Web: www.daic.net E-mail: daic@daic.net

Suministros Informáticos DAIC, S.L.

C/ Juan Ramón Jiménez, 12 - Bajo
Teléfono: 902 903 589 - Fax: 947 48 64 38
09007 - BURGOS.

www.escuelaformativa.com

Manual de Seguridad Informática.
Nivel I.

Defiende tu PC

Guía de seguridad para ordenadores personales

Sacha Fuentes Gatius

http//www.defiendetupc.com

Créditos

Editor: Gatex Quality, S.L.
Autor: Sacha Fuentes Gatius

Consejo de Ciento 453 entº 1ª; 08013
Barcelona, España
gatex@gatexquality.com

Primera edición: 2005, Barcelona

Índice de contenido

[Introducción]

Cuando conducimos una automóvil solemos ser conscientes de que problemas puede traernos un mantenimiento inadecuado de este. Tenemos claro que si dejamos la puerta de casa abierta es fácil que alguien entre a robarnos. Normalmente no se nos ocurrirá ir por la calle con una gran cantidad de dinero en metálico y mucho menos ir enseñándolo, por simple prudencia.

Por desgracia, lo más normal es que el usuario habitual de un ordenador no sea consciente de cuales son los problemas de seguridad y pérdida de privacidad que puede producir este uso. La mayoría de usuarios lo acaban aprendiendo una vez estos problemas les suceden a ellos, con las consecuencias que ello comporta. Esto es debido a la falta de un lugar donde se recopilen y se expliquen estos problemas; de aquí la necesidad de este libro, que pretende ser una introducción básica pero suficiente para que cualquiera pueda trabajar con su ordenador de modo seguro.

En el libro no se pretende que el usuario se convierta en un experto en seguridad informática sino que, simplemente, sea capaz de tomar las decisiones adecuadas cuando se enfrente a alguno de los problemas que aquí se explican y consiga salir airoso de la situación sin necesidad de recurrir al típico formateo y reinstalación del sistema.

Espero que la información proporcionada les sea útil.

ATENCIÓN

Supondremos que el ordenador utilizado por el usuario es un PC o compatible con el sistema operativo Windows 2000 o Windows XP instalado, ya que esta es la opción más generalizada entre la mayoría de usuarios de ordenadores.

[Capítulo 1]

Seguridad general

Parches

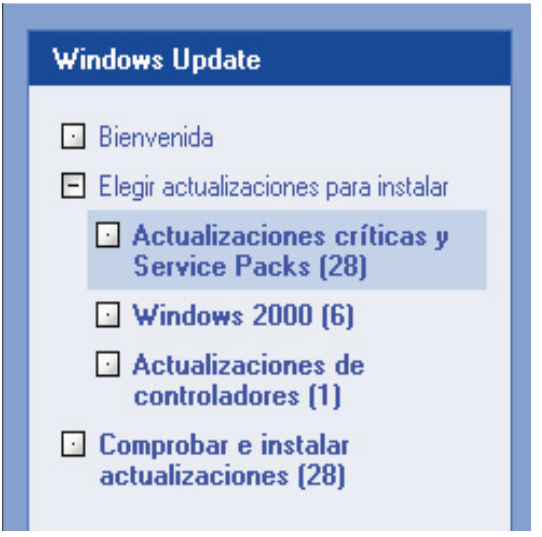
Cualquier programa de ordenador necesita de actualizaciones periódicas para solucionar posibles problemas que hayan podido descubrirse o ofrecer nueva funcionalidad. Estas actualizaciones son especialmente importantes en el sistema operativo, ya que es el que ofrece los servicios al resto de programas y el que más problemas de seguridad puede provocar. Las actualizaciones suelen ofrecerse en forma de parches que solucionan los errores de seguridad que se van descubriendo. Es muy importante estar al dia de estas actualizaciones para evitar posibles problemas.

Cada programa dispone de su manera particular de ser actualizado (sitio donde conseguir los parches, forma de aplicarlos,...) por lo que será importante conocerla individualmente para poder aplicarla.

Windows Update

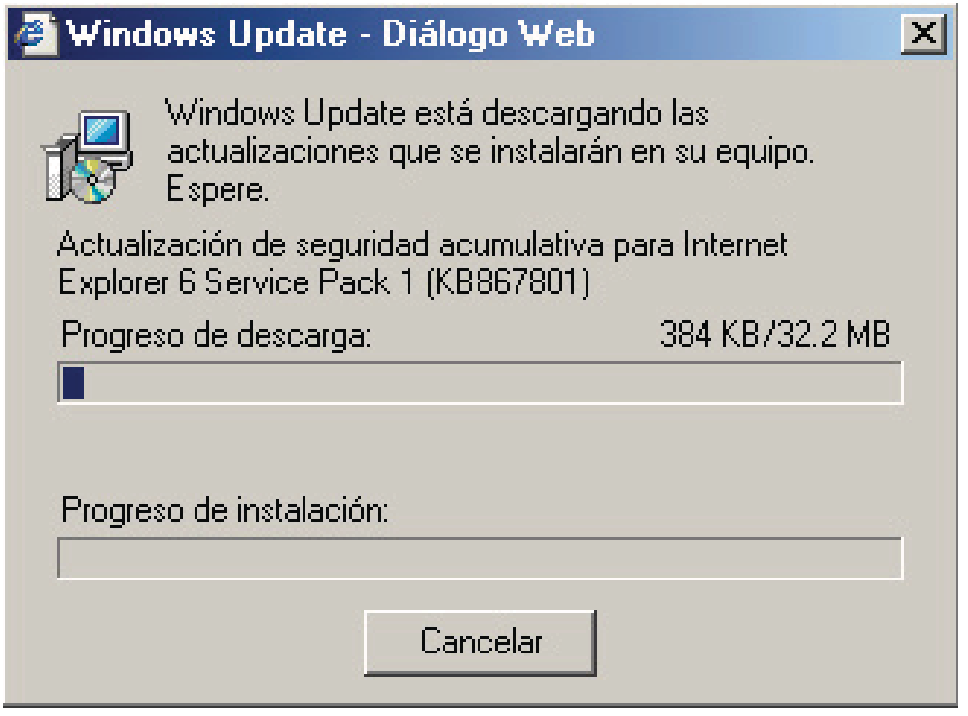
Una manera sencilla de mantener el sistema operativo actualizado es a través de Windows Update, la web de Microsoft donde, a través de un interfaz web, podremos ver cuales son las actualizaciones que tenemos instaladas y las que nos falta por instalar.

