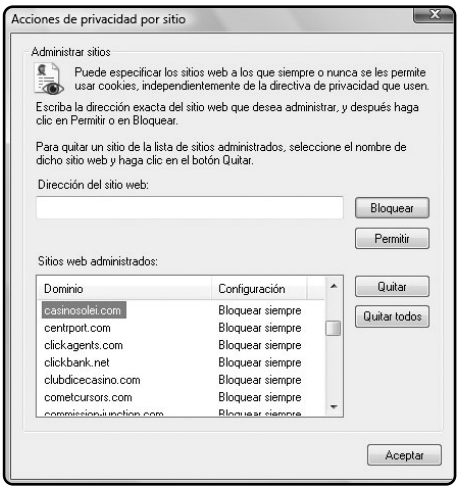


FIGURA 12. Una vez bloqueado o liberado un sitio, es posible quitarlo de la lista de excepciones seleccionándolo y presionando luego `Quitar`.

Privacidad, accederemos a un cuadro que permitirá especificar qué hacer con las cookies de los diferentes sitios y con las cookies de terceros. No se recomienda el uso de esta opción en tanto el uso de la directiva general, además de la especificación de sitios, debería ser suficiente para establecer una navegación funcional y a la vez segura.

Si todavía queremos utilizarla, debemos marcar la casilla **Invalidar la administración automática de cookies** y presionar **Aceptar** (**Figura 13**).

FIGURA 13. Al tildar la casilla `Aceptar siempre las cookies de una sesión`**, aquellas que identifiquen los nombres de usuario y contraseña a sitios que los requieran serán permitidas para así automatizar los accesos.**

Bloqueador de ventanas emergentes

Esta función (también conocidas como **bloqueador de POP-ups** o **POP-up blocker**) evita la aparición de esas molestas ventanas que se abren (pop-ups) sin que el usuario las haya pedido y que muestran, en la mayoría de los casos, publicidades no deseadas.

El bloqueador de ventanas puede activarse y desactivarse tildando la casilla de verificación **Activar el bloqueador de ventanas emergentes** en la solapa **Privacidad** del cuadro **Opciones de internet**. Las excepciones pueden definirse presionando el botón **Configuración**.

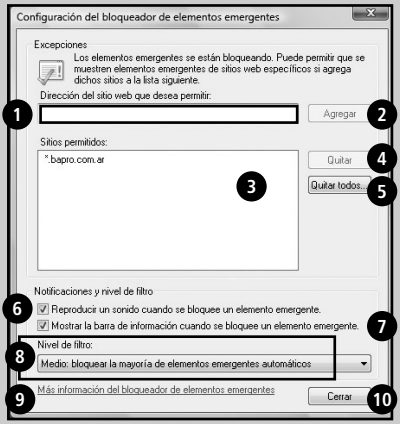
Informe de privacidad

Es posible ver el **informe de privacidad** de los últimos sitios visitados y del sitio en el cual Internet Explorer se encuentra actualmente.

BLOQUEO DE VENTANAS EMERGENTES

Es común que algunos sitios pidan los datos de inicio de sesión con una ventana emergente. En la barra de herramientas, una línea amarilla notificará el bloqueo, y alcanzará con hacer clic sobre ella para abrir la ventana y admitir su aparición de allí en adelante.

GUÍA VISUAL /1
Bloqueador de ventanas emergentes



1. En este campo, se debe ingresar la dirección web a la que se permiten todos los elementos emergentes para el sitio.
2. Agrega a la lista de sitios permitidos la dirección escrita en la línea **`Dirección del sitio web que desea permitir`**.
3. Muestra los sitios donde los elementos emergentes están permitidos.
4. Quita de la lista de permitidos el sitio seleccionado en la lista **`Sitios permitidos`**.
5. Borra todos los sitios de la lista **`Sitios permitidos`**.
6. Indica si se reproducirá un sonido o no al bloquear un elemento emergente.
7. Especifica si se mostrará o no la barra de información debajo de la barra de herramientas, al bloquear un elemento emergente. No es recomendable desactivar esta opción.
8. Establece el nivel del filtro. En una máquina sin adware ni spyware, el nivel **`Medio`** debería ser suficiente y funcional a la vez. **`Alto`**: bloquea todos los elementos emergentes a menos que se haga clic sobre un vínculo presionando **`CTRL+ALT`**; **`Bajo`**, permite todas las ventanas emergentes de los sitios considerados seguros.
9. Abre la guía de preguntas frecuentes para el bloqueador de elementos emergentes. Esta guía es un documento informativo sobre el modo en el que el programa funciona.
10. Cierra el cuadro y acepta las opciones seleccionadas.

Datos útiles para tener en cuenta

APLICACIONES P2P LIMPIAS

Los programas de intercambio de archivos suelen ser los que más adware y spyware incluyen, y sus usuarios los que menos leen el contrato de licencia. El sitio VSAntivirus publicó en **www.vsantivirus.com/lista-p2p.htm** una lista actualizada de los software de intercambio que incluyen software no deseado y los que no lo hacen.

TARJETAS SEGURAS

Algunos bancos ofrecen a sus clientes tarjetas de crédito y débito con **contraseñas diferenciales** para ciertos servicios. Así, envían junto con la tarjeta una grilla de números y letras, y no preguntan al usuario por un número fijo, sino por los datos de las coordenadas de la grilla. Esto aumenta la seguridad de las transacciones electrónicas.

CARACTERES ADMITIDOS

Algunos servidores no admiten el uso de ciertos símbolos en las contraseñas. Como mínimo, cualquier servidor permitirá utilizar letras, números y símbolos universales además de distinguir entre mayúsculas y minúsculas.

Un informe de privacidad es un documento que da cuenta del modo en el que el sitio en cuestión utiliza la información del navegante y ofrece información sobre las entidades que certifican la propuesta del sitio.

Hay que hacer clic en el ítem **Directiva de privacidad de la página web…** del menú **Página** del navegador para acceder al informe que mostrará, en primer lugar, el sitio actual y, luego, una lista con todos los demás sitios visitados (**Figura 14**).

FIGURA 14. Al hacer clic en `Configuración`, accederemos a la solapa `Privacidad` del cuadro `Opciones de Internet`.

Para poder leer el informe completo de privacidad para un sitio, hay que hacer doble clic sobre él en la lista o seleccionarlo y presionar el botón **Resumen**. Así, se verá una ventana como la de la **Figura 15** que, a la vez, dará la opción de decidir cómo será la utilización de cookies para el sitio web informado.

Al finalizar el libro, encontraremos dos apéndices. En el primero, hallaremos todo sobre el spam y cómo evitarlo. En el segundo, conoceremos programas alternativos a los que vimos hasta ahora.

En Configuración, en el vínculo Obtener más información acerca de las cookies, veremos un documento sobre temáticas relacionadas

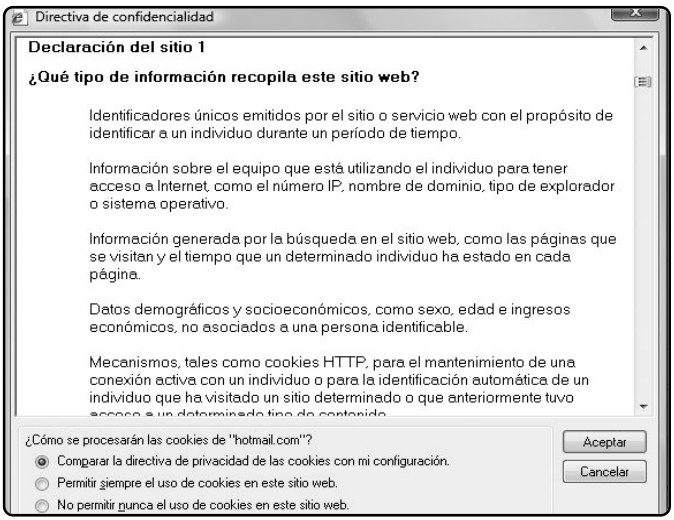


FIGURA 15.
Al leer la `Directiva de confidencialidad` **de un sitio, nos estaremos informando al detalle de las políticas del sitio para el manejo de información del usuario e, incluso, de ventanas emergentes de cualquier tipo.**

RESUMEN

Ahora que sabemos cómo manejarnos sin riesgos en la Web, si contamos también con un equipo cuya configuración de seguridad es correcta y además somos usuarios responsables, habremos vencido definitivamente los ataques informáticos.

Multiple **choice**

1 ¿Qué software podemos utilizar para proteger los agujeros de privacidad causados por el mal uso de las cookies?

a- Windows Sidebar.
b- Spybot search & destroy.
c- OldVersion.
d- Firefox.

2 ¿Qué genera el uso de cookies?

a- Una navegación más lenta.
b- Una navegación más rápida y dinámica.
c- Un cambio en la interfaz del navegador.
d- Ninguna de las anteriores.

3 ¿En Internet Explorer, es posible ver el informe de privacidad de los últimos sitios visitados?

a- Sí.
b- No.
c- Solo en Windows 7.
d- Ninguna de las anteriores.

4 ¿En Internet Explorer, se puede activar el bloqueador de ventanas emergentes?

a- Sí.
b- No.
c- Solo en Windows 7.
d- Ninguna de las anteriores.

5 ¿Cuáles son las aplicaciones que contienen más adware y spyware?

a- Las de la suite Office.
b- Las de la suite Adobe.
c- Los programas de intercambio de archivos.
d- Ninguna de las anteriores.

6 ¿Cuál de los siguientes niveles de privacidad de Internet explorer solo evita las cookies de terceros?

