Gonzalo Asensio

Prologado por **José Barberá Heredia**
Doctor Ingeniero de Telecomunicación.
Asesor del Secretario de Estado
de Telecomunicaciones
y para la Sociedad de la Información.

Para usuarios
de **Windows XP**

Seguridad en Internet

Una guía práctica y eficaz para **PROTEGER SU PC**
con **SOFTWARE GRATUITO**

Recomendado por:
redes

nowtilus

manuales_PC

SEGURIDAD EN INTERNET

Una guía práctica y eficaz para proteger su PC
con software gratuito

Gonzalo Asensio Asensio

nowtilus

A mi padre, madre y hermana por creer en mí desde el principio

A mis abuelos por todo su cariño

Agradecimientos especiales a mi mujer, Susana, por su amor y apoyo incondicional y a mis hijos, Mónica y Marcos, por el tiempo cedido para realizar esta obra.

MUCHAS GRACIAS A TODOS

Gonzalo

Colección: Manuales PC (www.manualespc.com)
www.nowtilus.com

Título: *Seguridad en Internet*
Subtítulo: Una guía práctica y eficaz para proteger su PC con software gratuito
Autor: © Gonzalo Asensio

Doña Juana I de Castilla 44, 3º C, 28027 Madrid

Editor: Santos Rodríguez
Responsable editorial: Teresa Escarpenter
Coordinador Editorial: Sergio Remedios

Diseño y realización de cubiertas: Carlos Peydró
Diseño de interiores y maquetación: Grupo ROS
Producción: Grupo ROS (www.rosmultimedia.com)

ISBN: 84-9763-293-1
ISBN13: 978-849763293-5
Depósito legal: M. 15.578-2006
Fecha de edición: Mayo 2006

Printed in Spain
Imprime: Imprenta Fareso, S.A.

Índice

1

Introducción

En este primer capítulo vamos a hacer un repaso general de la informática desde su aparición. De forma más concreta, veremos la evolución que ha tenido la seguridad y analizaremos ese nuevo mundo llamado «**la era de Internet**».

El autor no pretende entrar en detalles en este aspecto y de ninguna manera pretende aburrir al lector con una historia tecnológica, pero cree importante mencionar unas líneas para situar la comprensión actual en grandes rasgos generales.

Los avances tecnológicos del ser humano a lo largo de la historia son innumerables. Sin duda alguna estos adelantos nos han situado en una sociedad marcada por la tecnología, en la que unos pocos han intentado olvidarse de ella y se han visto retrasados ante el avance de la vida actual.

En siglos anteriores, la situación era diferente, ya que estos adelantos (como la electricidad entre otros), en un principio fueron privilegio de unos pocos adinerados de la época, y no todo el mundo podía acceder a ellos.

Pues bien, con los ordenadores pasaba lo mismo, había pocos y para unos pocos. Allá por los años cincuenta cuando se pusieron en servicio los primeros ordenadores, la seguridad informática no era una cuestión que plantease problemas a los administradores de sistemas ni a lo empresarios. Es más, ésta se basaba ante todo en una **seguridad física** (acceso físico al ordenador) y sólo especialistas cualificados podían controlar esas enormes máquinas, previniendo así la mala conducta de un trabajador malintencionado.

La tecnología fue avanzando con el paso de los años. Estas máquinas ya iban ocupando muchas habitaciones dentro del ámbito empresarial y sobre todo en el ámbito doméstico, y cada vez había más gente con conocimientos informáticos. No obstante, el mayor miedo de entonces, era que nos dejaran un disquete infectado por algún virus (cuyos efectos no pueden ni compararse con los de ahora), pero que hacía que muchas empresas o personas perdieran tiempo de trabajo y dinero. Puedo recordar uno de los primeros virus, que recibió el nombre de Cookie: apagaba el ordenador si el usuario no escribía la palabra Cookie. Si te apetece recordarlo, se habla del virus en la película **Hackers** (muy divertida por cierto).

La revolución en la informática llegó cuando, a mediados de los años 80, los ordenadores personales comenzaron a comunicarse entre sí mediante un dispositivo llamado **módem**. Este adelanto tecnológico abrió un sinfín de posibilidades en cuanto a negocio y comunicación, pero, al mismo tiempo, produjo una disminución de la seguridad informática, al exponer a equipos y redes completas a grandes ataques, desde virus a intrusiones malévolas.

Módem de 56 Kbytes

A partir del desarrollo del primer gusano informático o virus (su autor fue **Robert. T. Norris**, y se activó el 22 de noviembre del **año 1988)**, que produjo grandes perdidas económicas a muchas empresas, se creó en EE.UU. un organismo cualificado. Encabezado por ingenieros, y con el

nombre de **CERT** (*Computer Emergency Response Team*) (www.cert.org), se ocupó sobre todo de temas de seguridad y respondía de inmediaro después de un nuevo ataque con el antídoto y el aviso correspondiente.

Pagina Oficial del CERT

A partir de esos años, las empresas ya no sólo tienen que proteger físicamente sus sistemas, sino que además deben proteger sus comunicaciones, que es sin duda lo más costoso y difícil de conseguir.

En la actualidad, los ordenadores se han convertido en parte de nuestras vidas con la llegada de la red de redes (Internet).

>>> ¿Qué es Internet?

Internet es un espacio formado por dispositivos de comunicaciones, servidores y ordenadores que gracias a su estructura permite la comunicación entre millones de ordenadores.

Sin duda es difícil encontrar una empresa o incluso casa que no disponga de ordenadores y servicios de Internet. Por ello, es muy importante tener en cuenta que estos dispositivos están altamente ligados al negocio y al trabajo personal, y que de ellos dependen miles y miles de millones de euros.

Mapa mundial de comunicaciones en Internet

La tecnología ha hecho que estemos en un mundo estructurado con hilos de fibra. Ahora es cuando debemos plantearnos el reto de saber de seguridad informática. En el futuro, será como saber cocinar, es decir, algo cotidiano y normal, ya que nuestras vidas estarán aún mas sujetas a los avances tecnológicos. Esto es sólo el principio. Imaginad que tenemos un negocio y que lo llevamos a través de un móvil. Pues bien, recientemente se han descubierto varios virus para el teléfono móvil; si nos infectásemos con uno de ellos, todo nuestro negocio quedaría nulo por completo.

De igual forma, dentro de un tiempo todas las casas estarán robotizadas (domótica). Es un proceso que no tiene fin. Por eso, animo

2

Seguridad Informática para tod@s

En este capítulo se aborda la introducción de la seguridad informática, lo que necesitamos, lo que es la seguridad informática y sobre todo qué es lo que buscamos.

La intención de todo el libro es que el lector se sienta cómodo, que no crea que está leyendo un libro de informática, sino que está hablando con un amigo que antes tenía sus mismos problemas pero que ahora, gracias a unos consejos que ha aprendido, ya no los tiene, y se lo esta contando tranquilamente y de manera amena, ya sea en el sofá de un salón, en la playa o en el trabajo.

>>> ¿Por dónde empezar?

La verdad, aunque suene a broma, es que lo primero que necesitamos es tener ordenador, y digo esto porque seguro que el 98 % de los lectores tienen ordenador, o al menos eso espero, ya que de poco servirá leer este libro en caso contrario. Hago mención de este tema tan simple, por el hecho de que es hora de plantearse varias cosas acerca de nuestro ordenador tanto personal como empresarial.

Igual es buen momento para pensar en cambiar de ordenador o a lo mejor hay algún lector que está en la situación de querer comprarse uno. Por ello, daré algunos consejos sobre el sistema operativo. En el plano del hardware (parte física del ordenador), en general ya vienen muy bien equipados. Desde un procesador de 2,6 Ghz en adelante, y una memoria de 1 giga de RAM, da igual si es Intel o AMD, ambos van muy bien.

Algunos tendrán el sistema operativo **Windows XP profesional**, otros el Home Edition, y los más antiguos Windows 2000 profesional, Windows 98 y 95. Mi consejo personal es que siempre se tenga el sistema más moderno, ya que con el tiempo dejan de dar soporte y los fallos de seguridad se multiplican mes a mes.

Es por tanto un primer consejo, que además nos ayudará a ir siguiendo la guía de seguridad paso a paso. En este caso nosotros utilizaremos Windows XP profesional, aunque la mayoría de las herramientas nos sirven para otros sistemas operativos de igual tecnología como es el Windows 2000 Profesional. Para quien no tenga instalado ningún sistema, tiene fácil decisión, para quien lo tenga instalado, le recomiendo que comience una instalación nueva, ya que nunca sabemos qué es lo que puede tener ese sistema. Es, por tanto, un momento fenomenal de darnos una oportunidad para empezar a conocer nuestro sistema y asegurarlo de manera eficaz desde el principio.

Aprender a instalar un sistema puede parecer en principio complicado para el lector, y yo afirmo que instalar Windows no es nada complicado, pero hay que hacerlo al menos una vez para ver cómo se hace. Es la única forma de tomar la confianza necesaria para saber lo que hacemos y para saber lo que tenemos.

La gente tiene la idea de que arreglar ordenadores es complicado, pero yo afirmo que el 95% de las roturas son muy fáciles de solucionar, ya que sólo se trata de cambiar una pieza, y un ordenador no tiene demasiadas piezas. Es bueno que se comience cacharreando con algún ordenador viejo; verá que es más sencillo de lo que parece.