Una vez entremos en esta página, haremos clic en *Buscar actualizaciones*, momento en el cual se analizará el sistema para ver que actualizaciones son necesarias y podremos seleccionar individualmente cuales queremos instalar y cuales no.



Por defecto, el sistema seleccionará automáticamente todas las incluidas en *Actualizaciones críticas y Service Packs*. Podemos instalar el resto si las seleccionamos de la lista mediante la opción *Agregar*.

Una vez seleccionadas todas las opciones que nos interesen, pulsaremos *Comprobar e instalar actualizaciones* y finalmente haremos clic en *Instalar ahora*. En ese momento, se nos mostrará un diálogo donde aparece el estado actual de la instalación de las actualizaciones.



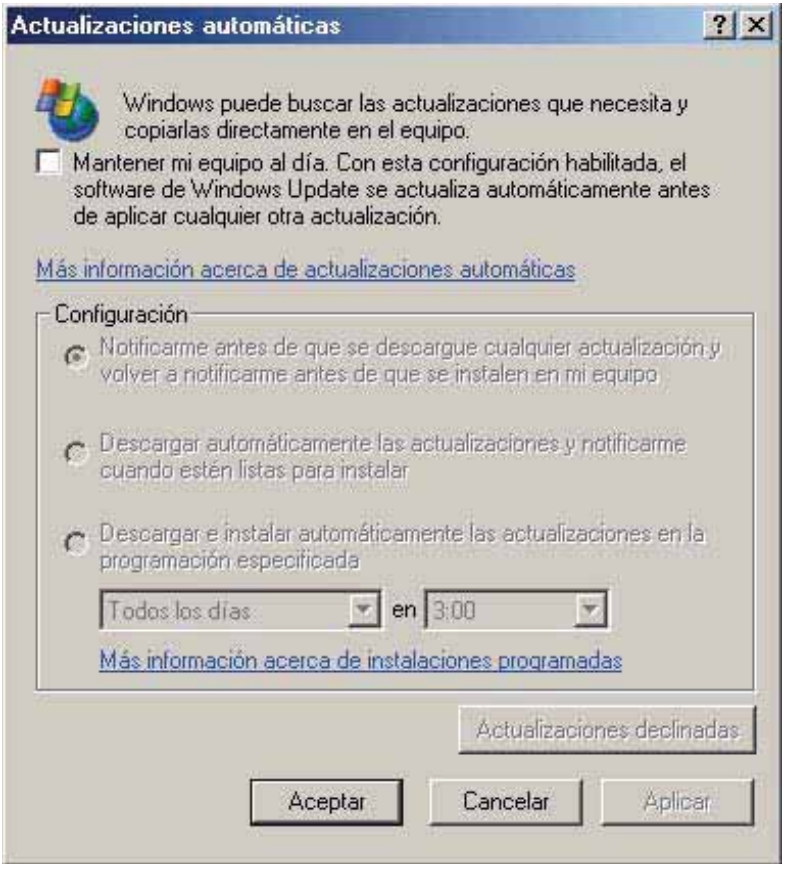
Una vez finalizado este proceso deberemos reiniciar el ordenador para que se apliquen todos los cambios. Además, es recomendable volver a ejecutar este proceso, ya que puede haber nuevas actualizaciones que deban instalarse a causa de las que hemos instalado anteriormente.

Actualizaciones automáticas

Aunque la primera vez que vayamos a instalar actualizaciones para el sistema operativo es recomendable hacerlo a través de *Windows Update*, este no es un sistema cómodo de mantenerse al día. Por ello, podemos utilizar el sistema de actualizaciones automáticas que Windows pone a nuestra disposición.

Para activarlas debemos ir a:

Inicio -> Configuración -> Panel de control -> Actualizaciones automáticas



En esta pantalla deberemos seleccionar *Mantener mi equipo al día* y en *Configuración* deberemos escoger entre las tres opciones disponibles:

- *Notificarme antes de que se descargue cualquier actualización y volver a notificarme antes de que se instalen en mi equipo*: Esta opción nos avisará cuando existan nuevas actualizaciones y nos permitirá seleccionar cuales queremos descargar y posteriormente cuales queremos instalar.
- *Descargar automáticamente las actualizaciones y notificarme cuando estén listas para instalar*: Esta opción nos avisará cuando las actualizaciones ya estén descargadas y listas para instalarse y nos permitirá seleccionar cuales queremos instalar.
- *Descargar e instalar automáticamente las actualizaciones e instalarlas en la programación especificada*: Esta opción nos permite despreocuparnos totalmente de las actualizaciones del sistema operativo, ya que él mismo se encargará de los nuevos parches que vayan apareciendo. Es recomendable activarlo de forma que compruebe las actualizaciones diariamente.

MBSA

Otra herramienta que nos permitirá mantener nuestro sistema al día es Microsoft Baseline Security Analizer (*MBSA*), un software de Microsoft que nos comprobará el sistema de forma parecida a Windows Update. La diferencia entre *Windows Update* y *MBSA* es que el primero nos ofrece más actualizaciones que el segundo, ya que también nos da la posibilidad de instalar nuevo software, mientras que *MBSA* se preocupa solamente de las actualizaciones de seguridad

MBSA nos ofrece las siguientes características:

- Nos permitirá buscar vulnerabilidades en las siguientes aplicaciones: Windows (NT, 2000, XP y 2003), Internet Explorer, Microsoft Office, Windows Media Player, MDAC, la máquina virtual Java y otras aplicaciones (más orientadas a servidores)

- Comprueba la configuración y activación del Internet Connection Firewall.