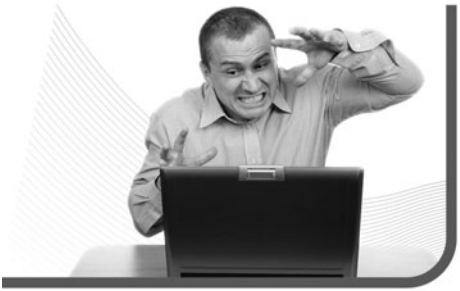
a- Aceptar todas las cookies.
b- Baja.
c- Media.
d- Alta.

Respuestas: 1b, 2b, 3a, 4a, 5c y 6b.

Apéndice
Spam

Veremos, en este capítulo,
el más molesto de los ataques
contra el usuario: el spam.

A lo largo de este libro, hemos analizado todas las amenazas que derivan en problemas técnicos de la computadora: bajas en el rendimiento, ventanas que se abren inexplicablemente todo el tiempo, conexiones robadas y redes inseguras. Veremos, en este capítulo, el más molesto de los ataques contra el usuario: el spam.



Orígenes y razones de su existencia

El **spam** es el correo electrónico que recibimos sin haberlo pedido. Por lo general, es de corte comercial y se envía de manera indiscriminada a múltiples destinatarios, por usuarios que suelen mantenerse en el anonimato. También se llama de esta forma a los mensajes comerciales enviados a listas de correo y foros.

El spam es, además, conocido como **UCE** (**Unsolicited Comercial Email** o correo comercial no solicitado); **UBE** (**Unsolicited Bulk Email** o correo genérico no solicitado); correo gris (**grey mail**) o, simplemente, **correo basura** (**junk mail**). El spam es utilizado con propósitos de venta y, en algunos casos, para difundir comentarios de corte político o social (**Figura 1**).

Mucha gente también afirma que spam significa **sales promotional advertising mail** (correo publicitario promocional de ventas) o **simultaneously posted advertising message** (mensaje de propaganda enviado en forma simultánea).

El spam es recibido por el usuario, por lo general, como un e-mail con un dudoso contenido que incita a la compra de algún producto, cuya procedencia es, en la mayoría de los casos, incierta. Lo que siempre debemos tener claro, aunque este tipo de mensaje ofrezca precios y productos por demás convenientes, es que **jamás** se debe acceder a los sitios de compra propuestos o dejar un número de tarjeta para la compra del producto.

El spam deriva la mayoría de las veces en estafas o crímenes digitales. Desafortunadamente para los

LEYES ANTISPAM

En el sitio **www.spamlaws.com**, podremos encontrar el texto completo de todas las leyes antispam existentes en el mundo. Si bien solo pocos países han legislado sobre este tema, conocer sus medidas es importante para plantear un futuro libre de correo basura.

FIGURA 1.
Los vínculos que se incluyen en el spam apuntan a confirmar que nuestra dirección de correo existe para mandarnos cada vez más correo basura.

usuarios y con suerte para los **spammers**, está confirmado que el spam funciona. En tanto el e-mail es un medio de publicidad bastante barato, mientras que una pequeñísima parte de los mensajes enviados sean respondidos, el engaño habrá surtido efecto.

¿POR QUÉ ENVIAR SPAM?

El spam existe porque, como ya hemos dicho, funciona. Si tenemos en cuenta que el e-mail es un recurso gratuito, entenderemos el gran negocio que es enviar mil mensajes aun cuando solo dos o tres surtan efecto. Por lo general, los sitios de Internet se benefician no solo por la venta, sino también por el simple hecho de que un usuario ingrese en ellos. De este modo, si a cada spammer se le pagara una pequeña suma de dinero, por mínima que fuese, cada vez que alguien visitara un link enviado mediante el spam, incluso, cuando de mil correos enviados respondiera solo uno el asunto, esto resultaría ser un negocio. Si se tiene en cuenta que los spammers suelen mandar millones y millones de correos diarios, queda claro que las ganancias se multiplican.

Los spammers utilizan, para reenviar sus mensajes de correo, listas que pueden conseguirse con facilidad. Por este motivo, hay que tener cuidado a la hora de informar a diferentes empresas sobre nuestra dirección de e-mail. Es probable que, cuando completemos un formulario para un sorteo en la calle, la dirección que introduzcamos vaya de manera directa

GLOSARIO ANTISPAM

En el sitio del antivirus **Sophos**, existe un interesante glosario para todos aquellos que quieran saber más sobre el spam y sus prácticas asociadas. La guía está escrita en castellano, se puede leer en **http://esp.sophos.com/security/spam-glossary.html**.

a una lista que será utilizada para reenviar correo basura o, peor aún, será vendida a spammers que pretenden aumentar su negocio (**Figura 2**).

Las medidas cada vez más sofisticadas de los **filtros de spam** -hablaremos de ellos más adelante- en servidores y computadoras personales hace que la llegada de correos basura sea cada vez menor. Sin embargo, esto obliga a los spammers a mandar más y más mensajes para que el rendimiento del negocio se mantenga, lo cual hace aumentar la complejidad de la vida de los usuarios sin protección.

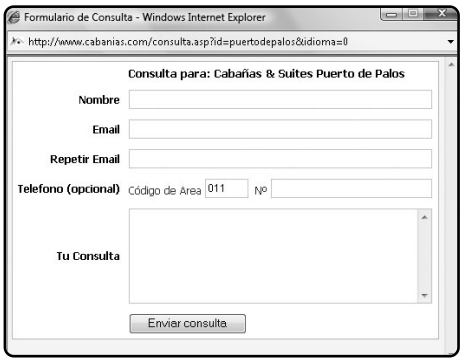


FIGURA 2. Cualquier sitio con el cual contactemos nos pedirá una dirección de correo electrónico. Si la empresa no es confiable, conviene leer la declaración de privacidad.

Quienes negocian con el spam suelen decir que sus prácticas son legales. Se escudan en el hecho de que, tanto en radio como en TV -y mucho más en Internet- los consumidores reciben muchísima publicidad que nunca pidieron. Además, afirman que su técnica no consume tiempo de los usuarios, que pueden elegir no abrir los correos, ni recursos naturales como sí consumen las publicidades en papel. Desde ya, todos sus argumentos son muy discutibles.

Cómo evitar el spam

Revisada la historia reciente de la problemática del spam, queda claro que este tipo de ataque está alineado con los adware y spyware, más alejado de virus y otros ataques. Como pasa con los primeros, para prevenir el ataque del spam es muy necesario contar con una serie de políticas de navegación especialmente duras. Porque, como ocurre con los adware y spyware, las herramientas de protección y de limpieza son por lo general insuficientes y, a medida que la casilla de correo recibe mayor cantidad de spam, aumenta la dificultad para limpiarla. De hecho, en el caso del spam, es muy importante,

NUNCA RESPONDER

Muchos correos electrónicos basura incluyen, sobre el final, un párrafo declarando que el mensaje no puede ser considerado spam, mientras el usuario pueda ser removido de la lista. Jamás debemos responder a estos mensajes.

incluso, que evitemos comenzar a recibirlo ya que, en cuanto nuestra dirección forma parte de una lista, es probable que en poco tiempo sea distribuida a otras. Entonces, ya no habrá posibilidad de parar la recepción de correos basura, salvo con el uso de herramientas dedicadas (**Figura 3**).

Las políticas para navegar sin correr el riesgo de convertirnos en receptores constantes de spam van más allá del simple uso habitual de Internet y sus derivados. De hecho, muchísimas veces, la dirección de correo electrónico de un usuario es puesta en peligro en eventos públicos y concursos ocurridos lejos de una computadora. La regla de oro es, entonces, no facilitar nunca a nadie nuestra dirección de correo electrónico a menos que la reputación del solicitante amerite la excepción. Por eso es que jamás debe anotarse la dirección de correo en encuestas y sorteos públicos. Mucho menos, debemos proporcionarla a instituciones de cualquier tipo, a menos que sea realmente necesario para recibir informes deseados o datos de inicio de sesión.

De no seguir estos consejos, es muy probable que a las pocas semanas de haber entregado la dirección la casilla brindada comience a llenarse de correo

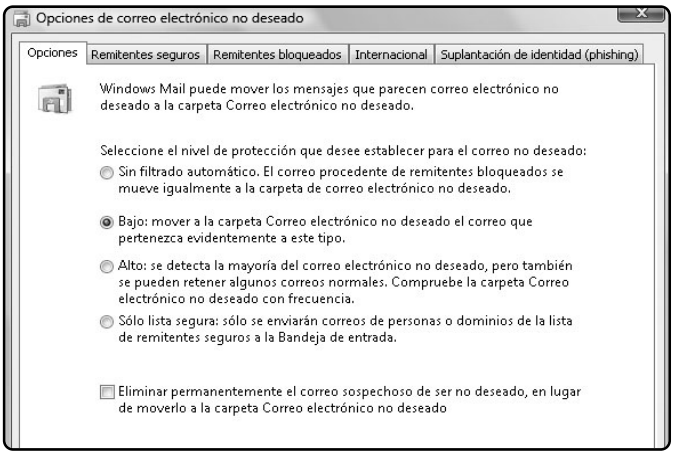


FIGURA 3.
Aunque los servicios web y locales tienen herramientas de prevención cada vez más efectivas, evitar poner en riesgo la dirección de correo sigue siendo lo más efectivo.

LUCHADORES ANTISPAM

En **http://spam.abuse.net/**, se congregan los desarrolladores y creadores de productos web que intentan luchar contra el spam. Si somos parte de la comunidad de desarrolladores o queremos ayudar a eliminar esta molesta amenaza, no dejemos de visitar este sitio.

basura, proveniente de remitentes desconocidos. Esto habrá tenido que ver, sin duda alguna, con que la información proporcionada a empresas de dudosa seriedad, cruzada con datos personales obtenidos del mismo formulario o de la Web, fue utilizada para introducirnos en una lista de correo de la que difícilmente seremos eliminados (**Figura 4**).