>>> ¿Qué es la seguridad informática?

Aunque no existe una definición exacta, es la capacidad de mantener intacta y protegida la información de sistemas informáticos.

3

Hackers, crackers y mundo underground

¿Cuántas veces has oído hablar de hackers?, ¿sabes quiénes son?, ¿por qué lo hacen? Estas y muchas otras preguntas se plantean un gran número de personas a las que nadie les resuelve su duda.

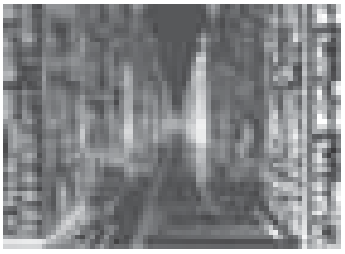
En este capítulo se habla de ello de manera general y la lectura del mismo lleva a la comprensión de conceptos que sólo conocemos de manera escasa y confusa.

Sin duda alguna es un tema apasionante, lleno de incógnitas y misterios ocultos, ya que los verdaderos hackers permanecen escondidos ante la mirada crítica de las empresas.

Veremos los diferentes términos con los que se les conoce a los llamados hackers, y su conducta dependiendo de su ideología.

Actualmente hay una mala interpretación guiada principalmente por gobiernos y medios de comunicación que hacen que el ciudadano de a pie entienda las cosas de manera equivocada.

Hay un gran interés en que la gente vea a los hackers como personas oscuras, malvadas y esto en realidad es una equivocación y ahora veremos y comprenderemos por qué.



>>> Mundo Underground

Llamamos mundo **underground** a toda esa comunidad de individuos que permanecen «ocultos» para compartir entre ellos sus conocimientos y experiencias.

Cada vez es más habitual la creación de grupos que en ocasiones rivalizan entre ellos aportando sus conocimientos. En Internet hay multitud de comunidades, la mayoría muy cerradas y ocultas, que tratan, explorar e indagan sobre cualquier tema tecnológico.

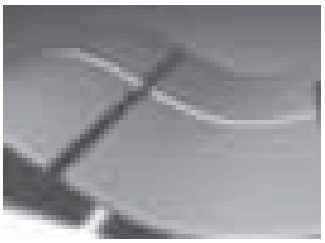
>>> Términos Hackers

En cuanto al término hackers, podemos distinguir entre varios tipos, según su conducta.

- **Crackers**: son aquellas personas que no respetan las leyes, se dedican a romper protecciones de programas, y cuando asaltan sistemas los dañan o perjudican de alguna manera. Sin duda alguna, cuando el telediario da una noticia sobre «un hacker asalta la base de datos de una empresa» se refiere a los crackers y no a los hackers.
- **Phreaker**: estas personas son especialistas en telefonía. Su función es la de intentar hablar gratis a través de cualquier medio telefónico. También son personas muy buscadas por la justicia sobre todo debido a la presión de las grandes empresas de telecomunicaciones.
- **Lamers o lammers**: son individuos que no tienen mucha formación técnica, pero saben manejar muchas herramientas para realizar un ataque. Están al día en los foros y tienen mucho tiempo libre. A menudo son acusados de ser los culpables de que los hackers tengan mala fama, ya que los lammers tienen una conducta ilegal e irresponsable.

4

Instalación del sistema operativo Windows XP Profesional



En este capítulo de instalación se va a explicar paso a paso cómo instalar un sistema operativo y aunque muchos lectores ya lo habrán hecho varias veces, mi recomendación es que sigan los consejos por si su sistema carece de alguno de los elementos.

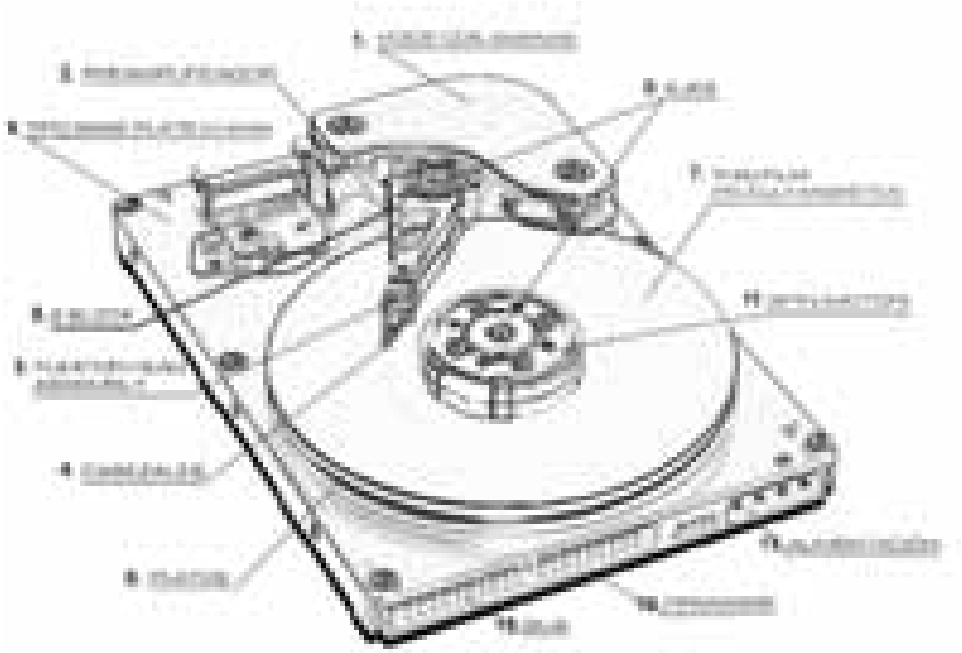
Este apartado es de mucha importancia, ya que va a ser la base de nuestro libro. Sobre este sistema operativo vamos a instalar y configurar todas nuestras herramientas de seguridad, por tanto debemos de hacer hincapié en los puntos más importantes del mismo.

Llega la hora de la instalación y algunos tendrán un ordenador nuevo que normalmente ya viene con un sistema operativo. La recomendación para este caso es que sigan la guía con ese sistema, pero si ya lo tienen hace un tiempo (por ejemplo, más de 15 días), recomiendo hacer una instalación limpia.

Cuando hablamos de una instalación limpia, nos referimos a que todos los datos que están en el disco duro se borrarán y se instalará un sistema nuevo encima. Aun así ese sistema estará obsoleto ante la seguridad y habrá que actualizarlo correctamente como veremos más adelante.

Imaginad que tengo 40 gigas de disco duro. Lo que haría entonces sería dejar 20 gigas para el sistema y 20 para datos.

Hay todo un debate sobre si es o no bueno particionar el disco, desde ya os digo que sí. Las razones, entre muchas otras, son que el sistema funciona más rápido y, sobre todo, el propósito principal de este libro: «es mas seguro», ya que los virus afectan principalmente a la partición del sistema, y si tenemos que reinstalar nuestro sistema de nuevo, siempre tendremos nuestra partición con nuestros datos; esto no se pierde nunca.



Partes de un disco duro

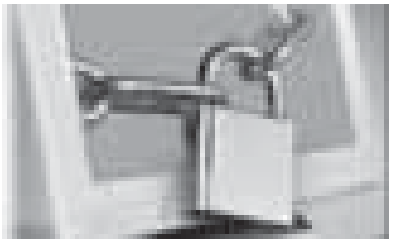
En el caso de que alguien ya tuviera un sistema instalado, aparecerá en pantalla una partición o varias. En este caso, debe eliminarlas con la **tecla «D»** y luego volver a crearlas de la misma manera que hacemos aquí.

NOTA: 1.000 MB es igual que 1 Giga.

Pulsando la **tecla «C»,** como podemos ver en la imagen, aparecerá una pantalla donde podemos seleccionar la cantidad de **MB** que queremos en las particiones.

5

Seguridad informática en Windows XP desde cero



En este capítulo abordaremos el tema de las principales configuraciones que dotarán nuestro sistema de seguridad, fiabilidad y compatibilidad.

Se explicará mediante ejemplos prácticos para aportar una visión más realista al lector.

Se trata el tema de la creación segura de usuarios tanto para compartir el ordenador como para compartir archivos con otros usuarios de la red. Aprenderemos a distinguir extensiones de archivos y, sobre todo, a establecer permisos de usuarios y a crear de manera óptima contraseñas eficaces y seguras para nuestro sistema.

Veremos diversos puntos, desde parámetros que vienen mal configurados por defecto en Windows, hasta las«molestas» pero necesarias actualizaciones del sistema. Las actualizaciones están a la orden del día y es una de las primeras responsabilidades del usuario informático, con ellas conseguimos que nuestro sistema esté siempre actualizado ante las últimas vulnerabilidades conocidas.

Al finalizar tendremos una amplia visión de lo que es la seguridad en cuanto al sistema operativo. Una vez realizadas las principales configuraciones en el sistema, dispondremos de un sistema seguro que será la base de la utilización de las herramientas de seguridad que se describen posteriormente.

Sin duda alguna se trata de un capítulo que sorprenderá a más de uno por los temas tratados y por la forma en la que se trata.