- Comprueba que la configuración de las zonas de Internet Explorer sea correcta

- Comprueba que las actualizaciones automáticas estén activadas

- Detecta servicios innecesarios que tengamos activados (por defecto FTP, Telnet, WWW y SMTP)

- Detecta contraseñas vacías o muy sencillas de adivinar

Para instalar este programa, debemos acudir a la página del programa y descargarlo desde allí (solo existen versiones en inglés, francés, alemán y japonés). Una vez instalado *MBSA* le indicaremos que escanee nuestro sistema y este nos indicará todas las posibles vulnerabilidades que haya encontrado, su importancia y la forma de solucionarlo. Para indicar la importancia de cada una de las vulnerabilidades lo hará a través de una serie de iconos que nos indicará en que grado puede afectar al sistema:

En *Security Update Scan Results*:

 indica que falta una actualización crítica

 indicación no crítica, por ejemplo que el Service Pack instalado no es el último

 aviso, suele indicar que no se ha podido confirmar si una actualización está instalada

En *Windows Scan Results*:

 indica un error de configuración grave

 indica un error no crítico (por ejemplo, una contraseña que no expira nunca)

 indica que la comprobación ha sido correcta

 nos da una indicación de una buena práctica que deberíamos utilizar

 nos da información sobre la máquina como el sistema operativo instalado

Actualizaciones del resto de programas

Además de mantener actualizado nuestro sistema operativo es importante, también, que actualicemos el resto de programas que estén instalados en nuestro ordenador, especialmente los que necesiten acceder a la red para funcionar (por ejemplo, el lector de correo o el programa de mensajería instantánea).

Para saber como actualizar estos programas deberemos revisar la documentación de cada uno de ellos y comprobar como hacerlo. La forma habitual, si el programa no lleva ya una opción incluida para actualizarse automáticamente, es visitar la página del fabricante y comprobar si existen nuevas versiones. Si existen, deberemos ver si hay algún requisito previo a su instalación (frecuentemente, es necesario desinstalar la versión anterior para poder instalar la nueva o tendremos que hacer copias de seguridad de los datos anteriores).

Muchos programas disponen de listas de correo donde se avisa de la aparición de nuevas versiones o actualizaciones. Es aconsejable estar suscrito en estas listas, cuando existan, puesto que es la manera más rápida de saber cuando debemos actualizarnos.

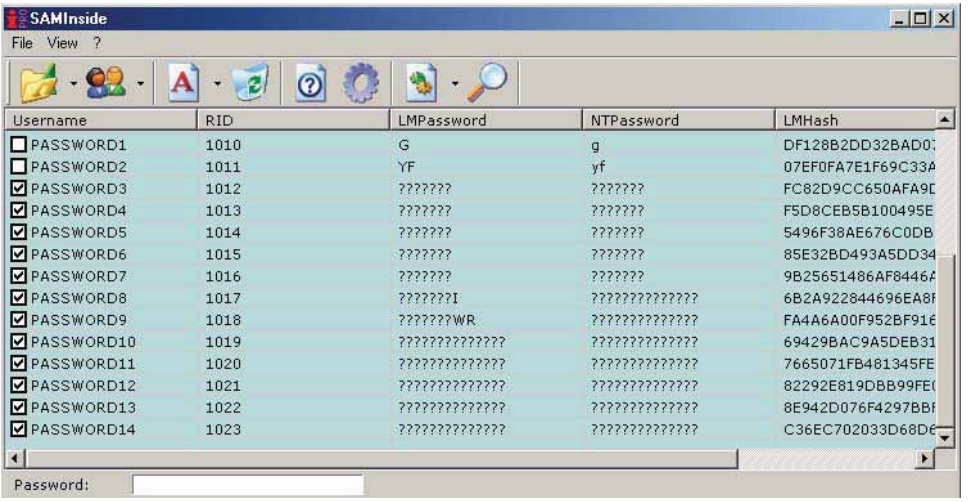
Contraseñas

En la mayoría de los casos, la autenticación en los ordenadores (es decir, demostrar quien somos ante el ordenador para poder acceder a algún recurso) se hace a través de contraseñas. Esto es bastante peligroso, ya que mucha gente no conoce el método para escoger una buena contraseña y, aunque lo conozca, la mayoría de personas no son capaces de recordar una contraseña que sea lo suficientemente segura.

Un buen sistema de autenticación debe basarse en combinaciones de varios factores a la vez: algo que sabemos, algo que tenemos, algo que somos,... Por ejemplo, para identificarnos en un cajero automático utilizamos dos factores: algo que tenemos (la tarjeta de crédito) y algo que sabemos (el número secreto o PIN). En el caso de las contraseñas, solo estamos utilizando uno de los factores, algo que sabemos, por lo que este debe ser lo más seguro posible.

Como podemos saber si una contraseña es segura? En primer lugar, debemos saber cuál es la longitud mínima que debe tener para ser segura. Para ello, veamos un ejemplo práctico.