Hoy en día, muchos de los proveedores de servicios de Internet aplican filtros antispam en sus servidores de correo. Para esto, suelen clasificar los mensajes y agregar un texto del siguiente tipo a la línea **Asunto: [SPAM??]**. Con esto, ayudan a los usuarios a detectar los mensajes spam.

Otras técnicas pueden ser muy simples y muy efectivas también a la hora de lidiar con el spam: los mensajes que incluyen la dirección de correo en el campo **CC:** o **CCO:** solamente y contengan muchos destinatarios, es probable que sean correo no deseado. Tener en cuenta estas dos cosas, a la vez que los cuidados antes mencionados en este capítulo, puede liberar de esta molestia a los usuarios más cuidadosos (**Figura 5**).

USO DE REGLAS

Si encontramos la forma de detectar correo basura en la bandeja de e-mails de nuestro cliente de correo favorito, podremos configurar una regla de correo para eliminar de forma más rápida los mensajes basura.

FIGURA 4.
Muchas empresas exigen una cuenta de e-mail para iniciar una sesión. Es importante en estos casos leer la declaración de privacidad de la compañía para saber qué se hará con nuestra información personal.

FIGURA 5.
Los ISP más conocidos suelen ofrecer filtros antispam por software de dudosa efectividad, como complemento a sus servicios de Internet.

Para esto debemos contar, desde ya, con una cuenta de correo de tipo **POP3** y un cliente de correo como **Eudora**, **Thunderbird** o **Windows Mail**. Analizaremos como ejemplo la creación de reglas en el cliente de correo gratuito de Microsoft, **Windows Mail** (antes conocido como **Outlook Express**).

La idea será, entonces, crear una regla de correo que filtre los mensajes de modo que aquellos que estén marcados en su línea **`Asunto`** como spam sean automáticamente señalados como leídos y movidos a una carpeta que llamaremos **`SPAM`**.

Una **regla** es la acción que se ejecutará sobre un mensaje si éste cuenta con ciertas condiciones definidas con anterioridad. Así, si queremos que el mensaje de un destinatario sea guardado en determinada carpeta, podemos crear una regla donde se especifique que, al recibir correo de tal dirección, se ejecute la acción de moverlo a cierta carpeta (la carpeta **`SPAM`**, en nuestro ejemplo).

Las acciones y las condiciones están predefinidas en el cliente de correo de Microsoft, pero son bastantes y se puede elegir más de una condición y más de

¿QUÉ SIGNIFICA POP3?

POP3 son las siglas de **Post Office Protocol versión 3**. Este protocolo de oficina de correo es un lenguaje que conecta dos computadoras y permite que el correo electrónico se aloje en un servidor, solo hasta que la computadora cliente lo acceda.

una acción para crear una regla. De este modo, la combinación de las diferentes condiciones y acciones brinda un amplio abanico de posibilidades a la hora de administrar el correo entrante. Aprenderemos a crear una regla en el **Paso a paso 1**.

La regla creada, como ya habíamos especificado, marca los mensajes que incluyan la palabra **spam** en el asunto y aquellos que solo nos incluyan en la línea **CC**, y los mueve a una carpeta de nombre **SPAM**. Es conveniente revisar esta carpeta de manera regular para detectar mensajes marcados erróneamente.

SPAMfighter

El programa que utilizaremos para ayudar a los usuarios que quieran personalizar más su protección antispam o a aquellos usuarios que requieran una protección alta es **SPAMfighter**.

Este programa, además, puede reemplazar perfectamente a los filtros de clientes de correo POP como Windows Mail o Outlook, que muchas veces resultan insuficientes. Esta aplicación cuenta con una versión paga completa, pero utilizaremos la gratuita, cuyas restricciones son mínimas y su funcionalidad muy alta (**Figura 6**).

Una vez descargado el archivo, hacemos doble clic sobre él para iniciar el proceso de instalación y contar con este útil programa en nuestro sistema.

FIGURA 6. Para iniciar la descarga, ingresamos en el sitio www.spamfighter.com/Lang_ES/Download_Download.asp y hacemos clic en el botón `Descargar ahora`.

PASO A PASO /1
Crear reglas antispam en Windows Mail

1

Abra Windows Mail haciendo clic en **Inicio/Todos los programas/ Windows Mail**. En el programa, haga clic en el menú **Herramientas** y, luego, en **Reglas del Mensaje / Correo**.

2

Si ya había creado una regla alguna vez, en el cuadro **Reglas del mensaje** haga clic en el botón **Nueva...**; de otro modo, continúe con el siguiente paso.

Para las condiciones de la regla, tilde **La línea asunto contiene las palabras especificadas** y **La línea CC contiene nombres de personas**, mientras que para las acciones seleccione **Moverlo a la carpeta especificada** y **Marcar como leído**.

PASO A PASO /1 (cont.)

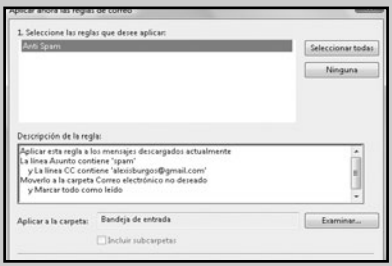
3

En el cuadro **Descripción de la regla**, pulse clic sobre el vínculo **contiene las palabras especificadas** y escriba **spam**. Haga clic en **Agregar** y en **Aceptar**.

4

En el cuadro **Descripción de la regla**, haga clic en **contiene personas** y escriba su propia dirección de correo electrónico. Haga clic en **Agregar** y en **Aceptar**. Pulse clic en **especificada**. Seleccione de la lista la carpeta **Correo no deseado**. Haga clic en **Aceptar**. Haga clic en el vínculo **y**. Luego, seleccione la opción **Los mensajes cumplen cualquiera de los criterios**. Presione **Aceptar**.

5



Para finalizar, en **Nombre de la regla**, escriba **Anti Spam** y presione **Aceptar**. La regla habrá sido creada. Puede filtrar los mensajes anteriores a la creación de la regla presionando el botón **Aplicar ahora...** y luego, una vez más, **Aplicar ahora**.

CONFIGURACIÓN

La instalación de SPAMfighter es muy sencilla y no presenta problemas para ninguno de los niveles de usuarios. El programa está escrito en español, y la interfaz de la instalación es sumamente amigable.

Durante la instalación, configuraremos una cuenta de SPAMfighter en el sistema, para lo cual introduciremos nuestra dirección de correo electrónico y una contraseña, que debe ser confirmada cuando nos sea requerido. Es recomendable que la cuenta de SPAMfighter y la de correo utilicen la misma contraseña. Durante el proceso de instalación, la aplicación armará por defecto una **lista blanca** integrada por los contactos que tenemos en la libreta de direcciones.

Una lista blanca es una base de datos con direcciones de correo electrónico certificadas. Esto quiere decir que recibiremos cualquier correo cuyo remitente sea parte de la lista blanca. Así, los mensajes de aquellos amigos que constantemente envían bromas, fotos y demás a todo el mundo no serán marcados como correo basura (**Figura 7**).

COMUNIDAD ANTISPAM

El concepto con el cual SPAMfighter trabaja para eliminar el correo no deseado es remotamente parecido al de un antivirus. Cada vez que el usuario recibe un e-mail en cualquiera de las cuentas de correo configuradas en Outlook o Windows Mail,

FIGURA 7. Si ya hemos utilizado SPAMfighter, aun en otro equipo, es recomendable utilizar la misma cuenta que teníamos para maximizar la eficacia de nuestra lista negra**.**

CERTIFICADO POR MICROSOFT

SPAMfighter, si bien está producido por la empresa **ASP Shareware**, cuenta en su desarrollo con el aporte de Microsoft. En el uso del programa y también en su **look and feel**, la mano de esta segunda empresa se hace notar.

el filtro antispam compara la dirección del remitente y el contenido del mensaje con una base de datos disponible en su servidor.

De haber coincidencia, marca el mensaje como spam y lo envía a la carpeta **SPAMfighter** en el cliente de correo del usuario. De este modo, el usuario puede corroborar qué se eliminó y qué no para decidir si un mensaje fue marcado de manera errónea. Asimismo, puede marcar como spam un mensaje recibido, haciendo clic en el botón **Bloquear** de la barra de herramientas SPAMfighter (**Figura 8**).

USAR SPAMFIGHTER

En la **Guía visual 1**, veremos la barra que se agrega al cliente de correo. El uso básico del programa se reduce a la posibilidad de marcar como spam o liberar de esa marca a aquellos mensajes que el programa no haya detectado o que, por error, haya marcado.

Por ejemplo, cuando recibimos un mensaje no deseado, para que esta situación no se repita, hay que seleccionar el mensaje y presionar, de la barra **SPAMfighter**, el botón **Bloquear**. Si el problema fuera al revés, en la carpeta **SPAMfighter**, debemos marcar aquel mensaje bloqueado erróneamente y presionar el botón **Liberar**.