>>> Actualización del sistema

Antes de llegar a los programas que nos harán la vida más fácil, voy a dar unos consejos de cómo configurar nuestro sistema operativo de una manera segura, y diréis: «¿Si está recién instalado, cómo es que está mal?».

Pues sí, Windows XP viene con algunas cosas mal configuradas y, lo más importante de todo, está sin actualizar. Haced por un momento cálculos:

Si para Windows XP salen unas 50 vulnerabilidades mensuales, eso multiplicado por los meses que han pasado desde que salió el sistema la primera vez hasta ahora, dan muchos fallos de seguridad acumulados. Por ello es fundamental actualizar el sistema y mantenerlo siempre al día. Para ello nos vamos a la página de Microsoft **http://www.microsoft.com** y pinchamos sobre **Windows- update**:

Windows update es el nombre que reciben los servidores principales de Microsoft, para descargar e instalar las actualizaciones tanto de seguridad como del propio sistema.

6

Configuración óptima de usuarios y la importancia de las contraseñas

Algunas veces en charlas o coloquios personales he oído hablar a ciertas personas de que si yo era un exagerado por tener **usuario** y **contraseña** en el ordenador de mi casa, pero no puedo evitar decirles y comentarles los peligros que eso conlleva y no me refiero a peligros del tipo «¿Quién va a usar tu ordenador en tu casa?». No, aquí hay algo más peligroso que si tu hermano, padre o hijo pueden ver tus datos personales y es que los puedan ver personas ajenas desde Internet u otra ubicación.

En nuestra completa instalación, hemos puesto contraseña al usuario administrador.

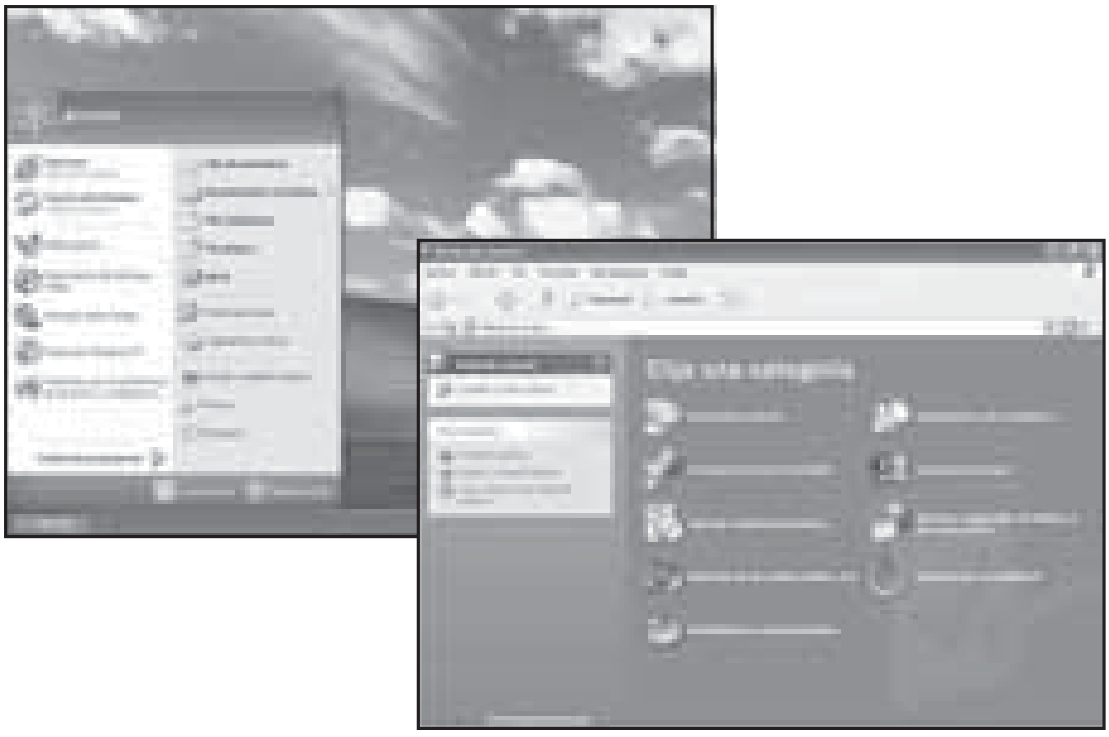
>>> ¿Quién es el administrador del sistema?

El **administrador** es un usuario en Windows llamado así porque es el usuario con más privilegios dentro del sistema y hablamos de privilegios en el sentido de que puede hacer lo que quiera, como, por ejemplo, instalar programas, crear usuarios, poner permisos a otros en las carpetas, etc.

Pero este usuario no es el único administrador del sistema operativo, ya que podemos crear muchos usuarios con igualdad de privilegios que este usuario. Es el caso del usuario que creamos al final de la instalación (ver capítulo de instalación), pero con el gran inconveniente de que este usuario no tiene contraseña, ya que Windows no nos la pide en ningún momento. Esto es un gran error, ya que si sufrimos un ataque desde fuera (Internet) y consiguen entrar por no tener contraseña en el usuario, el atacante o intruso dispondrá de permisos suficientes para realizar cualquier maldad dentro de nuestra máquina.

Pues bien lo primero que debemos hacer es poner contraseña a nuestro usuario, para ello hay diferentes maneras, pero yo aquí voy a ir a lo **práctico** y **sencillo**, pero, sobre todo, a lo **efectivo**.

Lo primero que haremos será ir a **INICIO**, **PANEL DE CONTROL**.



Después, pulsamos sobre **CUENTAS DE USUARIO** arriba a la derecha. Como podéis ver en el Panel de control, tenemos diferentes apartados importantes para el sistema. Aquí es donde se puede configurar gran parte del sistema operativo como impresoras, instalar o quitar programas, etc.

7

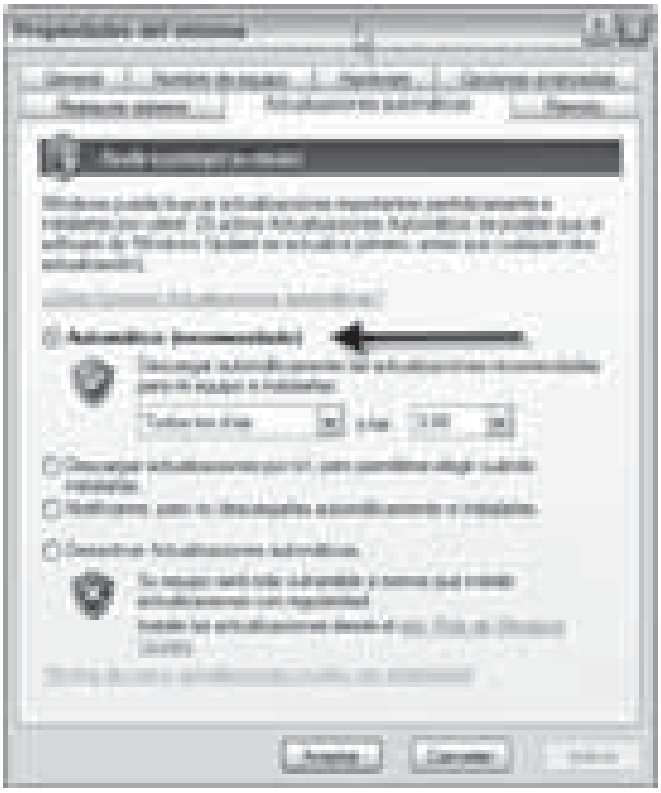
Primeras recomendaciones de seguridad en el sistema

En este apartado, voy a explicar las primeras recomendaciones que debemos tener en cuenta a la hora de configurar nuestro recién instalado sistema operativo.

A diferencia de lo que creen algunos, el sistema operativo como hemos podido ver en el anterior capítulo con las actualizaciones, no viene nada seguro por defecto. Esto es comprensible en cuanto a las actualizaciones, ya que nuestro CD con el sistema operativo no va a evolucionar con los últimos parches de seguridad. En el caso de la configuración por defecto, Microsoft no lo pone nada fácil; en vez de venir con ciertas configuraciones ya predeterminadas, los Windows y en este caso el XP, viene con ciertas carencias que si el usuario de a pie no conoce no puede valorar y solucionar.

Este tema es precisamente el que vamos a tratar en este capítulo del libro. Veremos cómo sacar partido a ciertos atributos que vienen ocultos y sin ninguna explicación en el sistema operativo.

Lo primero que vamos a ver es cómo podemos saber todas la extensiones de los archivos. Esto lo hacemos para determinar si es



Aquí tenemos que pinchar sobre la pestaña **ACTUALIZACIONES AUTOMÁTICAS** y en ella seleccionar **AUTOMÁTICO (RECOMENDADO)**. Con esta medida, conseguiremos que nuestro ordenador se preocupe de buscar actualizaciones de seguridad y del sistema.

Al configurar este parámetro veremos cómo en el Centro de Seguridad se pone verde la opción de las actualizaciones automáticas.

>>> Referencias

Página oficial para buscar extensiones de archivos y ver si son o no peligrosas.

http://filext.com/index.php

Página donde encontrar multitud de artículos básicos y sencillos, además de recursos de herramientas para proteger el PC.