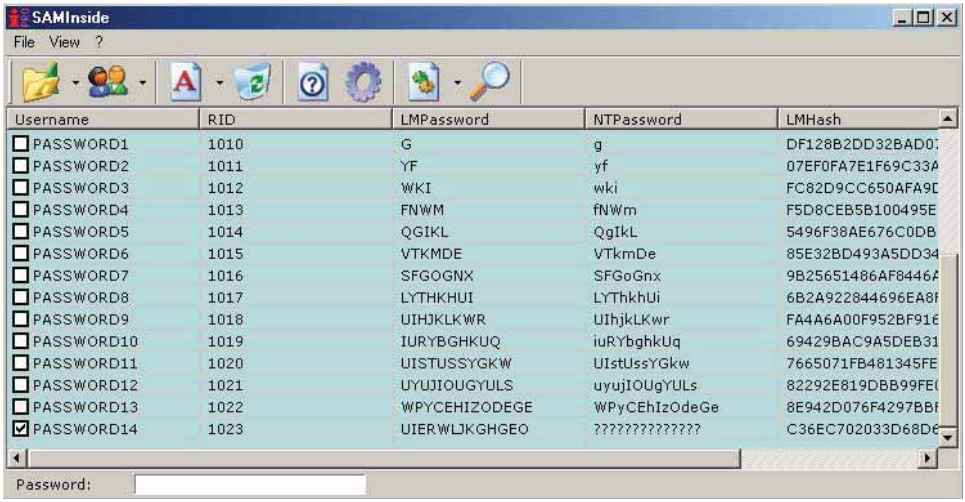
Hemos creado un total de 14 usuarios en nuestro sistema (con nombre PASSWORDx, donde la x corresponde a la longitud de la contraseña), cada uno de ellos con una clave aleatoria formada por letras mayúsculas y minúsculas. Para encontrar las contraseñas usaremos el programa SamInside en su versión de demostración.



Vemos que al cargar el programa, este directamente ha encontrado dos de las contraseñas, la de longitud uno y la de longitud dos. Si ponemos a trabajar al programa podemos ver cuanto tarda en encontrar el resto.

Longitud	***Tiempo***
1,2	Automático
3,4,5,6	< 1:00
10	17:37
13	19:23
14	22:42
9	24:12
11	40:05
8, 12	43:45
7	50:22

Vemos que las contraseñas de longitud menor que 7 son encontradas casi instantáneamente, mientras en el resto hay variación entre ellos sin ajustarse a un orden lógico creciente. Esto es debido a que, por defecto, Windows 2000 guarda las contraseñas en dos partes, cada una de ellas de longitud 7 y con todas las letras en mayúsculas, por lo que utilizar passwords de entre 7 y 14 caracteres no aumenta la seguridad (esto solo ocurre en este tipo de sistema, la seguridad del resto de contraseñas si que mejora si aumentamos la longitud)



Hemos podido comprobar que con un simple ordenador de escritorio podemos encontrar cualquier contraseña de longitud 7 en menos de una hora, siempre que esta sólo utilice letras.

Veamos una serie de reglas a seguir para conseguir contraseñas más seguras:

- Utilizar la contraseña más larga posible (como mínimo de longitud 8). Windows acepta contraseñas de hasta 128 caracteres, lo que deja espacio a la creatividad. No utilizar NUNCA contraseñas de 6 letras o menos.
- Mezclar letras mayúsculas y minúsculas, números, signos de puntuación (puntos, comas, paréntesis,...). Como más signos diferentes se utilicen más difícil será descubrirla..
- No incluir información personal o que pueda relacionarse con nosotros en la contraseña. No usar fechas de cumpleaños, números de teléfono, direcciones,... pues son fácilmente adivinables.
- No hacer público nuestra contraseña bajo ningún concepto. Nunca debemos apuntarla en un papel, ni en un post-it, ni en un fichero que guardemos en el disco.
- No utilizar la misma contraseña en dos sistemas diferentes. Debemos tener contraseñas distintas en cada sitio. Si no cumplimos esta regla y alguien descubre nuestra contraseña podrá utilizarla múltiples veces en diferentes sistemas.
- Cambiar la contraseña regularmente, por ejemplo cada dos o tres meses, de forma que si alguien está intentando encontrarla por fuerza bruta, cuando lo encuentre, ya no le sirva puesto que lo habremos cambiado.

Cómo escogemos nuestra contraseña para que cumpla estas reglas? Dependiendo del sistema donde estemos trabajando podemos escoger dos opciones:

- En Windows está permitido el uso de espacios en las contraseñas, de manera que podemos utilizar frases; una sentencia como: “Yo y mi ontraseña (6756276) no tenemos ninguna relacion!!! - Es una buena opcion” cumple la mayoría de las propiedades que debe tener una buena contraseña.

- En el resto de sistemas que o bien no aceptan espacios o bien no aceptan contraseñas de longitud mayor de 14 caracteres podemos escoger una frase un poco larga y coger la primera letra de cada palabra. P.ej.:

  Todos los passwords que utilizo son seguros al 100 por 100.

  Cogemos la primera letra de cada palabra:

  T L P Q U S S A 1 P 1

  Ahora, mezclamos mayúsculas con minúsculas:

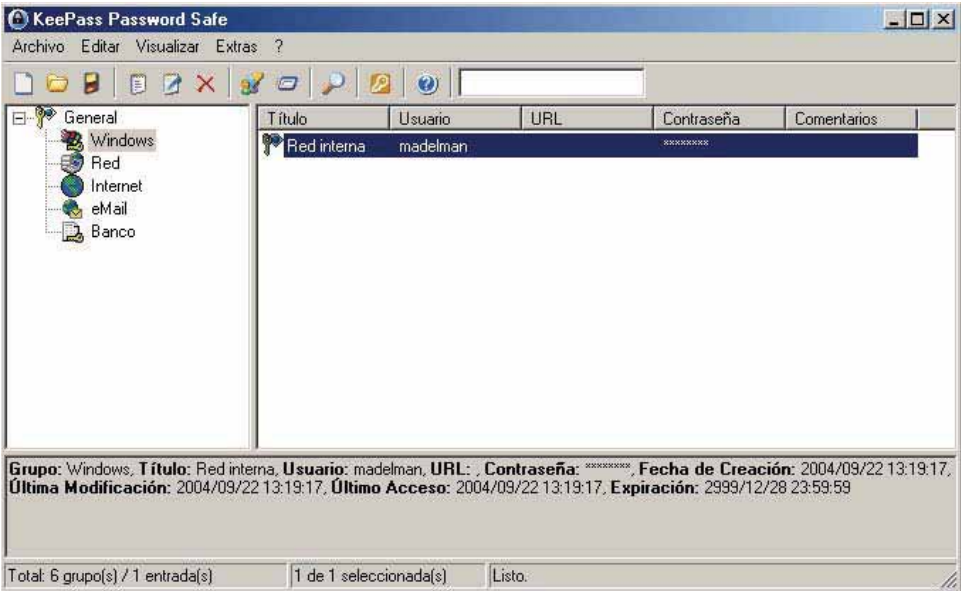
  TlpQusSa1p1

  Con esto conseguiremos una buena contraseña que será fácil de recordar.