Cuando un mensaje se detecta como spam, es movido a la carpeta con el nombre del programa y, allí, queda marcado como no leído. Esto es una ventaja en tanto uno puede ver con rapidez si nuevos

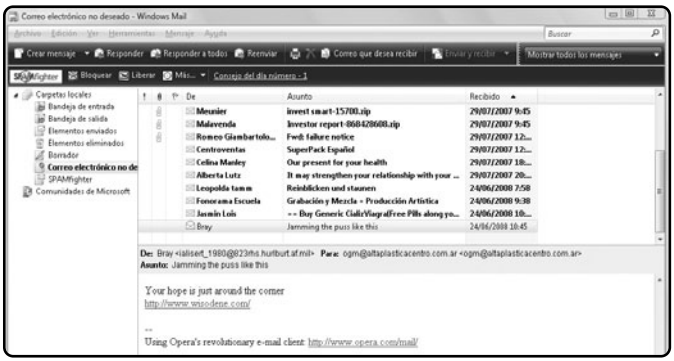
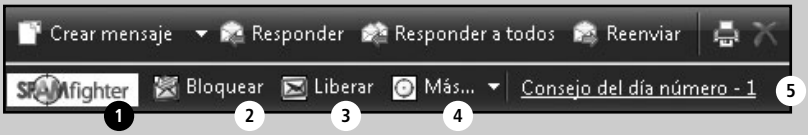


FIGURA 8. SPAMfighter agrega una barra de herramientas a la interfaz del cliente de correo que utilicemos.

MARCAR COMO LEÍDOS LOS CORREOS DE SPAM

Es posible que, después de un tiempo de uso y de configurar de manera correcta el programa, sean muy pocos los mensajes erróneamente filtrados y por eso, decidamos activar la opción que permite marcar como leídos los spam.

GUÍA VISUAL /1
Barra de SPAMfighter



1. Permite acceder a la página web personal del usuario de SPAMfighter, para encontrar información del perfil de la cuenta y el tiempo restante de uso de la versión PRO.
2. Mueve el mensaje seleccionado a la carpeta **SPAMfighter** y lo marca como tal en el servidor del programa para que otros usuarios puedan evitar su ataque.
3. Desmarca en la computadora local (y en el servidor si el mismo usuario fue quien lo marcó como spam originalmente) el mensaje seleccionado en la carpeta **SPAMfighter**. Mueve también el mensaje a su ubicación original y lo marca como no leído.
4. Al hacer clic en la opción **Más...**, muestra las opciones de configuración del programa y da acceso a la lista blanca y a la negra.
5. Accede a la página web del programa con un consejo sobre la protección antispam o sobre el uso de la aplicación.

mensajes fueron o no detectados y, a la vez, ayuda a recordar que es muy importante revisar de manera habitual la carpeta para desmarcar aquellos mensajes mal detectados.

EL BOTÓN MÁS...

El botón **Más...**, que se agrega a la barra de botones de SPAMfighter en Windows Mail, agrupa las opciones de listas negra y blanca, y algunas opciones menores. Resumiremos su contenido en la **Guía visual 2**.

La lista blanca y la lista negra, como ya hemos dicho, se refieren a los mensajes que el usuario considera deseados no deseados, respectivamente. Si bien el uso de la lista negra, aquella que bloquea mensajes, está más claro, tal vez haga falta explicar algo sobre la blanca.

Al agregar un mensaje o un dominio a la lista blanca, todos los e-mails recibidos de ese remitente o de remitentes de ese dominio serán aceptados.

Esto resulta muy útil cuando, por ejemplo, el usuario es miembro de algún programa de recompensas que envía newsletters de manera habitual, con el comentario de sus nuevos regalos. Por defecto, estos mensajes serían marcados como spam, mientras que al usuario, en realidad, le interesaría saber de qué se trata (**Figura 9**).

GUÍA VISUAL /2
El botón Más... de la barra de SPAMfighter

1. Administra el agregado de direcciones particulares y dominios completos a la lista negra.
2. Administra el agregado de direcciones particulares y dominios completos a la lista blanca.
3. La opción **`Limpiar carpeta`** borra todos los posibles spam descargados antes de la instalación del producto de la carpeta seleccionada.
4. Borra los mensajes marcados como spam por el filtro de la carpeta **`SPAMfighter`**.
5. Permite enviar una invitación a alguna persona conocida para descargar y comenzar a utilizar el programa **SPAMfighter**.
6. Este botón solo se encuentra disponible en la versión PRO del programa y brinda acceso a numerosas posibilidades de configuración.

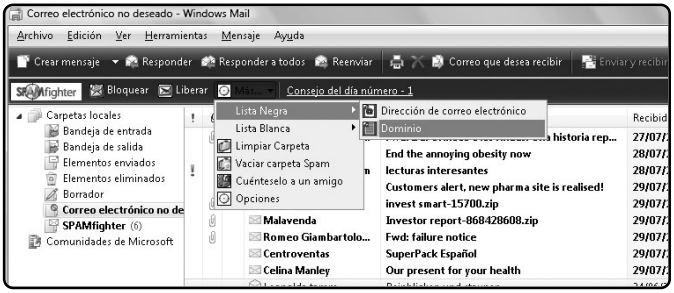


FIGURA 9.
No es recomendable agregar a la lista negra dominios de servidores gratuitos como Gmail o Hotmail.

Filtros en correos web

Herramientas prácticas como SPAMfighter solo están disponibles para correos de tipo POP configurados en máquinas hogareñas o de oficina que utilicen clientes para descargar sus correos. Esto hace que aquellos usuarios que consulten su correo electrónico desde afuera de su casa u oficina, o utilicen como correo siempre un cliente web, no puedan disfrutar de filtros de este tipo. Sin embargo, los servidores de correo electrónico web más renombrados incluyen avanzados filtros antispam en su propia interfaz web. Analizaremos los servicios de los proveedores más utilizados del momento: **Hotmail** y **Gmail**.

GMAIL

Los usuarios del correo electrónico web de **Google** cuentan con una eficaz protección contra el correo no deseado. Sin siquiera tener que activar ninguna opción, los filtros de Gmail aplicarán de manera automática, la etiqueta **Spam** a todos los mensajes considerados como tal y los moverán a la carpeta con ese nombre. Esto hará que para verlos haya que hacer clic sobre esa carpeta que aparece en el costado izquierdo de la pantalla.

Si el filtro hubiese sido aplicado de manera incorrecta, siempre existe la posibilidad de marcar el mensaje -al tildar la casilla de verificación en la derecha de cada uno- y de presionar el botón **No es spam** para que nunca más una conversación con ese contacto sea considerada spam (**Figura 10**).

PROTECCIÓN EN OTROS SERVICIOS

Aunque en este libro nos vamos a centrar en la protección que ofrecen **Gmail** y **Hotmail**, cabe aclarar que los demás servicios de correo web ofrecen también efectivos sistemas de protección antispam. **Yahoo**, por ejemplo, incluye un filtro muy efectivo.

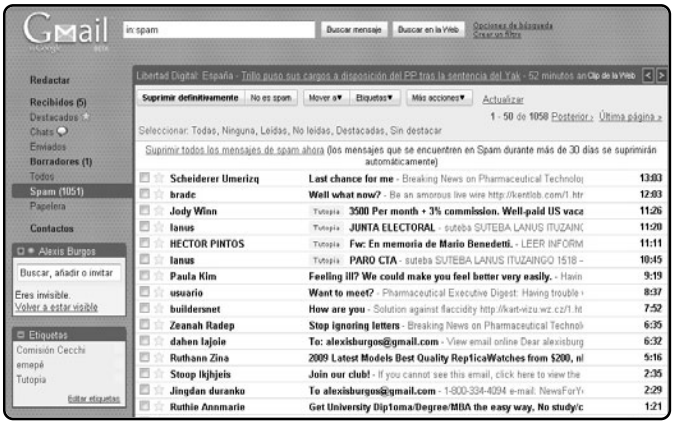


FIGURA 10.
El filtro antispam de Gmail funciona muy bien, aunque es bastante estricto y elimina mensajes de manera injustificada.

FIGURA 11.
Hotmail mueve los mensajes marcados como spam a la carpeta Correo no deseado.

PRECAUCIÓN AL DESCARGAR APLICACIONES ANTISPAM

No debemos descargar, de ninguna página web, programas antispam sin certificado o de origen desconocido. La mayoría de ellos están diseñados con el fin de diseminar publicidad e incluyen una absurda cantidad de adware y spyware.

HOTMAIL

Cuando un mensaje es reconocido como spam por el servidor de Hotmail, se mueve a una carpeta predefinida para esto. Lejos de la eficacia del filtro antispam de Gmail, la protección contra el correo electrónico no deseado de Hotmail posee menor efectividad, pero resulta mucho más configurable (**Figura 11**).

Para hacer de la protección brindada por Hotmail algo útil, veamos los puntos más importantes de su configuración. Para ello, al conectarnos a nuestra cuenta, hacemos clic en el enlace **Opciones** de la esquina superior derecha de la pantalla y, allí, en **Más opciones**. Por último, pulsamos clic en el vínculo **Filtros e información**. Veamos, en la **Guía visual 3**, los parámetros del filtro para poder configurarlos de manera efectiva.

El único nivel de protección antispam de óptima efectividad entre los que ofrece Hotmail es el **Exclusivo**. Sin embargo, este nivel puede resultar incómodo aun si lo usamos en conjunto con una configuración de eliminación automática del correo basura en 10 días. Si lo que necesitamos es un servicio de correo con filtros efectivos, tal vez sea buena idea migrar a otro servidor y seguir utilizando Hotmail como correo secundario o como cuenta de base para acceder a los servicios de la comunidad **Windows Live**.

Datos útiles para tener en cuenta

ADWARE Y SPAM

Muchos de los adware más peligrosos se ocupan de robar información personal del usuario que utilizan, para reenviar publicidad orientada a determinados consumidores. Las bases de datos que con esa información se crean son, muchas veces, vendidas a spammers, que las usan para reenviar el correo no deseado por el destinatario.