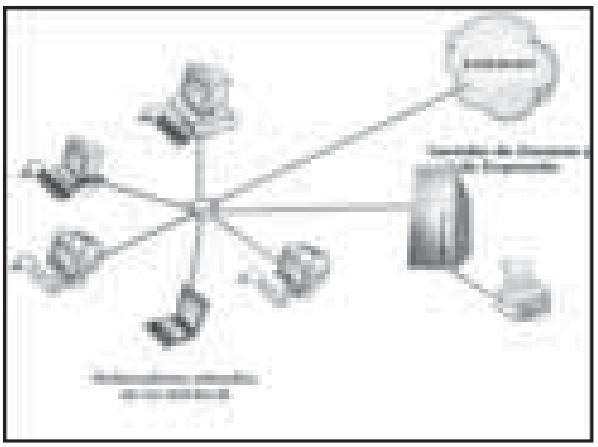
http://alerta-antivirus.red.es/portada/

8

Redes locales y seguridad en Windows

>>> Configuración de la tarjeta de red para hacer una red local domestica

Para poder comunicarnos con otras máquinas de nuestra red, necesitamos varios ordenadores cada uno con tarjeta de red, un router (con varias bocas) o un hub/switch para poder conectar varios ordenadores.



Esquema típico de red local con router y servidor de dominio e impresión

Nuestra tarjeta de red requiere ser configurada para poder comunicarnos con un lenguaje común.

Para configurarla debemos ir a **MI PC**, **PANEL DE CONTROL**, **CONEXIONES DE RED E INTERNET**, **CONEXIONES DE RED** y vemos esto:

Aquí podemos ver nuestros dispositivos de red. El que nos interesa configurar es **CONEXIÓN DE ÁREA LOCAL.** Hacemos doble clic sobre él y vemos esta ventana:

Aquí tenemos que pinchar en la pestaña **PROPIEDADES** y vemos en la opción del medio al final esto:

Pulsamos sobre **PROTOCOLO INTERNET (TCP/IP)** (más tarde veremos qué es esto) y al seleccionarlo pulsamos **ACEPTAR.**

9

Seguridad más avanzada en Windows XP

Todos estos consejos son muy interesantes y efectivos pero recordad que la mayor parte de la seguridad está en vuestras manos, en vuestro comportamiento, en vuestra decisión. Perdonad si soy algo pesado con este tema recordándolo constantemente durante el libro, pero la intención es la de concienciar no sólo al usuario, sino también a la persona.

Después de esta breve reflexión, vamos a continuar con el tema que nos atañe.

Hasta ahora todas las técnicas explicadas eran para proteger el sistema y así evitar desastres no deseados. Pero bien, estos siguientes puntos tratan por supuesto de prevención, pero también de observación y conocimiento de lo que ocurre en nuestro sistema operativo. A priori son explicaciones para personas cualificadas o metidas en el mundo informático, pero mi explicación seguirá en el mismo tono que hasta ahora, por lo tanto intentaré que todos los lectores sepan qué es lo que pasa en su sistema de manera amena y comprensible.

Antes de llegar al ejemplo práctico, quiero explicar cada concepto de la manera más sencilla y posible.

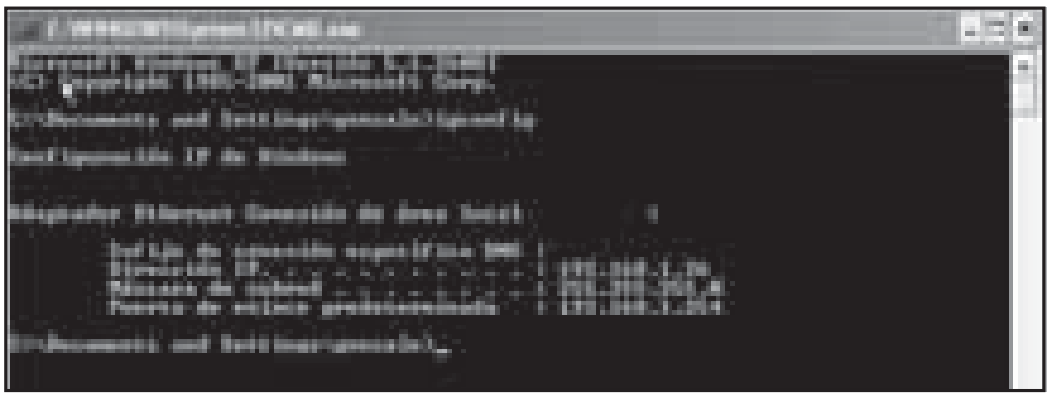
Al pulsar **ACEPTAR**, en ese momento nos saldrá una ventana como ésta:

La vuestra será igual, pero con otro nombre de usuario, que en mi caso es Gonzalo.

Esta misteriosa ventana negra no es otra cosa que una consola interna de comandos. Desde aquí podemos hacer infinidad de cosas todas ellas por comandos y la mayoría en formato texto. Esta consola es muy importante para cualquier administrador de sistemas, y por supuesto para nosotros ya que nos servirá para conocer mucho más nuestro sistema.

>>> ¿Cómo saber la dirección IP del ordenador?

Lo primero que debemos saber es nuestra dirección IP. Una IP es como el D.N.I. de una persona, es como la dirección de una casa, y gracias a esa IP (que es un número) los ordenadores saben dónde están los otros en cada momento. Para saber cuál es nuestra IP desde la línea de comandos (cmd), tenemos que poner el comando **IPCONFIG** (en minúsculas) y al pulsar **INTRO** nos saldrá algo como esto:



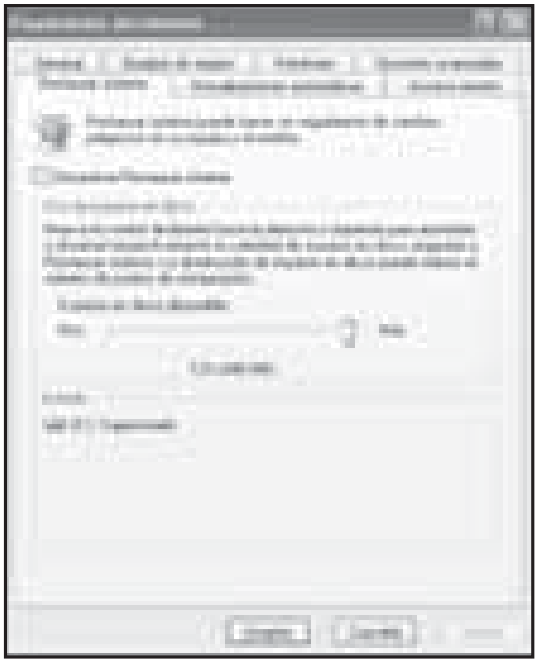
10

Técnicas para recuperar el sistema operativo y proteger datos

Poco a poco pero de manera eficiente, estamos consiguiendo un sistema cada vez más seguro. Gracias a estos sencillos consejos podemos disponer de un ordenador bien protegido, pero el tema de la seguridad va más allá y me refiero a que a veces no basta con tener un sistema protegido hasta los dientes. ¿De qué sirve tener todo protegido si un día sale un nuevo virus que nuestro antivirus no reconoce y perdemos toda la información que hay en nuestro ordenador? En esta parte del libro veremos una herramienta para evitar el desastre en nuestros datos y realizar planes de contingencia.

En primer lugar deberemos siempre mirar por la protección de nuestros datos, sobre todo de aquellos que son importantes para nuestro día a día o que, simplemente, tienen un cierto valor. ¿Os acordáis al principio cuando recomendaba realizar dos particiones? Pues bien, esa es una de las medidas, ya que lo que tenemos que hacer es guardar toda la información valiosa dentro de esa partición. Yo, por ejemplo, estoy guardando lo que escribo del libro en otra partición; cuando digo otra partición, me refiero a una distinta a la que tiene el sistema instalado, que suele ser por defecto la unidad (c:). Lo bueno de esta configuración es que cuando el sistema operativo quede

Al pulsar sobre **PROPIEDADES**, aparecerá una ventana con varias opciones y parámetros tales como el nombre del equipo y las características técnicas. Pero la pestaña que nos interesa es la llamada **RESTAURAR SISTEMA**. Pulsaré sobre ella y aparecerá un recuadro similar al que muestra la siguiente imagen:



Tras asegurarnos de que la pestaña que pone **DESACTIVAR RESTAURAR SISTEMA** no está activa, ya podemos realizar nuestro primer punto de restauración.

CONSEJO: Para realizar un punto de restauración, debemos estar seguros de que nuestro sistema está tal y como queremos que esté. Esto quiere decir que esté libre de virus, con todos los drivers instalados y con todos los programas que queramos utilizar, ya que cuando lo restauremos volverá a este estado en el que lo marcamos como punto de restauración. No obstante, después podemos ir añadiendo programas y otras cosas, verificar que todo va bien y volver a crear un punto nuevo de restauración más actual. También es normal que alguna actualización del sistema o incluso determinados programas te creen puntos de restauración en el sistema, por lo tanto siempre podremos recurrir a ellos en caso de producirse un error.

11

Amenazas en Internet, navegando de manera segura

Sin duda alguna el mundo de la informática no hubiese llegado a este nivel de expansión sin uno de los mayores inventos de la historia, me refiero por supuesto a Internet.