Cumplir todas estas normas acostumbra a ser una tarea complicada para cualquiera, especialmente si necesitamos tener multitud de contraseñas diferentes. Por ello, es aconsejable el uso de un *Password Wallet*. Este tipo de programas nos permiten almacenar todas nuestras contraseñas con su nombre de usuario asociado en un solo sitio, de forma que siempre estén disponibles y no tengamos que recordarlas todas. El nombre *Password Wallet* se refiere al hecho que viene a ser como un papel que llevamos en nuestra cartera con todas las contraseñas apuntadas (cosa que evidentemente no debemos

hacer nunca), pero en este caso el programa protegerá el resto de nuestras contraseñas con una contraseña maestra que nos dará acceso a las demás. Habitualmente, estos programas disponen también de un generador de contraseñas, de forma que no debamos preocuparnos nosotros de generar una contraseña segura.

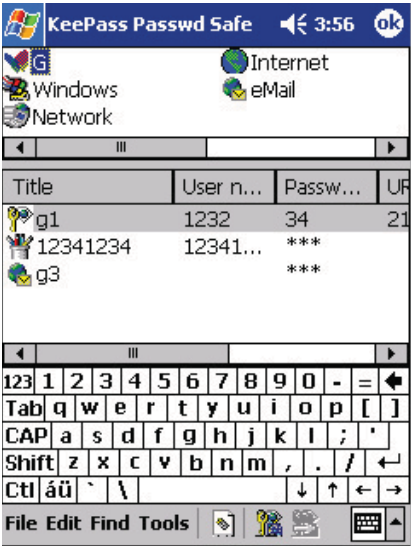
Un *Password Wallet* bastante interesante (además de ser gratuito y de código abierto) es *KeePass Password Safe*.



Este programa nos permite guardar todas nuestras contraseñas en un solo fichero que se almacenará cifrado con una clave maestra. Solo introduciendo esta clave seremos capaces de recuperar el resto de contraseñas, por lo que es muy importante que la clave maestra sea muy segura. El propio programa nos ofrece la posibilidad de generar la clave por nosotros, asegurándose de que tenga longitud suficiente; igualmente también puede generar el resto de contraseñas que vayamos a almacenar en el programa.

Otra posibilidad que nos ofrece *KeePass* es el uso de un disco llave para proteger nuestras contraseñas. De este modo ni tan siquiera necesitaremos recordar la clave maestra, sino que los datos se cifraran con una clave que estará almacenada en un soporte externo (un disco, un CD-ROM,...). No debemos guardar la base de datos en el mismo soporte en el que guardemos el disco llave, ya que entonces la protección sería nula, sino que debemos tenerlos en soportes separados y llevar siempre el disco llave con nosotros.

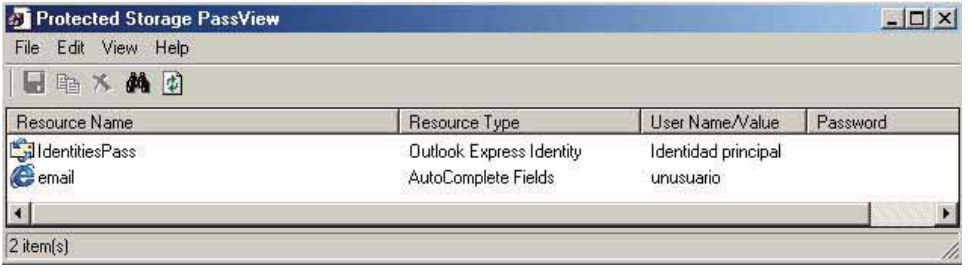
Existe también una versión para *PocketPC* de *KeePass*, que nos permite almacenar todas nuestras contraseñas en nuestra PDA y poder llevarlas siempre con nosotros.