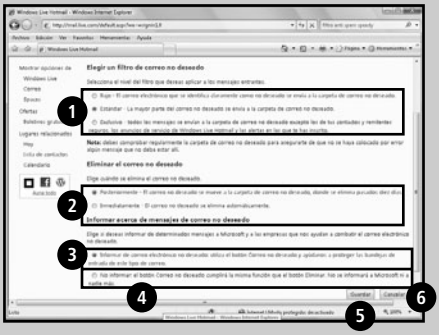
INFORMACIÓN SOBRE EL SPAM

La página web del antivirus Panda incluye en sus tutoriales una completa guía sobre el funcionamiento más profundo del spam. En **www.pandasecurity.com/spain/homeusers/security-info/types-malware/spam/**, encontraremos una guía en castellano, para conocer las características de esta amenaza.

SPAMFIGHTER Y MOZILLA THUNDERBIRD

Aunque SPAMfighter es una herramienta que también puede funcionar sobre el cliente de correo electrónico **Mozilla Thunderbird**, tendrán cubiertas sus necesidades con el filtro nativo que brinda este software.

GUÍA VISUAL /3
Correo electrónico no deseado de Hotmail



1. Permite definir el nivel del filtro de correo electrónico: **`Bajo`**, **`Estándar`** o **`Exclusivo`**. Este último solo admite la recepción de mensajes cuyo remitente sea un contacto existente en la libreta de direcciones de Hotmail. Por defecto, deberíamos usar el nivel **`Estándar`**.
2. Define si el correo no deseado será eliminado al llegar, o luego de 10 días, de modo que el usuario pueda revisarlo. Esta última opción es la recomendada.
3. Si esta opción está seleccionada, compartirá con los demás usuarios de la comunidad los mensajes que haya marcado como no deseados, con lo cual mejora la eficacia del filtro antispam. Se recomienda activarla.
4. Si esta opción está activada, el correo basura se eliminará y no será compartido con la comunidad. No se recomienda su activación.
5. Guarda las preferencias del usuario.
6. Cancela los cambios.

RESUMEN

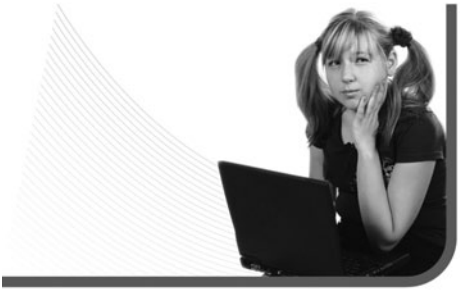
El spam es una de las más molestas amenazas informáticas. Aunque con el avance de los filtros antispam, en correos POP y web, la situación ha mejorado bastante, muchos usuarios se sienten particularmente abrumados por publicidades y correo basura.

Apéndice

Programas alternativos

Analizaremos herramientas alternativas a los productos de seguridad vistos en los capítulos anteriores.

A lo largo del libro, hemos visto un completo detalle de aplicaciones que colaboran con el usuario en lo que se refiere a proteger la seguridad de su equipo. En este capítulo, analizaremos las mejores herramientas alternativas para todos los que quieren ver la opción "B" de los productos de seguridad desarrollados en los capítulos anteriores.



Alternativas en antivirus: avast!

Quienes no usan **AVG Free Edition AntiVirus** suelen preferir, casi en la mayoría de los casos, el famoso antivirus comercial de **Norton** o el producto de **ESET**, **Nod32**. Sin embargo, en la red, existe un excelente antivirus gratuito muy fácil de usar y de gran potencia, cuyo nombre es **avast!**. Este antivirus es una aplicación liviana y muy efectiva que, además, permite trabajar con skins y cuenta con un motor de actualizaciones muy rápido. Veamos cómo instalar este producto en nuestro sistema.

DESCARGA E INSTALACIÓN

La página oficial de la descarga de **avast!** se encuentra en el vínculo **www.avast.com/esp/download-avast-home.html**. Desde allí, podemos obtenerlo haciendo clic en el botón **`Download`** de la línea **`avast! 4 Home - Versión en Español (length 32.80 MB)`** como se muestra en la **Figura 1**.

FIGURA 1.
Desde la página de descarga, además de obtener el instalador, podremos acceder a otra documentación y a recursos relacionados con el producto.

Los editores ofrecen también descargarlo desde **Donwload.com** (al hacer clic en el botón **`Download now`**), pero en ese caso solo obtendremos un instalador web liviano de **300 KB** y no el instalador completo. Esta opción se recomienda solo para usuarios de **netbooks** y equipos donde el espacio disponible es muy limitado (**Figura 2**).

FIGURA 2. Programar una búsqueda al reiniciar el sistema es una buena idea, sobre todo si estamos migrando de otro antivirus anterior, hacia avast!

EL PROGRAMA EN ACCIÓN

Este software funciona de manera sencilla, y su interfaz llama la atención por su simplicidad. Debemos considerar, sin embargo, que estamos ante una versión simplificada.

El **avast! Profesional** cuenta con una interfaz avanzada mucho más compleja y configurable, pero para acceder a él debemos pagar. Por lo pronto, aprenderemos a utilizar la interfaz principal de **avast! Free Edition** en la **Guía visual 1**.

Para iniciar un análisis, seleccionamos un área (discos duros, extraíbles, archivos o carpetas) y hacemos clic en el botón **`Iniciar`**, indicado en el **Punto 2 de la Guía visual 1**. Las opciones de configuración de avast!, a las que accedemos con **`Menú`**/**`Configuración`**, ofrecen algunas opciones interesantes que mejoran la eficacia y la funcionalidad del producto, como las **exclusiones**. Si por alguna razón debemos excluir momentáneamente una determinada cantidad de objetos del análisis residente, podremos definirlos en el apartado **`Exclusiones`**. El botón **`Examinar...`** nos permitirá elegir los elementos que después suprimiremos con **`Eliminar`** (**Figura 3**).

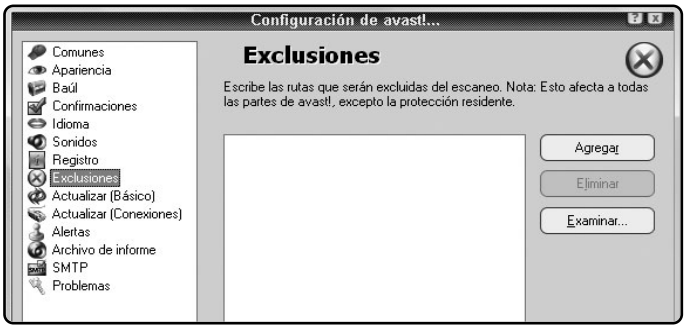
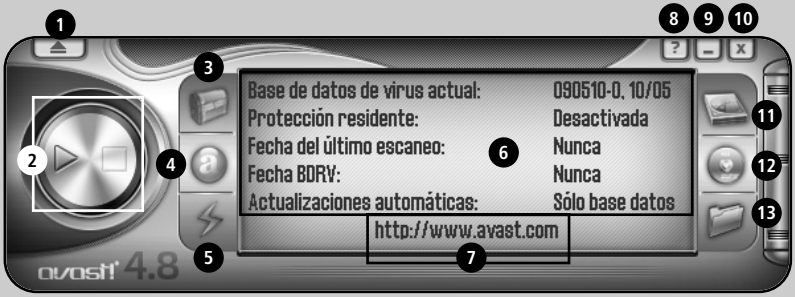


FIGURA 3.
El botón `Agregar` permite definir una máscara para las exclusiones. Esto es útil si, por ejemplo, deseamos que no se analicen archivos con una extensión determinada.

GUÍA VISUAL /1
Pantalla principal de avast! Antivirus



1. Muestra el menú de opciones de avast! antivirus.
2. Inicia o detiene el tipo de análisis seleccionado.
3. Esta opción premite acceder y administrar el baúl de virus; una herramienta similar a la bóveda de virus de AVG, que mantiene los archivos infectados en cuarentena, hasta tanto exista una cura definitiva para la amenaza.
4. Define la sensibilidad (y por tanto la velocidad) del escáner residente.
5. Actualiza la base de datos de definiciones de virus manualmente. Las actualizaciones automáticas, de cualquier modo, se siguen efectuando.
6. Muestra el estado actual de los componentes del programa.
7. Conecta con el sitio oficial del producto, **www.avast.com**.
8. Muestra la ayuda del programa.
9. Minimiza la aplicación.
10. Cierra la pantalla principal, pero mantiene activo el módulo residente.
11. Permite especificar las condiciones del análisis de discos duros.
12. Permite especificar las condiciones del análisis de discos extraíbles.
13. Permite especificar las condiciones del análisis de archivos y carpetas.

Alternativas en firewalls: ZoneAlarm

Los firewalls con los que hemos trabajado en este libro son productos más fáciles de utilizar que de configurar. Sin embargo, existen en el mercado productos de excelente calidad y niveles de protección superlativos que le exigen al usuario un tiempo de acostumbramiento, que será pagado con creces en lo que a seguridad se refiere. Uno de ellos es, sin duda, **ZoneAlarm**: un clásico del mundo de los firewalls avanzados (**Figura 4**).

Las razones para elegir un firewall de este tipo son muchas, en particular asociadas a un mayor control de todo lo que pasa en nuestra red y, en especial, del origen y el destino del tráfico entrante y saliente. Con ZoneAlarm, podemos controlar todo lo que a tráfico de red se refiere. Si usamos un firewall como este software en conjunto con un servidor proxy, es decir, con una máquina que funciona como servidor en lugar de un router, podremos definir los permisos de acceso a Internet de cada usuario y los límites de su navegación.