Gracias a Internet, millones de personas pueden comunicarse entre sí y pueden compartir el conocimiento haciendo mucho más grande el intelecto personal de la gente. En Internet nos encontramos con todo un universo de datos con un solo clic. Es una ventana a un nuevo mundo en el que nadie quiere faltar, lo que ha provocado que ocupe un lugar muy importante tanto para empresas como para particulares.

Para navegar por Internet sólo hace falta una conexión y un navegador. Es este último el que interpreta el lenguaje de los ordenadores para navegar (HTTP- Hyper Text Transfer Protocol) y no lo muestra de manera normal a los usuarios.

Como he comentado antes, en Internet está absolutamente todo, tanto lo bueno como lo malo, y eso hace que debamos ir preparados para evitar más de un disgusto.

Las amenazas más típicas de Internet van desde el contagio con un virus a ser hackeado por un troyano, etc.

La inocencia de ir navegando y pinchar en algo llamativo puede provocarnos más de un problema, puesto que con ese clic puedes estar aceptando que un archivo espía registre las paginas que visitas o incluso que te localicen el número de la tarjeta de crédito.

Para estar bien preparado e ir por Internet sin miedo a nada, basta con un poco de sentido común y un buen navegador; es el caso del navegador de moda: **FIREFOX**.

Firefox es una derivación del proyecto Netscape. Se trata de un navegador web rápido, estable, fiable y sobre todo muy seguro.

>>> ¿Por qué Firefox es seguro?

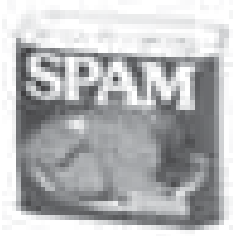
¿Y por qué es seguro? Es seguro porque su configuración desde el código ha sido pensada para ser segura y eficaz. A diferencia de Internet Explorer (que es el navegador que Microsoft incluye en sus sistemas operativos), Firefox presenta seguridad a la hora de visitar páginas Web anómalas o simplemente bloquear esos popups publicitarios llenos de spyware y malware. Gracias a su sencillo uso, podemos disponer de una navegador sensacional para disfrutar en Internet.

Una de las cosas comunes entre los navegadores es que la mayoría de los virus, troyanos, spyware, etc. están programados para que Internet Explorer se vea afectado por ellos, con lo que corremos mucho riesgo de ser infectados por cualquier archivo anómalo.

Hay últimamente una serie de artículos que hablan de que Internet Explorer es más seguro que Firefox. Mi recomendación es que se lea con precisión ya que se ha demostrado que Firefox no sólo es más seguro sino que sus desarrolladores tardan muchísimo menos que Microsoft en sacar un parche con la solución. También se ha demostrado que las vulnerabilidades encontradas en Internet Explorer son mucho más graves y han estado durante bastante más tiempo sin ser resueltas. Lo que pasa que hay muchos intereses creados con respecto a este tema. Sin duda alguna hasta la aparición de Firefox nadie le había hecho frente a Internet Explorer.

12

Seguridad en el correo electrónico, luchando contra el spam



En este capítulo hablaremos de una de las acciones más comunes por parte de los internautas, que es precisamente el uso del correo electrónico. Enviar y recibir correo se ha convertido en más que una simple acción. Internet y, en especial, el correo electrónico ha revolucionado la tecnología tanto en las empresas como en el hogar.

Una de las principales lacras con las que cuenta el correo es el famoso SPAM o correo basura. Este nombre se aplica porque el spam era un sustituto de la carne durante la segunda guerra mundial con lo que se daba a entender que era carne adulterada.

No obstante, el problema del spam va más allá que carne adulterada. Actualmente es una de las mayores preocupaciones en la era tecnológica, contra la que desgraciadamente podemos decir que no existe una solución total.

>>> ¿Por qué se envía spam?

Pues muy sencillo, porque es fácil, cómodo y rápido. Existen en el mercado muchos programas que permiten mandar miles de correo

en un espacio muy reducido de tiempo y con que sólamente una de las personas a las que llegue compre el producto, ese envío masivo habrá sido más que rentable.

En este apartado se explica cómo los **spamer** (personas que se dedican a mandar spam) se hacen con nuestra cuenta de correo para luego lucrarse con la venta de bases de datos con miles de correos y mandar millones de correos spam ofreciendo alargadores de miembros sexuales, métodos de adelgazamiento o cualquier otra cosa que se les ocurra.

>>> ¿Dónde denunciar el abuso del spam?

Tanto la polémica **ley 34/2002** de Servicios de la sociedad de la información y de comercio electrónico (**LSSICE**), como la ley orgánica **15/1999** de protección de datos de carácter personal (**LOPD**) protegen jurídicamente al usuario ante acciones de envío de correo comercial no autorizados expresamente por él mismo.

Cualquier persona puede denunciar el envío de spam a su cuenta de correo personal o de empresa. Una de las direcciones de las que podemos valernos para cualquier denuncia en cuanto a delito informático es la de la página web de la Guardia Civil, más concretamente el equipo de delitos informáticos (ahora llamado Grupo de delitos telemáticos):

http://www.guardiacivil.org/telematicos/creacion.htm

>>> ¿Cómo encuentra el spamer nuestro correo?

Nuestro correo es un tesoro muy buscado por los spamer, ya que cuando cuentan con un amplio número de correos, ganan mucho dinero en la venta de los mismos o mediante otros métodos. Por ejemplo, una empresa contrata a un spamer para intentar vender un producto y el spamer nos manda un correo con la publicidad y un link como éste:

http//www.loquesea.com/productos/id=2342

fraudulento, con lo que evitarás ser estafado con este método. También la herramienta Netcraft (explicada en el capítulo de navegación segura) nos ayuda en este tipo de fraudes, ya que nos marca los correos que intentan hacer phising como de riesgo elevado.

IMPORTANTE: ¡No utilicéis los link para ir a webs!

>>> Spamfighter. Instalación, configuración y uso de la herramienta Spamfighter

Para su descarga tenemos que ir a su página oficial que es:

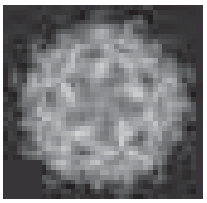
http://www.spamfighter.com/download_download.asp

Debemos descargarnos la versión gratuita que es muy buena y perfecta para un uso personal.

Una vez descargado el programa, debemos pinchar sobre el archivo .exe y tras una breve mini-instalación nos aparecerá esta pantalla:

13

Di ¡no! a los virus, aprende a luchar contra ellos



Hoy en día y sin duda alguna, una de las cosas más comentadas por los usuarios de las nuevas tecnologías es la frase «mi ordenador se ha infectado con un virus», «he perdido los datos por un virus», etc. Estas y muchas otras frases hacen que cada día miles de empresas pierdan miles de millones de euros. Es, por lo tanto, uno de los problemas más importantes a tener en cuenta dentro de una estructura empresarial a nivel usuario y también en nuestra propia casa. Debemos poner las barreras suficientes para evitar que esta plaga entre en nuestros ordenadores.

En este capítulo voy a exponer una breve definición de lo que es un virus, qué características tiene y cómo se pueden clasificar según su conducta. Tras esta explicación y con un ejemplo práctico instalaremos un antivirus freeware (siguiendo la política del libro).

Todo ordenador que esté conectado a una red, ya sea una Intranet o cualquier tipo de red en la que se puedan compartir archivos por el protocolo que sea, debe tener un antivirus instalado. Pero, como se ha demostrado a lo largo de la historia, incluso las máquinas que no

y para su mayor propagación cuando infectan a un ordenador, se apropian de la lista de contactos del cliente de correo y se propagan enviando correos con la dirección robada a todos nuestro contactos (como si fuésemos nosotros). De esta forma, nuestros amigos o compañeros pensarán que realmente somos nosotros los que les hemos enviado un archivo adjunto, lo abrirán y volverán a infectarse y a propagarlo a otra agenda de contactos; todo de manera muy rápida y eficiente.

>>> Extensiones peligrosas de archivos

Para evitar ser infectados con virus a través del correo debemos seguir las instrucciones que vimos en el capítulo de spam. No obstante y vuelvo a insistir en ello, la prudencia y la educación del usuario frente a estos temas es más eficiente que cualquier antivirus.

Por ejemplo, si nos llegan correos con archivos adjuntos, nunca debemos ejecutar los que contengan extensiones como las siguientes, ya que éstos, si llevan un virus, tienen la capacidad de ejecutarlo infectando nuestro ordenador:

- **.exe (programa ejecutable)**
- **.com (programa ejecutable)**
- **.vbs (scripts de Visual Basic)**
- **.src (salvapantallas de Windows)**
- **.pif (archivos de información de programa)**
- **.bat (archivos de proceso por lotes)**
- **.eml (mensajes de correo electrónico, Microsoft Outlook)**
- **.dll (librería de vínculos dinámicos)**

Y si apreciamos algo raro, como, por ejemplo, que un documento Word ocupe demasiado en cuanto a tamaño, debemos confirmar con el emisor del correo si de verdad nos lo ha mandado él o no. De esta manera evitaremos el 90% de los virus.

>>> Propagación a través de disquetes y CD

Esta vía de infección es más tradicional y en la actualidad no funciona demasiado, ya que los creadores de virus no ven en ella la fuerza o repercusión que pueden tener con otras vías tales como el correo.