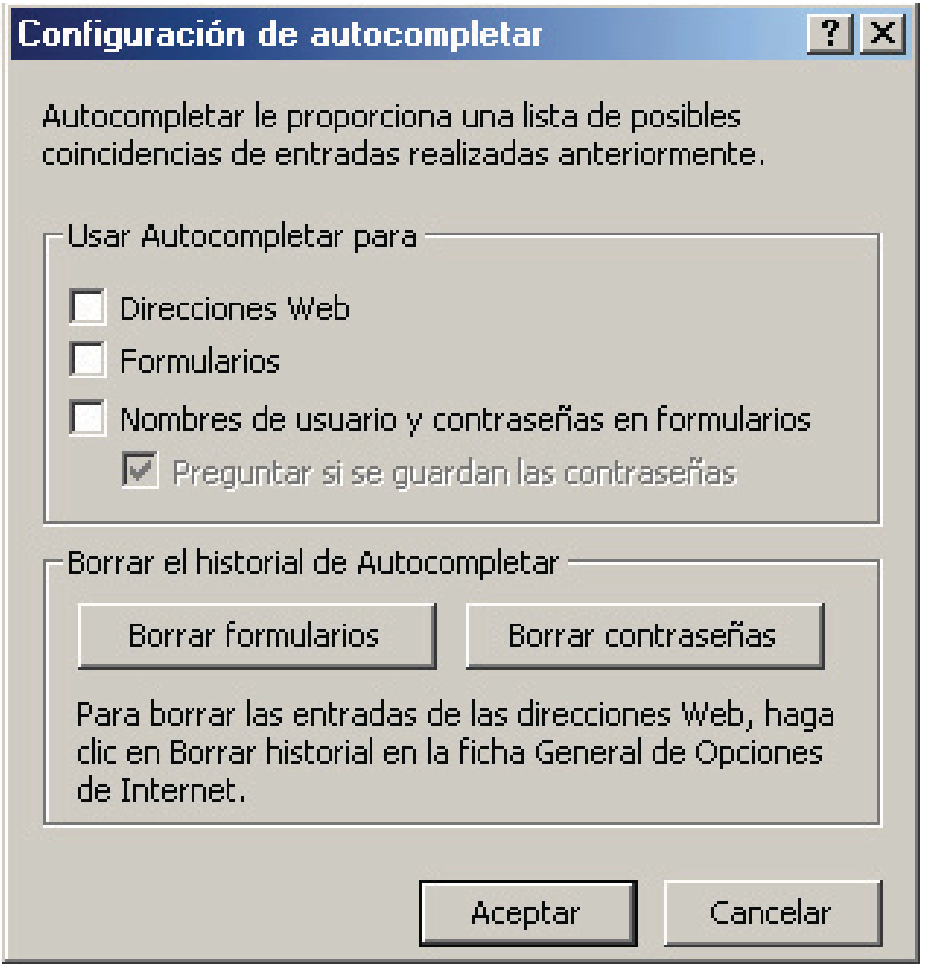
Como no recordar las contraseñas

La mayoría de navegadores incluyen una función para recordar las contraseñas de los diferentes sitios que visitamos. Usar esta funcionalidad ayuda a no tener que usar la misma contraseña para cada sitio que visitemos, evitando tener recordar cientos de contraseñas diferentes. Pero esto comporta un serio problema, si el navegador es capaz de enviar nuestras contraseñas sin que nosotros tengamos que indicarle nada, porque no pueden hacerlo el resto de programas?

Existen algunas aplicaciones que permiten mostrar las contraseñas almacenadas por nuestro navegador, como Protected Storage PassView, que muestra las de Internet Explorer y las de cliente de correo Outlook Express.



En Internet Explorer, la opción de recordar nombres de usuario y contraseñas es conocida como Autocompletar y podemos encontrarla dentro del menú Herramientas -> Opciones de Internet en la pestaña Contenido. Si queremos borrar las que ya tenemos almacenadas podemos entrar en ese menú y pulsar sobre Borrar formularios y Borrar contraseñas. Posteriormente, desactivaremos todas las opciones que nos ofrece Autocompletar, de forma que no se almacene nada que nosotros no queramos.


Configuración de autocompletar
Autocompletar le proporciona una lista de posibles coincidencias de entradas realizadas anteriormente.
Usar Autocompletar para
Direcciones Web
Formularios
Nombres de usuario y contraseñas en formularios
Preguntar si se guardan las contraseñas
Borrar el historial de Autocompletar
Borrar formularios
Borrar contraseñas
Para borrar las entradas de las direcciones Web, haga clic en Borrar historial en la ficha General de Opciones de Internet.
Aceptar
Cancelar

Virus

La característica básica de un virus informático es la capacidad de crear copias de si mismo y replicarse en otros ordenadores. Además de ello, algunos virus son malignos y además de rutinas para reproducirse incorporan otras para destrucción de datos. Los virus no solamente afectan a los ficheros ejecutables (los típicos .exe) sino que pueden estar contenidos en cualquier tipo de fichero que contenga código que vaya a ser interpretado. Un ejemplo son los ficheros del programa Microsoft Office, en cuyo interior puede haber macros, trozos de código que Office ejecuta; estas macros pueden contener virus y infectar otros archivos, por lo que debemos tener cuidado con ficheros de cualquier tipo y no solo ejecutables corrientes.

Aunque anteriormente los virus viajaban de un ordenador a otro a través de disquetes, hoy en día la forma más habitual de reproducción de estos es a través del correo electrónico. Muchos virus disponen de la capacidad de buscar direcciones de correo dentro de nuestro ordenador (no solamente en la agenda de nuestro programa de correo, sino en cualquier fichero del disco duro) y de enviarse automáticamente a esas direcciones.

Debemos tener una especial precacución para evitar ser infectados por un virus a través del correo electrónico, por lo que nunca debemos abrir un fichero que hayamos recibido, aunque el remitente sea de confianza. En primer lugar deberemos asegurarnos que el fichero ha sido realmente enviado por el remitente; en este caso puede ser muy útil una simple llamada de teléfono para confirmarlo. En caso de que no sea posible ponerse en contacto con el remitente, nunca debemos abrir directamente el fichero desde el programa de correo. Para asegurarnos de la inocuidad de este, lo guardaremos primero en el disco y lo escanearemos con un programa antivirus para asegurarnos

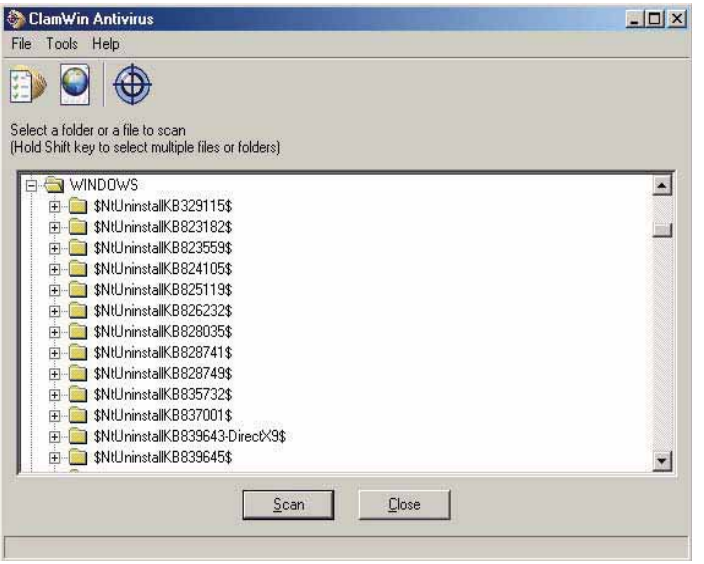
que no está infectado. Una vez lo hayamos comprobado, podemos abrir el fichero sin temor a que un virus entre en nuestro ordenador.