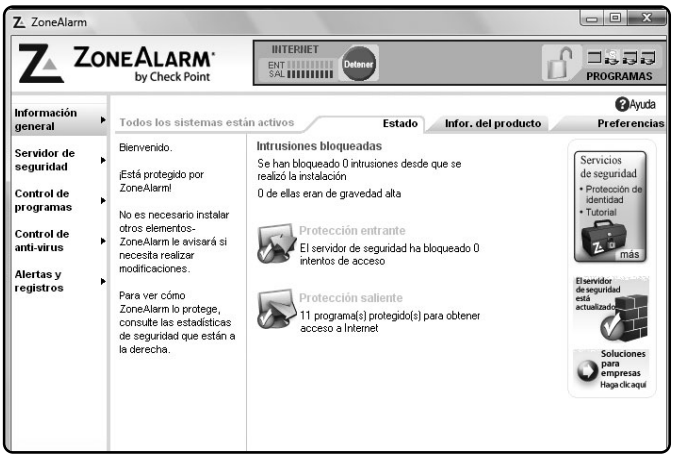


FIGURA 4.
ZoneAlarm fue, en el comienzo de la historia de los firewalls, el producto más elegido por los usuarios.

SKINS PARA AVAST!

El programa **avast! Antivirus** permite trabajar con **skins**, es decir, con máscaras que cambian la apariencia de la pantalla principal de la aplicación; algunas de ellas son realmente vistosas. Se consiguen en el sitio web **www.avast.com/esp/skins.html**.

DESCARGA E INSTALACIÓN

El producto se puede descargar de manera gratuita desde el sitio **www.zonealarm.com/security/es/zonealarm-pc-security-free-firewall.htm**. Allí deberemos hacer clic en **Descargar ahora** para comenzar la descarga del instalador, que pesa alrededor de 205 KB. Si bien existe una versión paga de ZoneAlarm llamada Pro, la versión gratuita será más que suficiente para nuestras necesidades de protección en el ámbito hogareño (**Figura 5**).

EL PROGRAMA EN ACCIÓN

Una vez instalado, ZoneAlarm colocará en la zona de notificación del área de tareas un icono que indicará en verde el nivel de tráfico saliente y en rojo el de entrante. Si hacemos doble clic sobre él, podremos acceder a la pantalla principal del producto, desde donde controlaremos su comportamiento y su accionar. En la **Guía visual 2**, veremos sus principales opciones.

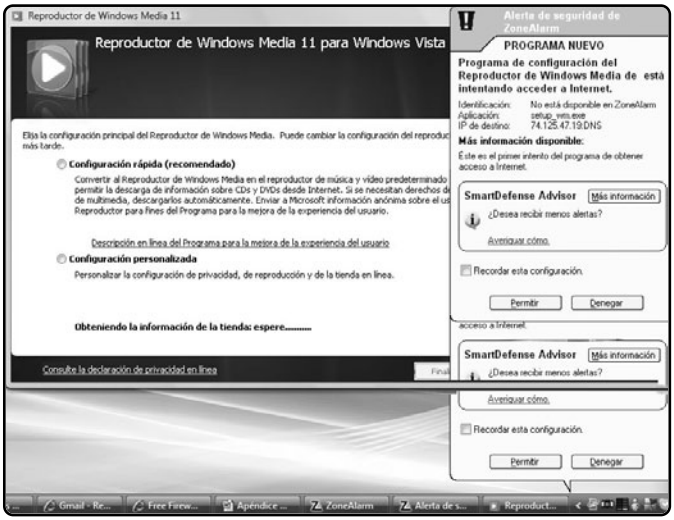


FIGURA 5.
ZoneAlarm bloquea las transferencias de todas las aplicaciones que no hayamos certificado, incluso los productos de Microsoft.

KERIO PERSONAL FIREWALL

Otra alternativa dentro de los firewalls personales se llama **Kerio Personal Firewall**. Este producto es tan fácil de usar como ZoneAlarm y brinda un nivel de protección muy alto. Se puede descargar desde el sitio web **www.kerio.com/firewall**.

Servidor de seguridad

Al hacer clic sobre **Servidor de seguridad** en la pantalla principal de ZoneAlarm, podremos cambiar el comportamiento básico del firewall. El primer parámetro por definir es la **Seguridad en la Zona de Internet**, que determina el modo en el que se comportará el firewall en relación con los equipos remotos. El nivel **Alto**, que es a la vez el predefinido y el recomendado, impide que alguien pueda ver nuestro equipo, así como también el acceso a los datos en él alojados. El nivel **Medio** permite que otros equipos vean el nuestro, pero impedirá que accedan a él, mientras que el nivel **Desactivado** permitirá cualquier transferencia entre nuestro equipo y otros remotos.

Por supuesto, este nivel no es recomendable, a menos que el administrador de la red nos indique que lo utilicemos porque existe un firewall por hardware.

El segundo parámetro es el que se refiere a la **Seguridad en la Zona de Confianza**, es decir, en la red local. El nivel **Alto** nos aislará de la red, en tanto nadie podrá vernos ni interactuar con nosotros. El nivel **Medio**, que es el indicado y recomendado, permite compartir archivos y ser descubierto en la red. Sin embargo, para activarlo es recomendable que el nivel de seguridad en la **Zona de Internet** sea **Alto**. El nivel **Desactivado** deja de lado el firewall y habilita el tráfico en la red, lo que puede suponer un agujero de seguridad grave (**Figura 6**).

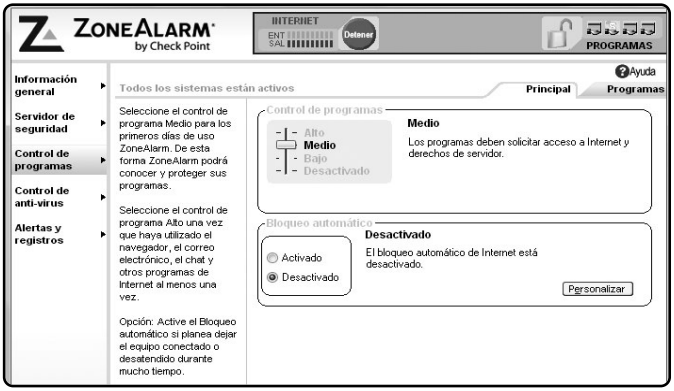
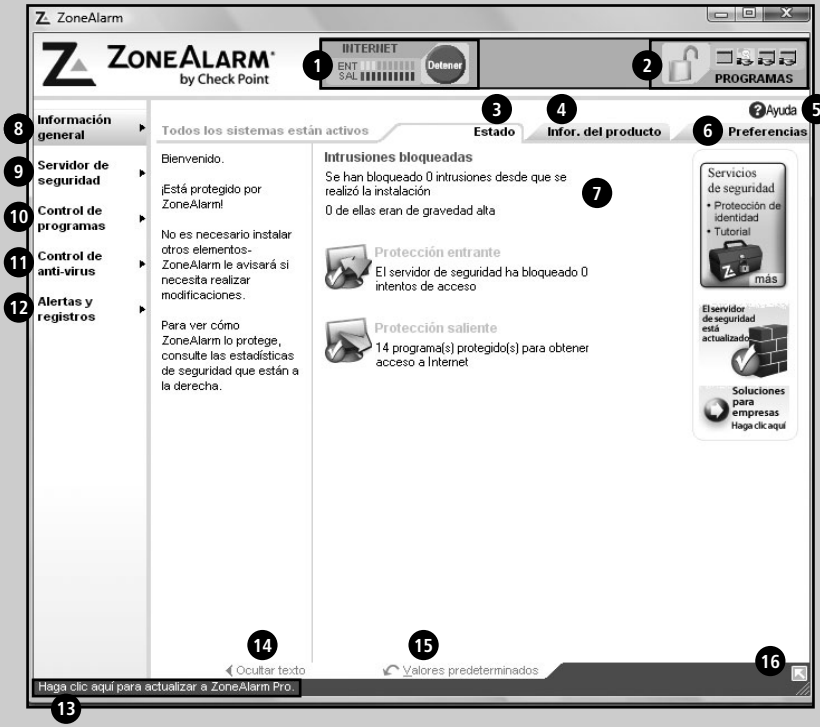


FIGURA 6.
No es recomendable desactivar el firewall a menos que recibamos estrictas indicaciones por parte de un encargado de sistemas.

PROXY+

Proxy+ es el mejor de los servidores proxy gratuitos, si buscamos un producto poderoso que administre nuestra red local. No es fácil de usar, ni tiene una interfaz simpática, pero su poderío es muy alto. Se consigue en **www.proxyplus.cz/download.php?lang=en**.

GUÍA VISUAL /2
Pantalla principal de ZoneAlarm



1. La función de esta opción es indicar el tráfico entrante y saliente. El botón **`Detener`** anula las transmisiones de cualquier tipo en forma instantánea.
2. Muestra los programas que están accediendo a Internet. El botón del candado bloquea el tráfico de todas las aplicaciones de una vez.
3. Muestra la pantalla de estado general de la aplicación.
4. Muestra información técnica del producto.
5. Abre la ayuda de la aplicación.

GUÍA VISUAL /2 (cont.)

6. Permite cambiar y administrar las preferencias de ZoneAlarm.
7. Área de trabajo de la aplicación.
8. Accede a las opciones generales de ZoneAlarm.
9. Permite controlar el comportamiento del servidor de seguridad.
10. Permite controlar el comportamiento del módulo de control de programas.
11. Si está instalado, permite controlar el módulo de control del antivirus de ZoneAlarm, solo disponible en la versión Pro.
12. Muestra alertas y registros de acción de la aplicación.
13. Abre el sitio web desde el cual se puede comprar ZoneAlarm Pro.
14. Oculta el texto de bienvenida del área de trabajo.
15. Restaura los valores predeterminados de la aplicación.
16. Reduce la ventana de modo que solo se vea el indicador de tráfico y de aplicaciones.