14

Control parental, cuida de tus hijos en Internet

Con la llegada de Internet, la sociedad actual ha vivido un revolucionario cambio, que en ocasiones puede llegar a ser incluso drástico y dramático según qué casos.

La conciencia del mañana ha cambiado el concepto de las cosas en las diferentes áreas de nuestra vida. Hoy en día ya es muy común que cualquier empresa tenga un portal en Internet, pero ya no es un simple portal, es toda una imagen corporativa, es toda una empresa virtual de nueva era. En Internet hay sitio para todos.

Debido a esta influencia de las nuevas tecnologías, los ciudadanos de a pie nos hemos visto obligados a involucrarnos de manera activa en esta fusión del avance y hemos tenido que aprender a mezclar las viejas costumbres con las nuevas.

Actualmente es muy raro ver o conocer alguna persona que no disponga de ordenador en casa. En los colegios se enseña a los niños desde pequeños a manejar ciertos programas educativos e incluso se ven obligados a buscar información en Internet para mejorar la calidad de sus ejercicios y trabajos.

>>> ¿Qué es y cómo actua un programa de control parental?

Un programa de control paternal tiene como principal finalidad controlar y gestionar la actividad de nuestro ordenador cuando no estamos presentes. Por lo tanto, controlamos el uso que los usuarios (que puede ser nuestro hijo) estén haciendo del ordenador.

Hay programas comerciales que permiten proteger los archivos poniendo permisos dentro del sistema, pero, como hemos visto en capítulos anteriores, eso no es muy difícil de realizar con nuestro propio sistema operativo.

>>> Elementos de un programa de control parental

Lo más importante que debe de llevar un programa de control paternal es:

- Filtrado de contenidos.
- Registro de conversaciones y actividad del ordenador.

El **filtrado de contenido** se basa en que cuando nuestro hijo vaya a navegar y quiera entrar por error o voluntariamente a una web con contenido restringido, este programa se encargue de evitar que pueda acceder a esa web. Es importante que este filtro de contenidos soporte diferentes idiomas para hacer una protección más eficiente y completa y que cuente con contraseña para proteger la configuración del mismo (hay mucho listo suelto). Además se recomienda que se pueda poner oculto a la vista, de tal manera que para el usuario sea completamente transparente e invisible.

En nuestro ejemplo práctico y para apoyarnos en herramientas gratuitas, voy a utilizar dos programas diferentes: uno es de filtrado de contenido y el otro es de captura de pulsaciones de teclado, lo que se le llama en el mundo de la seguridad **KEYLOGGER.**

>>> Uso del filtrado de contenidos Naomi. Instalación, configuración y uso de la herramienta Naomi

El primero se llama Naomi. El nombre viene de la dedicatoria del desarrollador del programa a la hija de su mejor amigo y lo podemos

15

Cuida tu privacidad. Archivos espías (Spyware y Malware), dialer, etc. Aprende a combatir contra ellos

Es indiscutible que los avances en la informática han revolucionado el mundo en todos sus aspectos, y han traído muchas ventajas en un cambio constante que no cesa.

Pero todo este avance en cuanto al tema de Internet tiene sus pros y contras como hemos visto durante toda la obra. Hay multitud de cosas de las que protegerse y de las que debemos hacer una valoración global para no flaquear en ninguna de ellas.

Todas las medidas son pocas en seguridad. No existen sistemas seguros 100%, hay sistemas más o menos fiables, pero no del todo seguros.

Una de las cuestiones que debemos tener en cuenta en nuestra seguridad personal es precisamente la **privacidad.**

En este capítulo se explica de manera práctica cómo proteger nuestra privacidad mediante herramientas, tanto del sistema operativo como herramientas externas.

>>> ¿Qué es la privacidad?

La privacidad se encarga de salvaguardar aquello que no queremos que sea visto o modificado por alguien que no tiene permisos para hacerlo. Es por tanto una cuestión vital, ya que aunque tengamos nuestro ordenador protegido «**hasta los dientes**» de nada servirá si alguien consigue acceder a los datos del mismo.

Con la entrada del comercio electrónico, empezó a aparecer una serie de nuevos programas denominador **spyware y malware** que tienen como finalidad robar la privacidad del usuario. Se instalan sin que el usuario lo sepa y algunos los podemos considerar como **mini-troyanos**, ya que actúan como un cliente (agente) que manda información (privada) del usuario de ese ordenador a servidores. Son capaces de saber las web por las que navegamos, qué links pinchamos, se adjudican las contraseñas almacenadas por defecto en el navegador, ralentizan nuestro ordenador, nos redirigen a otras web, etc.

Las principales vías de infección del spyware son:

- Al ejecutar algún archivo que contiene oculto spyware.
- Navegando por webs especialmente diseñadas para aprovechar alguna vulnerabilidad del sistema.
- Pinchando sobre algún POP-UP (ventana emergente).
- En la instalación de herramientas shareware o freeware (mirar la licencia).

Durante todo el libro hemos ido viendo medidas que ayudan a la privacidad, como por ejemplo eliminar los históricos del navegador, proteger las contraseñas almacenadas, correo cifrado, etc. Esto son medidas preventivas que debemos establecer para poner barreras de cara a proteger nuestra privacidad, pero las siguientes medidas son activas en el sentido que directamente vamos a ir a buscar los programas espías con la ayuda del mejor programa existente. Se llama **ADAWARE** y lo podemos descargar por supuesto gratuitamente desde este enlace en su web oficial:

http://www.lavasoftusa.com/spanish/support/download/#free

16

Sistema de detección de intrusos (IDS) ¡Aprende a pillarlos y acaba con ellos!

Sin duda alguna, es una realidad que hoy en día hay personas capaces de acceder a ordenadores a través de numerosas vulnerabilidades, y que, en la mayoría de los casos, no somos conscientes ni de a qué han accedido dentro de nuestro ordenador ni de quién ha entrado y de qué forma lo ha conseguido.

La seguridad informática ha evolucionado desde sus inicios. Actualmente hay métodos muy buenos para localizar ataques que sufren nuestros sistemas y redes, técnicas como el análisis forense pueden ayudarnos a encontrar la causa del ataque, quién y cómo lo ha hecho. Con estas técnicas obtenemos un doble beneficio, el primero emprender acciones legales contra el intruso y el otro corregir el fallo para que nadie más pueda aprovechar esa puerta que tenemos abierta.

>>> ¿Qué son los IDS?

Uno de los sistemas que se utilizan en la actualidad para asegurar redes son los llamados **IDS (Intrusión Detection System)**, sistemas

de detección de intrusos; éstos nos permiten detectar las intrusiones o accesos no permitidos en nuestra red y máquina.

Los IDS actúan como guardianes de la seguridad y en el momento que ven algo sospechoso lanzan una alarma para avisarnos de que algo inesperado está sucediendo, con lo que podemos actuar sobre ello.

En la familia de los IDS, se encuentran los **IPS**, que cuando detectan algo extraño, además de avisar, pueden actuar contra el ataque. Este sistema no es muy recomendable ya que puede haber falsos positivos y cortar nuestras propias conexiones legítimas.

>>> Diferentes tipos de IDS

En este capítulo, vamos hablar de los IDS, ya que es uno de los sistemas más importantes y sofisticados de cara a la seguridad. Dentro del grupo de IDS, tenemos diferentes definiciones:

- **HIDS (Host IDS)**: es un IDS que controla a una sola máquina, se encarga de monitorizar que el comportamiento de dicha máquina sea bueno; un IDS de host es capaz de protegernos ante modificaciones de un spyware de detectar si nos están creando nuevos servicios, etc.
- **NIDS (Network IDS)**: son IDS que analizan todo el tráfico de red que hay en ese segmento; son los más utilizados en empresas.
- **DIDS**: éste es un IDS que mezcla el HIDS y el NIDS (su uso es limitado dado la complejidad). Un buen ejemplo de DIDS es el proyecto OSSIM (Open Source Security information Management), en el cual yo trabajo actualmente como analista de integración junto al grupo de desarrolladores. Es un producto por supuesto opensource (código abierto y gratuito) y podemos encontrar información en su web oficial:

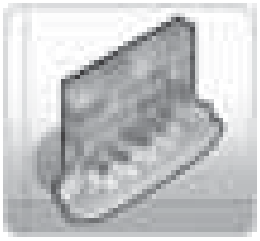
  http://www.ossim.net

Esta información es sólo para profesionales o personas con un conocimiento avanzado en temas de seguridad informática.

Desde aquí felicitar al equipo de **OSSIM** por su excelente trabajo y por su gran aportación al mundo de la seguridad informática. ¡Gracias chicos! ;-)

17

Firewall, pon una muralla en tu ordenador



Al principio de Internet, todos estábamos conectados sin protección alguna. Era una época en la que una masa minoritaria y, por qué no decirlo, privilegiada disfrutaba de una tecnología que no había tenido todavía su momento de explosión.

No existía la seguridad y ni tan siquiera nos importaba lo mínimo. Gracias a esto, los pocos intrusos o hackers del momento realizaron conductas llamativas y que todavía se recuerdan hoy.

Poco a poco y conforme las empresas fueron percatándose del peligro a base de perder tiempo y dinero, se empezaron a crear sistemas de seguridad para redes, entre ellos se encuentran los famosos Firewall.