De todas formas, no debemos confiarnos nunca, puesto que los virus no solo nos van a llegar por correo electrónico. Actualmente, hay múltiples maneras de recibir uno: a través de programas de compartición de ficheros (Kazaa, eMule,...), bajados de la web, en disquete o CD-ROM, a través de programas de mensajería instantánea (MSN Messenger, Yahoo Messenger,...) por lo que debemos comprobar todos los ficheros que lleguen a nuestro ordenador.

Qué antivirus utilizar?

Podemos escoger entre una gran variedad de antivirus, algunos de pago y otros gratuitos. Cuando seleccionemos el antivirus que queremos instalar debemos tener en cuenta varios factores, como el hecho de que esté mantenido, es decir, que haya gente trabajando en él y de que las actualizaciones de sus bases de datos de virus sean frecuentes, pues de nada nos servirá un antivirus que no pueda detectar los nuevos especímenes que vayan apareciendo.

Podemos ver una pequeña comparativa de tiempo de reacción de varios antivirus en Hispasec, en la cual *ClamWin* sale vencedor, seguido por F-Prot.



ClamWin es una implementación para Windows de *ClamAV*, un antivirus gratuito y de código abierto; permite el escaneo de ficheros de nuestro disco y la actualización automática de las bases de datos de virus, además de poderse integrar con el explorador de Windows para poder escanear ficheros desde el menú contextual. Su uso es muy sencillo, y solo debemos seleccionar el directorio o fichero que queremos escanear y pulsar *Scan* para que el programa realice su tarea.

El único inconveniente de *ClamWin* es que no es capaz de escanear los ficheros cuando accedemos a ellos, sino que tenemos que indicarle expresamente que queremos escanearlos. Esta funcionalidad puede ser muy útil, evitando que los virus lleguen a grabarse en nuestro disco. Si queremos un antivirus que implemente esto, *Grisoft* ofrece una versión gratuita de su antivirus *AVG* que implementa esta protección en tiempo real.

Finalmente, para las ocasiones en las que no dispongamos de un antivirus a mano, no podamos instalar programas en un ordenador o deseemos asegurarnos realmente que un programa no está infectado, en la página de VirusTotal (http://www.virustotal.com) nos ofrecen la posibilidad de enviar un fichero, que será escaneado mediante varios antivirus y nos mostrará el resultado de esos análisis.

Dialers

Un tipo especialmente deleznable de software que se puede instalar en nuestro ordenador son los programas conocidos como *dialers*. Estas aplicaciones intentan apoderarse de nuestra conexión a Internet, cambiando el número de teléfono al que llamamos para acceder a la red por un número con tarificación especial (un 803 o 806). De esta forma estaremos gastando mucho más dinero cuando estemos conectados, dinero que irá a parar a los bolsillos de quien controla ese número.

Estas aplicaciones suelen aparecer cuando en alguna página se nos ofrece algún "recurso gratuito", bien puede ser imágenes, programas, MP3s, etc... Para conseguir este recurso se nos pedirá que instalemos una aplicación y dispondremos de acceso a los ficheros. Esta aplicación será la que nos modificará el acceso telefónico. A veces, estos dialers pueden llegar a instalarse automáticamente en nuestro ordenador aprovechando vulnerabilidades del navegador.

Estos *dialers* solo funcionan con los usuarios que se conectan a Internet a través de un módem, por lo que si nos conectamos a través de ADSL o cable no tendremos problemas (aunque debemos vigilar igual, ya que si se instalan cabe la posibilidad de que activemos sin darnos cuenta la conexión a través del modem).

Afortunadamente, en España, el 21 de julio de 2004 se publicó una Orden del Ministerio de la Presidencia de forma que para poder conectarnos a través de uno de estos números de teléfono debemos darnos de alta previamente, por lo que poco a poco este tipo de programas tenderá a desaparecer, aunque siempre podemos encontrarnos alguno que utilice números de otro país.

Podemos comprobar si tenemos instalado algún dialer examinando las conexiones de acceso telefónico que tenemos instaladas y asegurándonos que el teléfono indicado corresponde al de nuestro ISP.

Para evitar que nos afecten los dialers podemos instalar Custodio Net que nos protege de conexiones telefónicas no deseadas.

Si tenemos instalado el sistema operativo Windows XP también podemos evitar que se añadan nuevas conexiones haciendo que el fichero `c:\Documents and Settings\All Users\Datos de programa\Microsoft\Network\Connections\Pbk\rashphone.pbk` sea de sólo lectura.

Con esto evitaremos que nos lleguen unas facturas telefónicas muy abultadas (al menos, las debidas a los dialers)

Spyware

El *spyware* es cualquier tipo de programa que registra alguna actividad en nuestro ordenador para después enviarla sin nuestro consentimiento. La actividad registrada puede ser de cualquier tipo: las páginas por las que navegamos, los teclas que pulsamos,...

Dentro del *spyware*, uno de los tipos menos peligrosos pero más molestos es el conocido como *adware*, el cual nos muestra ventanas con publicidad, normalmente relacionada con aquellas páginas que estamos visitando. Otros tipos de *spyware* son mucho más peligrosos, ya que pueden capturar nuestras contraseñas, nuestras cuentas bancarias,... y transmitirlas posteriormente a quien controle ese programa.