Control de programas

El **Control de programas** es una herramienta muy importante de ZoneAlarm, que permite controlar el acceso a la red de cada uno de los programas y servicios instalados en el sistema. Cada vez que el programa nos pide una autorización para una determinada aplicación, es el **Control de programas** el que está actuando.

Los niveles de protección que ofrece son tres (el más alto no está disponible en la versión gratuita de ZoneAlarm). **Medio**, que es el recomendado y no permite acceder a Internet a ninguna aplicación que no haya sido habilitada por el usuario. **Bajo**, que es un modo de aprendizaje en el cual el **Control de programas** toma nota de las aplicaciones que el usuario por lo general utiliza. **Desactivado**, es un nivel que inhabilita el **Control de programas** y no es recomendado.

El **Control de programas** ofrece una última opción realmente interesante, llamada **Bloqueo automático**. Ésta impide que ninguna aplicación, más allá de las que están funcionando, tenga acceso a la red y sirve para que, cuando nos alejamos de la computadora por un rato, nada ponga en riesgo la seguridad del equipo. Al volver, deberíamos hacer clic en **Desactivar** para que todo retornara a la normalidad (**Figura 7**).

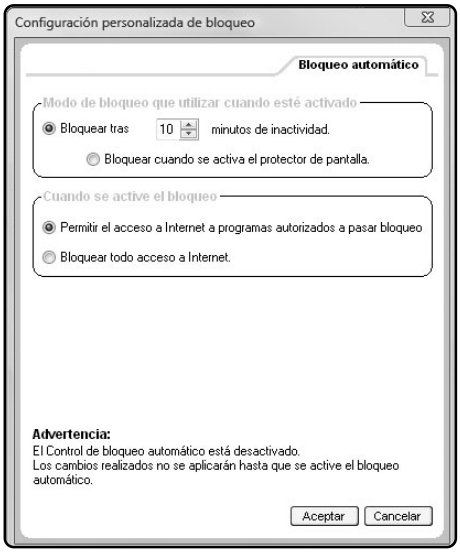


FIGURA 7. Al hacer clic en `Personalizar`, podremos definir un tiempo automático para la activación del bloqueo, que puede ser igual, al del protector de pantalla.

Alternativa en antispyware: Lavasoft Ad-Aware

Hace unos años, Spybot Search & Destroy tenía un contrincante muy fuerte: **Lavasoft Ad-Aware**. Este producto era tan efectivo como Spybot, pero muchísimo más fácil de usar, lo que lo convirtió en el preferido de la mayoría de los usuarios.

Sin embargo, la versión 2007 de Ad-Aware decepcionó a muchos por su alto contenido publicitario y por la lentitud con la que llevaba a cabo el escaneo. En la actualidad, la versión aniversario gratuita de Ad-Aware, **Ad-Aware AE**, recupera el esplendor perdido. Funciona de manera efectiva, y es rápido y confiable. El programa se descarga desde el siguiente sitio: **www.adaware.es**. Allí debemos hacer clic en **Descargar Ad-Aware FREE** y luego completar el formulario (**Figura 8**).

SYGATE PERSONAL FIREWALL

En el sitio web **OldVersion** (**www.oldversion.com**), podemos encontrar versiones funcionales de **Sygate Personal Firewall**, un servidor de seguridad que tiene ya unos años, pero que es de lo mejor que existe entre las aplicaciones de su clase.

FIGURA 8.
El formulario puede llenarse en unos instantes, y hay que hacer clic en `Enviar` para iniciar la descarga.

Después, hacemos clic en **`Enviar`** y pulsamos otro clic en el botón **`Probar gratis`**, para proceder con la descarga del instalador. Una vez instalado el programa, al reiniciar el equipo, el producto actualizará su base de datos de definiciones antes de cargar la interfaz del programa.

EL PROGRAMA EN ACCIÓN

Una vez terminada la actualización, el programa se iniciará y también lo hará su módulo de protección activa contra spyware **Ad-Watch**. Durante mucho tiempo, esta funcionalidad solo existía en las versiones pagas de Ad-Aware, aunque desde ahora está también disponible para la versión gratuita. Este módulo se encarga de monitorear el accionar de las aplicaciones del sistema en busca de comportamientos que puedan considerarse peligrosos. La ventana principal de la aplicación es muy simple, y la analizaremos en la **Guía visual 3**.

Diferentes tipos de análisis

Al hacer clic en el botón **`Analizar`**, se nos permitirá elegir un tipo de análisis e iniciarlo. Por defecto, utilizaremos el **`Análisis inteligente`**, que es un tipo de examen que solo escanea las zonas donde podría haber adware y spyware, y no busca más allá (**Figura 9**). Una vez terminada la revisión, veremos los resultados y eliminaremos las amenazas haciendo clic en el botón **`Realizar acciones ahora`**. Si no estamos seguros de las consecuencias de la limpieza, podemos crear un punto de restauración del sistema marcando la casilla de verificación **`Establecer punto de restauración`**.

FIGURA 9. Es recomendable llevar a cabo un análisis completo solo después de haber detectado una infección severa.

GUÍA VISUAL /3
Pantalla principal de Ad-Aware

1. Pantalla principal de Ad-Aware, desde donde se controla el accionar del programa.
2. Ofrece estadísticas de los últimos análisis y de las amenazas encontradas.
3. Abre la ventana de análisis del sistema.
4. Permite especificar la configuración del módulo de protección activa Ad-Watch.
5. Muestra las herramientas adicionales de la aplicación Ad-Aware.
6. Opciones de configuración del programa.
7. Inicia la actualización manual del sistema. La versión gratuita de Ad-Aware no incluye actualizaciones automáticas; es recomendable hacer clic aquí al abrir el programa.
8. En la versión paga de Ad-Aware, permite especificar análisis programados.
9. Muestra publicidad (muchas veces encubierta) e información de la licencia.
10. Abre la ayuda del programa.
11. Muestra información sobre la versión.

RESUMEN

Hemos conocido algunos programas alternativos para completar muchas de las tareas propuestas en los capítulos principales de este libro. Estos programas son muy efectivos, y muchos usuarios pueden preferirlos en lugar de los seleccionados en el desarrollo principal.

Servicios **al lector**

Encontraremos información adicional relacionada con el contenido, que servirá para complementar lo aprendido.

Índice **temático**

#

A

B

C

D

E

F

G

H

I

K

L

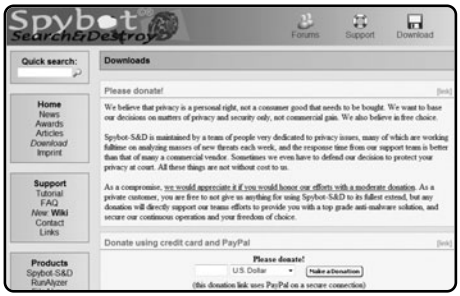
M

N

P

R

S



T

U

V

W

Z

CLAVES PARA COMPRAR
UN LIBRO DE COMPUTACIÓN

1 SOBRE EL AUTOR Y LA EDITORIAL

Revise que haya un cuadro "sobre el autor", en el que se informe sobre su experiencia en el tema. En cuanto a la editorial, es conveniente que sea especializada en computación.

2 PRESTE ATENCIÓN AL DISEÑO

Compruebe que el libro tenga guías visuales, explicaciones paso a paso, recuadros con información adicional y gran cantidad de pantallas. Su lectura será más ágil y atractiva que la de un libro de puro texto.

3 COMPARE PRECIOS

Suele haber grandes diferencias de precio entre libros del mismo tema; si no tiene el valor en tapa, pregunte y compare.

4 ¿TIENE VALORES AGREGADOS?

Desde un sitio exclusivo en la Red hasta un CD-ROM, desde un Servicio de Atención al Lector hasta la posibilidad de leer el sumario en la Web para evaluar con tranquilidad la compra, o la presencia de adecuados índices temáticos, todo suma al valor de un buen libro.

5 VERIFIQUE EL IDIOMA

No sólo el del texto; también revise que las pantallas incluidas en el libro estén en el mismo idioma del programa que usted utiliza.

6 REVISE LA FECHA DE PUBLICACIÓN

Está en letra pequeña en las primeras páginas; si es un libro traducido, la que vale es la fecha de la edición original.

usershop.redusers.com
VISITE NUESTRO SITIO WEB

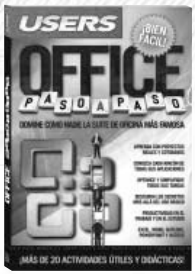
» Vea información más detallada sobre cada libro de este catálogo.
» Obtenga un capítulo gratuito para evaluar la posible compra de un ejemplar.
» Conozca qué opinaron otros lectores.
» Compre los libros sin moverse de su casa y con importantes descuentos.
» Publique su comentario sobre el libro que leyó.
» Manténgase informado acerca de las últimas novedades y los próximos lanzamientos.

TAMBIÉN PUEDE CONSEGUIR NUESTROS LIBROS EN KIOSCOS O PUESTOS DE PERIÓDICOS, LIBRERÍAS, CADENAS COMERCIALES, SUPERMERCADOS Y CASAS DE COMPUTACIÓN.

LLEGAMOS A TODO EL MUNDO VÍA »OCA * Y DHL**

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com // usershop@redusers.com



Office paso a paso

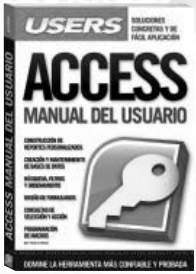
Este libro presenta una increíble colección de proyectos basados en la suite de oficina más usada en el mundo. Todas las actividades son desarrolladas en procedimientos paso a paso de una manera didáctica y fácil de comprender.