Este capítulo abarca el mundo apasionante de los firewall (corta fuegos), gracias a estos las redes y ordenadores se encuentran protegidas ante multitud de ataques desde y hacia Internet.

La finalidad de esta sección es hacer comprender al lector de manera popular (como en todo el libro) cómo se producen las

comunicaciones y cómo podemos controlarlas mediante un firewall personal.

Por tanto, al finalizar la lectura tendremos en nuestro ordenador uno de los mejores firewall del momento y seremos conscientes de las comunicaciones en nuestro sistema.

>>> TCP/IP ¿Qué es?

Cuando utilizamos nuestro ordenador para comunicarnos, estamos utilizando para ello un conjunto de protocolos (normas establecidas), que hacen que los ordenadores puedan «hablarse en entre sí», es decir, que se entiendan para poder realizar operaciones, tales como descargar un archivo, navegar, etc.

Estos protocolos están estructurados por capas y se establecieron como estándar para todos los fabricantes de tal manera que desde cualquier tipo de red podemos comunicarnos haciendo uso correcto de estas capas.

Los llamados protocolos **TCP/IP** son un conjunto de protocolos que se componen principalmente de 5 niveles:

APLICACIÓN
TRANSPORTE (TCP)
IP
RED
FÍSICO

- **Nivel físico**: Corresponde al hardware y al medio utilizado (es decir puede ser un cable de fibra óptica o una línea telefónica).
- **Nivel de red**: Independientemente de cuál sea el medio físico elegido, necesitamos una tarjeta de red específica para que se produzca una comunicación correcta.

18

Seguridad Wireless. El futuro ya está aquí, aprende a protegerlo

Cuando a mediados de los años 80 los ordenadores empezaron a comunicarse entre ellos mediante el módem se logró un avance tecnológico que llegaría a nuestros días actuales con una gran revolución en cuanto a la comunicación.

Si hace 20 años le cuentas a alguien que puede hablar con un teléfono que no tiene cables y que lo puede hacer desde casi cualquier sitio, se echaría a reír y te tomaría por loco. Esta misma reacción hubiese ocurrido si por entonces le dices a un informático que los ordenadores se podrían comunicar entre sí sin necesidad de cables: ésta es la base de la nueva **tecnología wireless**.

Las redes inalámbricas cuentan con multitud de ventajas, desde resolver el problema del espacio hasta los costes de instalación, ya que se prescinde de los cables.

Sin duda alguna, esta y otras muchas ventajas han hecho que en la actualidad esta tecnología no falte en empresas y casas particulares e incluso en establecimientos públicos con puntos llamados **Hot Spot**.

Cada vez son más los equipos y dispositivos que se adaptan a esta tecnología, desde ordenadores de sobremesa a portátiles, PDA, cámaras, etc.

Una de las mayores preocupaciones actuales y que no se tuvo en cuenta en su día fue la seguridad wireless. En este capítulo voy a explicar por encima los estándares de comunicación y, por supuesto, un ejemplo práctico de cómo asegurar nuestra red de casa.

La tecnología wireless surge legalmente con la creación el 1999 de la organización **Wi- Fi Alliance (www.wi- fi.com)**. Es la encargada de garantizar el cumplimiento de normativas y especificaciones para el correcto funcionamiento de las redes inalámbricas entre diferentes fabricantes compatibles con la norma **802.11b** desarrollada por el **IEEE (Institute and Electronics Engineers, Inc)**.

>>> Los estándares Wi-fi

Los estándares se componen principalmente de la siguiente manera:

- **Norma 802.11b** que opera en el espectro de los 2,4 GHz y puede llegar a tener una velocidad de transmisión de 11Mbps.
- **Norma 802.11a** que opera en la banda de 5GHz con velocidades de hasta 54 Mbps.
- **Norma 802.11g** que opera en las frecuencias 2,4-2,285 GHz. Este estándar fue aprobado en el año 2003 y su velocidad es de 36 a 54 Mbps.

Actualmente hay un estándar en fase de desarrollo denominado 802.11n, pensado para paliar las necesidades de velocidad y ancho de banda actuales en esta tecnología.

Este nuevo estándar promete velocidades de transmisión desde los 150 Mbps a 350 Mbps, esperando llegar en el futuro incluso a los 600 Mbps.

>>> ¿Son seguras las redes wireless?

Las redes inalámbricas, en todos sus ámbitos, se han convertido en una gran alternativa a las redes convencionales por cable. Pero todo este avance, ¿es seguro?

19

Seguridad en p2p. ¡No seas uno más! ¡No dejes que te espíen!

Cuando hablamos de Internet, estamos hablando de comunicación, libertad, expresión, etc. Sin duda alguna se trata de un espacio libre y abierto para que cualquier persona pueda exponer o buscar lo que desee.

Nadie en su momento se hizo eco de lo que puede suponer este avance tanto en lo positivo como en lo negativo, pero la realidad es que las cosas existen en Internet y creo sinceramente que deben de existir, señores:

«**Internet lo formamos tod@s y para tod@s**».

Tras esta breve reflexión mental que hace de entrada a este apasionante tema que es el de las redes p2p, lo que vamos a ver en este capítulo es cómo estar seguros utilizando programas de intercambio de archivos.

Actualmente no hay casi nadie que no haya oído hablar de las redes p2p, de su uso, de sus ventajas, desventajas, legalidad, etc.

coordina a los clientes. Los clientes para esta red son: eDonkey 2000 hibrido, Overnet.

- **eDonkey http://www.edonkey2000.com/**
- **Overnet http://www.overnet.com/**

La red Kademlia: Ésta es una de las redes más usadas en la actualidad; en ella se comparten todo tipo de archivos. Cliente bien conocido, eMule.

- **eMule http://www.emule- project.net**

La red bittorent: Esta red está adquiriendo mucha fama ya que su velocidad de descarga es superior que la de las otras redes. Aquí compartes lo que descargas, en ese mismo momento. Clientes: Bittorrent, Bitspirit, Bittornado, etc.

- BitTorrent http://www.bittorrent.com/
- Bitspirit http://www.167bt.com/intl/index.html#download/
- Bittornado http://www.bittornado.com/

La red Freenet: Ésta es una nueva red cuya característica principal es que es anónima, con todas las conexiones cifradas, con lo que garantiza la privacidad y seguridad del usuario. Cliente Freenet.

- **Freenet http://freenet.sourceforge.net/**

Como podemos apreciar, hay una cantidad de redes diferentes donde podemos elegir el cliente que queramos a nuestro gusto. Mi recomendación, siempre y cuando no se use la red freenet, es usar eMule, y en la red Bittorent, usar el cliente Bitspirit ya que satura muy poco los recursos del sistema.

>>> Recomendaciones de seguridad en las redes p2p

En cuanto a la seguridad p2p, debemos estructurarla por partes. La primera se basa lógicamente en fallos o vulnerabilidades en el propio cliente software, ya que mucha gente se intenta aprovechar de ello mediante fallos en viejas versiones no actualizadas.

Mucha personas se descuidan con respecto a las actualizaciones y esto es otro ejemplo claro de que debemos tener todo bien actualizado y parcheado. La solución para esta nota de seguridad está clara: tener

Conclusión

A lo largo de todo el libro, hemos tratado numerosos temas dentro del mundo de la seguridad informática y hemos conseguido, mediante el seguimiento de las prácticas, tener ahora un sistema más seguro y eficaz.

Se han tratado temas básicos, como es la instalación de un sistema operativo, pero visto desde el punto de vista de la seguridad; hemos comprendido por qué es mejor particionar y formatear con el sistema de archivos NTFS.

Una vez instalado nuestro sistema operativo, hemos configurado parámetros que no vienen por defecto con seguridad, hemos aprendido a crear usuarios, a compartir carpetas y a establecer permisos para que nuestros datos estén seguros.

A lo largo de la obra, he intentado concienciar al usuario de la importancia de las contraseñas, he mostrado cómo crear contraseñas seguras y cómo administrar un número elevado de ellas.

Para los más avanzados, se ha explicado cómo funcionan las comunicaciones, cómo identificarlas y cómo acabar con las que no son legítimas.

Conforme la obra ha ido avanzando, se han ido exponiendo temas y términos informáticos explicados de manera amena, de tal forma que ahora el lector se encuentra en una posición muy alta a nivel de «cultura informática» y sobre todo cultura del mundo de la «seguridad informática».

Se han realizado prácticas para navegar de manera segura, para salvaguardar nuestra privacidad navegando anónimamente y para adquirir una conciencia de la importancia de tener un buen navegador para protegernos en Internet.

Gracias al capítulo del correo hemos podido comprobar cómo se puede luchar contra el spam y cómo podemos configurar una cuenta anónima y gratuita para realizar acciones salvaguardando nuestro correo real.

Con este libro has adquirido un conocimiento global y certero de la seguridad. Es la primera obra que habla de manera clara, directa y práctica de temas como seguridad p2p, seguridad con IDS (Sistemas de detección de Intrusos) o seguridad parental.

Hemos aprendido que la seguridad es un cúmulo de cosas, es algo homogéneo, integral y que de nada vale estar muy seguro a nivel de Firewall, cuando nuestro sistema operativo es vulnerable y por lo tanto accesible.

Ahora disponemos de un sistema seguro y eficaz, lo único que debemos hacer es mantenerlo seguro con actualizaciones, mantener una actitud coherente hacia Internet y seguir los consejos que hemos visto desde el primer tema.