→ COLECCIÓN: PASO A PASO
→ 320 páginas / ISBN 978-987-663-030-6

101 Secretos de Hardware

Esta obra es la mejor guía visual y práctica sobre hardware del momento. En su interior encontraremos los consejos de los expertos sobre las nuevas tecnologías, las soluciones a los problemas más frecuentes, cómo hacer overclocking, modding, y muchos más trucos y secretos.

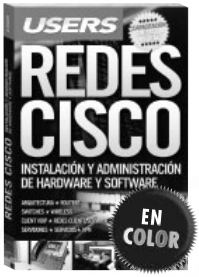
→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-029-0



Access

Este manual nos introduce de lleno en el mundo de Access para aprender a crear y administrar bases de datos de forma profesional. Todos los secretos de una de las principales aplicaciones de Office, explicados de forma didáctica y sencilla.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-025-2



Redes Cisco

Este libro permitirá al lector adquirir todos los conocimientos necesarios para planificar, instalar y administrar redes de computadoras. Todas las tecnologías y servicios Cisco, desarrollados de manera visual y práctica en una obra única.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-024-5

Proyectos con Office

Esta obra nos enseña a usar las principales herramientas de Office a través de proyectos didácticos y útiles. En cada capítulo encontraremos la mejor manera de llevar adelante todas las actividades del hogar, la escuela y el trabajo.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-023-8

Dreamweaver y Fireworks

Esta obra nos presenta las dos herramientas más poderosas para la creación de sitios web profesionales de la actualidad. A través de procedimientos paso a paso, nos muestra cómo armar un sitio real con Dreamweaver y Fireworks sin necesidad de conocimientos previos.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-022-1

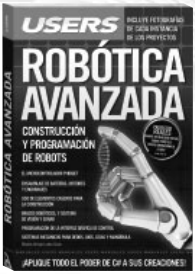
¡Léalo antes Gratis!

En nuestro sitio, obtenga GRATIS un capítulo del libro de su elección antes de comprarlo.

Excel revelado

Este manual contiene una selección de más de 150 consultas de usuarios de Excel y todas las respuestas de Claudio Sánchez, un reconocido experto en la famosa planilla de cálculo. Todos los problemas encuentran su solución en esta obra imperdible.

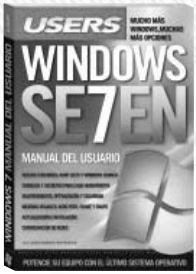
→ COLECCIÓN: MANUALES USERS
→ **336** páginas / ISBN 978-987-663-021-4



Robótica avanzada

Esta obra nos permitirá ingresar al fascinante mundo de la robótica. Desde el ensamblaje de las partes hasta su puesta en marcha, todo el proceso está expuesto de forma didáctica y sencilla para así crear nuestros propios robots avanzados.

→ COLECCIÓN: MANUALES USERS
→ **352** páginas / ISBN 978-987-663-020-7



Windows 7

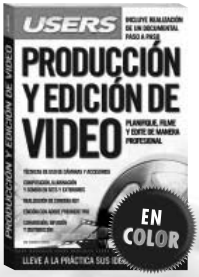
En este libro encontraremos las claves y los secretos destinados a optimizar el uso de nuestra PC tanto en el trabajo como en el hogar. Aprenderemos a llevar adelante una instalación exitosa y a utilizar todas las nuevas herramientas que incluye esta versión.

→ COLECCIÓN: MANUALES USERS
→ **320** páginas / ISBN 978-987-663-015-3

De Windows a Linux

Esta obra nos introduce en el apasionante mundo del software libre a través de una completa guía de migración, que parte desde el sistema operativo más conocido: Windows. Aprenderemos cómo realizar gratuitamente aquellas tareas que antes hacíamos con software pago.

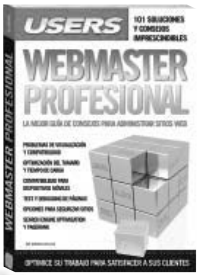
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-013-9



Producción y edición de video

Un libro ideal para quienes deseen realizar producciones audiovisuales con bajo presupuesto. Tanto estudiantes como profesionales encontrarán cómo adquirir las habilidades necesarias para obtener una salida laboral con una creciente demanda en el mercado.

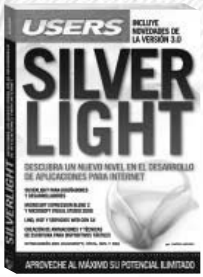
→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-012-2



Webmaster Profesional

Esta obra explica cómo superar los problemas más frecuentes y complejos que enfrenta todo administrador de sitios web. Ideal para quienes necesiten conocer las tendencias actuales y las tecnologías en desarrollo que son materia obligada para dominar la Web 2.0.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-011-5



Silverlight

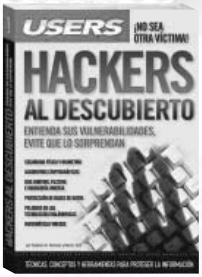
Este manual nos introduce en un nuevo nivel en el desarrollo de aplicaciones interactivas a través de Silverlight, la opción multiplataforma de Microsoft. Quien consiga dominarlo creará aplicaciones visualmente impresionantes, acordes a los tiempos de la incipiente Web 3.0.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-010-8

Flash Extremo

Este libro nos permitirá aprender a fondo Flash CS4 y ActionScript 3.0 para crear aplicaciones web y de escritorio. Una obra imperdible sobre uno de los recursos más empleados en la industria multimedia que nos permitirá estar a la vanguardia del desarrollo.

→ COLECCIÓN: MANUALES USERS
→ 320 páginas / ISBN 978-987-663-009-2



Hackers al descubierto

Esta obra presenta un panorama de las principales técnicas y herramientas utilizadas por los hackers, y de los conceptos necesarios para entender su manera de pensar, prevenir sus ataques y estar preparados ante las amenazas más frecuentes.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-008-5

Vista avanzado

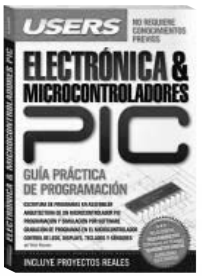
Este manual es una pieza imprescindible para convertirnos en administradores expertos de este popular sistema operativo. En sus páginas haremos un recorrido por las herramientas fundamentales para tener máximo control sobre todo lo que sucede en nuestra PC.

→ COLECCIÓN: MANUALES USERS
→ 352 páginas / ISBN 978-987-663-007-8

101 Secretos de Excel

Una obra absolutamente increíble, con los mejores 101 secretos para dominar el programa más importante de Office. En sus páginas encontraremos un material sin desperdicios que nos permitirá realizar las tareas más complejas de manera sencilla.

→ COLECCIÓN: MANUALES USERS
→ 336 páginas / ISBN 978-987-663-005-4



Electrónica & microcontroladores PIC

Una obra ideal para quienes desean aprovechar al máximo las aplicaciones prácticas de los microcontroladores PIC y entender su funcionamiento. Un material con procedimientos paso a paso y guías visuales, para crear proyectos sin límites.

→ COLECCIÓN: MANUALES USERS
→ 368 páginas / ISBN 978-987-663-002-3

CONOZCA LOS MEJORES TRUCOS DE LA PLANILLA MÁS POPULAR

Este libro presentan novedosos e increíbles aspectos de una de las herramientas más utilizadas en la oficina y el hogar. A través de sus páginas, los expertos en la planilla nos muestran nuevas formas de utilizar las herramientas y funciones de siempre.

» HOME / MICROSOFT
» 192 PÁGINAS
» ISBN 978-987-663-032-0

SOBRE LA COLECCIÓN desde Cero

» Aprendizaje práctico, divertido, rápido y sencillo.
» Lenguaje simple y llano para una comprensión garantizada.
» Consejos de los expertos para evitar problemas comunes.
» Guías visuales y procedimientos paso a paso.

OTROS TÍTULOS DE LA MISMA COLECCIÓN

PHOTOSHOP // OFFICE // HARD
WINDOWS 7 // BLOGS // REDES
SEGURIDAD // Y MUCHO MÁS

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com // usershop@redusers.com

Seguridad PC desde Cero

La seguridad de las computadoras es uno de los aspectos más sensibles de la informática en la actualidad. Este libro le mostrará cómo proteger la información de su PC de manera sencilla, repasando cada una de las estrategias de defensa, desde la instalación del antivirus hasta consejos de seguridad para navegar la Web ¡con total tranquilidad!

Dentro del libro encontrará

Un equipo seguro | Antivirus | Instalación y actualización | Adware, spyware y malware Spybot Search & Destroy | Copia de seguridad del registro | Análisis del sistema Vulnerabilidades en sistemas operativos | Actualizaciones en Windows | Service packs Firewall | Centro de seguridad | Redes inalámbricas seguras | Configuración del router Políticas de seguridad en la Red | Sensor biométrico | Encriptación de datos

Sobre la colección

- Aprendizaje práctico, divertido, rápido y sencillo
- Lenguaje simple y llano para una comprensión garantizada
- Consejos de los expertos para evitar problemas comunes
- Guías visuales y procedimientos paso a paso

Otros títulos de esta misma colección

Photoshop / Office / Hardware
Excel / Soluciones PC
Blogs / Redes

PC Security from scratch

Nowadays, security in one of the most sensitive subjects since the Internet presents opportunities for creating relations and better communications, but also, for intruders to acquire personal information. This book will teach you how to avoid any web based attack.

El contenido de esta obra formó parte del libro Seguridad PC.

RedUSERS.com

Nuestro sitio reúne a la mayor comunidad de tecnología en América Latina. Aquí podrá comunicarse con lectores, editores y autores, y acceder a noticias, foros y blogs constantemente actualizados.

Si desea más información sobre el libro:
Servicio de atención al lector **usershop@redusers.com**

ISBN 978-987-663-031-3