Es importante mantenerse actualizado en la información en el ámbito de la seguridad, por ejemplo, mediante listas de seguridad que nos mandan correos con fallos y vulnerabilidades aparecidas.

Con esta conclusión de que la seguridad está a partir de ahora en vuestras manos, me despido no con un adiós sino como un hasta luego.

Sin más os mando un cordial saludo y espero que la obra haya sido de vuestro agrado, y recordad:

«La seguridad informática es de tod@s y para tod@s»

Gonzalo Asensio Asensio
Master en Seguridad Informática

Anexo I: Analiza tu propia seguridad

En este apéndice vamos a aprender a conocer y valorar el nivel de seguridad de nuestro ordenador. Después de haber seguido las propuesta del libro, vamos a descubrir que podemos analizar la seguridad de otra máquina, ya sea de nuestra red local o de Internet.

Las auditorías de sistemas se realizan mediante muchas herramientas. Aquí vamos a explicar la herramienta para Windows, **X- Scan**.

Se trata de una magnífica herramienta que realiza ataques simulados contra la máquina que le digamos y elabora un informe muy completo sobre el nivel de seguridad de ese ordenador. También nos hace una recomendación de seguridad. El **X- Scan** se basa en las firmas del conocido programa de auditorias **Nessus http://www.nessus.org**, programa que hasta hace poco era **Open- Source** disponible para equipos **Unix/Linux**.

>>> Escaneador de Vulnerabilidades X-Scan

Podemos descargar X-Scan desde su web oficial:

http://www.xfocus.org/programs/200209/10.html
(La descarga no es muy rápida)

Una vez descargado, no requiere nada especial; sólo debemos de crear una carpeta y volcar el contenido del archivo descargado.

Al realizar esto, tenemos que hacer doble clic en el archivo **xscan_gui.exe** y veremos la pantalla principal; una vez aquí pulsamos sobre –**CONFIGURAR –PARAMETROS DE ANÁLISIS** y veremos una ventana como ésta:

Epílogo por José Barberá

«La seguridad informática es de tod@s y para tod@s», así finaliza este libro de Gonzalo Asensio, frase que resume la intención principal del autor, como deferencia y auxilio para todos los usuarios de Windows XP que navegan hoy por Internet.

Seguridad e Internet son hoy en día dos términos estrechamente asociados. En un estudio que el Gobierno holandés publicaba en agosto de 2005 sobre *El futuro de las comunicaciones electrónicas*, como base de reflexión para la elaboración de políticas infotecnológicas de cara al futuro, se indicaba que en la actualidad entre el 60 y el 80% del tráfico mundial de Internet es de aplicaciones bidireccionales (*peer-to-peer* o P2P), y que la seguridad, tanto global como individual, es el mayor problema al que se enfrenta la Red de cara al futuro: el tiempo medio que tarda actualmente cualquier ordenador nuevo que se conecta a Internet en ser atacado por algún tipo de software malicioso (*malware*: virus, programas espía, *phishing*, *zombies*, ataques de *hacker*...) es de 13 minutos.

Ésta es una de las preocupaciones transmitidas a lo largo de los diferentes capítulos: los riesgos que se deben afrontar cuando nuestro ordenador está conectado y las distintas maneras de protegernos. Hoy en día los ordenadores y la información no son nada si no están conectados. Esta conectividad la proporciona Internet, la red de redes, con las inmensas posibilidades de facilitar la comunicación entre personas y de proporcionar acceso a los servicios de la Sociedad de la Información, sobre cualquier medio y tecnología de transmisión, en cualquier lugar y desde una amplia gama de dispositivos.

De estos, el más extendido es el PC con el sistema operativo Windows XP. Sobre este entorno se desarrolla el trabajo del autor,

sistematizado a partir de sus conocimientos y experiencias personales, para hacer al usuario sentirse seguro, no solamente en el sentido de protegerse frente a posibles vulnerabilidades y ataques externos, sino también seguro en cuanto a la confianza en sí mismo, para manejar su barco particular mientras navega por las a menudo procelosas aguas de Internet.

Frecuentemente escuchamos en los medios de difusión que navegar por la red es fácil y sencillo, que está al alcance de cualquiera y que no requiere conocimientos especiales. Lo anterior es cierto, pero bajo unos determinados supuestos, que en ocasiones se obvian. Efectivamente, es fácil sentarse frente a un ordenador conectado a Internet y utilizar un navegador (el autor tiene claras sus preferencias: ¡*Firefox, por supuesto*!) para acceder a numerosas fuentes de información y sistemas de comunicación en todo el mundo. Esto lo hemos podido experimentar cuando navegamos desde la oficina, en un cibercafé o en casa de los amigos que tienen establecida su conexión a Internet y que alguien se ha preocupado de realizar.

La dificultad está muchas veces en llegar a configurar ese entorno de trabajo alrededor de uno o varios PC conectados, en el que nos sintamos seguros porque sabemos lo que hacemos y tenemos entre manos. Aunque cada vez resulta más sencillo poner en marcha el PC y el kit de conexión que hemos comprado en la tienda de informática, también es cierto que muchas veces vamos a piñón fijo para evitarnos sobresaltos. El libro pretende precisamente dar una serie de guías y orientaciones para conferir mayores destrezas al usuario. Siguiendo con el símil de la navegación, cualquier lector podrá profundizar en sus conocimientos técnicos para llegar a alcanzar el título de patrón de embarcación de recreo, patrón de yate o capitán de yate (dejamos para otra obra los títulos de la marina mercante).

Con un lenguaje coloquial, directo y comprensible, y con numerosos ejemplos prácticos de programas y aplicaciones a los que refiere al lector mediante la correspondiente dirección URL, Gonzalo Asensio nos va adentrando en las partes ocultas de Windows XP, ocultas no porque estén escondidas, sino porque normalmente no se presta atención a esas funcionalidades. De este modo, el lector podrá descifrar algunos «arcanos», como los temas relacionados con la compartición de archivos, en local o en red, por diferentes usuarios, caso típico de

familias como la suya, a la que usa como ejemplo a la hora de establecer la normativa de seguridad y los diferentes privilegios de acceso.

Configurar una red doméstica basada en Windows XP resulta ahora más sencillo tras haber recorrido los capítulos correspondientes. También se abordan temas de filtrado de contenidos y control parental, muy útil hoy en día en una buena parte de los hogares (aunque va siendo cada vez más frecuente que sean los hijos los que controlen el entorno informático). Precisamente por ello, a muchos padres les resultará de ayuda este libro, para sentirse seguros y mantener el ascendiente sobre sus hijos cuando de estos temas se trate.

El lector aprenderá fácilmente a distinguir los virus, los gusanos y los troyanos, así como a defenderse de ellos mediante herramientas que no tienen por qué ser onerosas. Lo mismo respecto a los programas de *spyware* y *malware* a los que me refería al principio, para los que da recetas y herramientas para proteger nuestra privacidad.

Especialmente prácticos e interesantes son los últimos capítulos dedicados a la detección de intrusos, la gestión de los cortafuegos y los procedimientos para aumentar la seguridad en redes inalámbricas Wi-Fi, aspectos todos ellos que están a la orden del día en pequeñas redes ofimáticas y domésticas, y que en muchos casos se suelen dejar a un lado por comodidad o por falta de confianza. Algunas veces hemos oído que seguridad y comodidad son dos términos contrapuestos. El libro de Gonzalo nos demuestra que tal contraposición es mucho menor de lo que puede parecer y que, en todo caso, vale la pena invertir algún esfuerzo en afianzar nuestro entorno informático.

Finalmente, el último capítulo dedicado a las redes P2P, que como vimos antes representa alrededor del 70% del tráfico mundial de Internet, nos sitúa en la perspectiva adecuada para considerar los diferentes aspectos de seguridad implicados, tanto en lo que se refiere a las vías de propagación de virus como al posible espionaje del que podemos ser objeto cuando nos asociamos a alguna de ellas.

Para concluir, solamente insistir en que este libro, de fácil lectura y tratamiento familiar, nos puede ayudar a desmitificar determinados misterios de Windows e Internet, de modo que podamos sentirnos más seguros y más libres cuando naveguemos desde nuestros ordenadores.

Los ejemplos y programas (gratuitos) que cita constituyen una valiosa ayuda para tal fin. Personalmente he tomado nota y descargado algunos de ellos; a partir de ahora espero poder bloquear en mi casa direcciones IP indeseadas, así como evitar intrusos o espías que invadan mi intimidad.

Gracias, Gonzalo, por haber contribuido a facilitar la navegación a este viejo lobo de mar. Seguro que habrá otros internautas que se sentirán más cómodos y confiados después de su lectura.

José Barberá Heredia

Doctor Ingeniero de Telecomunicación.
Asesor del Secretario de Estado de Telecomunicaciones
y para la Sociedad de la Información, Francisco Ros Perán

24 de abril de 2006

El lector que lo desee podrá ponerse en contacto con el autor en la siguiente dirección de correo electrónico:

gonzalo@seguridadeninternet.es

Así mismo, podrá encontrar nuevas informaciones y contenidos en las direcciones de internet:

www.seguridadeninternet.es

www.gonzaloasensio.com