Como entra el spyware en nuestro ordenador

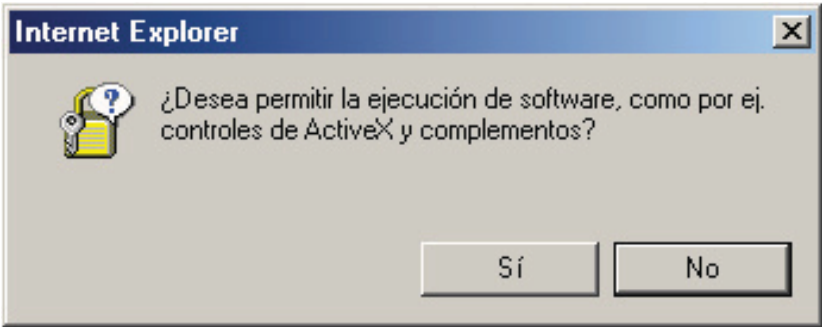
Estos programas pueden entrar de diversas formas a nuestro ordenador. Las más comunes son acompañando a algún programa que instalemos o bien a través de nuestro navegador si este no es lo suficientemente seguro.

Existen multitud de programas que llevan incorporado algún tipo de *spyware*. Por ejemplo, muchas de las aplicaciones de compartición de ficheros (como muchas de la versiones de *Kazaa*) llevan incorporados módulos que nos muestran publicidad, no solo dentro del programa sino también en ventanas externas cuando el programa no está funcionando. Estos módulos son a veces opcionales y piden permiso para ser instalados, pero otras veces se instalan automáticamente en nuestro sistema sin que nos demos cuenta. Es importante cuando instalemos algún programa en nuestro ordenador comprobar las opciones que seleccionamos para la instalación y asegurarnos que se

instala solamente aquello que nos interesa y no otros programas adicionales; para ello, es recomendable leerse las licencias que incorporan estos y ver si en alguna de las clausulas nos indica todo lo que se va a instalar en nuestro ordenador.

Otra forma que tiene el *spyware* para entrar en nuestro navegador es a través del navegador. Podemos ver un ejemplo en http://www.freescratchandwin.com (se recomienda no entrar en esta página bajo ningún concepto). En la página nos ofrecen la posibilidad de jugar a una especie de lotería que nos permitirá ganar dinero y, para ello, nos piden que nos instalemos una pequeña utilidad para poder jugar.

Si entramos en la página de *Download now* y, dependiendo de la configuración de nuestro navegador, se instalará el programa o nos aparecerá una ventana pidiendo permiso para instalarlo.



Si damos permiso para instalar el programa, este se descargará en nuestro ordenador y nos instalará diversos ficheros que modificarán el comportamiento de nuestro ordenador. A partir de ese momento, la página de inicio de nuestro navegador se modificará para apuntar a http://www.xzoomy.com (no entrar en esta página) y periódicamente se abrirán ventanas en nuestro escritorio mostrándonos publicidad.

Podemos ver que estas ventanas se muestran sin barra de título, de forma que sea más difícil cerrarlas (podemos hacerlo pulsando simultaneamente las teclas ALT y F4), además de mostrarse repetidas veces si no las vamos cerrando, de forma que podemos acabar con el escritorio lleno de ventanas que no nos dejan trabajar con normalidad en nuestro ordenador.

Como librarnos del spyware

Existen dos aplicaciones básicas para librarnos de este tipo de programas: *Ad-aware* y *Spybot*.

Ad-aware

Este programa nos permite eliminar de nuestro ordenador multitud de parásitos, tanto *spyware* como *dialers*, troyanos,... Una vez descargado e instalado el programa debemos comprobar si existen actualizaciones de su base de datos, cosa que podemos hacer desde el mismo programa con la opción *Check for updates now*. Una vez actualizados los ficheros necesarios, procedemos a comprobar nuestro sistema y *Ad-aware* buscará rastros de ficheros sospechosos en nuestro disco.

Una vez se haya acabado el análisis de nuestro sistema, podemos seleccionar todo lo que queremos borrar y *Ad-aware* lo borrará dejando nuestro ordenador limpio de *spyware*.

Referencias

Dirección de Windows Update
http://windowsupdate.microsoft.com

Dirección de descarga de MBSA
http://www.microsoft.com/spain/technet/seguridad/herramientas/mbsa.asp

Por qué es conveniente usar frases como contraseñas
http://blogs.msdn.com/robert_hensing/archive/2004/07/28/199610.aspx

Artículo acerca de los dialers
http://www.noticiasdot.com/publicaciones/2004/0704/2207/noticias220704/noticias220704-8.htm

Dirección de descarga de Sam Inside
http://www.insidepro.com/eng/saminside.shtml

Dirección de descarga de KeePass Password Safe
http://keepass.sourceforge.net/

Dirección de descarga de KeePass for Pocket PC
http://doncho.net/kppc/index.php

Dirección de descarga de Protected Storage PassView
http://www.nirsoft.net/utils/pspv.html

Comparativa de tiempos de respuesta ante nuevos virus
http://www.hispasec.com/unaaldia/2115

Dirección de descarga de ClamWin
http://www.clamwin.com

Dirección de descarga de la versión gratuita de AVG
http://free.grisoft.com/freeweb.php/doc/2/

Dirección de descarga de Custodio Net
http://www.seguridadenlared.org/es/index24esp.html

Dirección de descarga de Ad-Aware
http://www.lavasoftusa.com/default.shtml.es

Dirección de descarga de Spybot
http://www.safer-networking.org/es/index.html

[Capítulo 2]

TCP/IP

Arquitectura de TCP/IP

Al navegar por Internet estamos utilizando, probablemente sin darnos cuenta, toda una serie de protocolos que funcionan mediante una arquitectura de capas, es decir, cada capa de esta serie de protocolos utiliza el protocolo que está situado por debajo para recibir y transmitir los datos. El protocolo de nivel más bajo es el encargado de enviar los datos al destinatario (normalmente, a través de un medio físico como un cable). Cuando estos datos llegan al destino este mismo protocolo los leerá y los pasará a los niveles superiores para que puedan tratarlos.

La arquitectura por capas utilizada más habitualmente en Internet es:

Aplicación
TCP
IP
Red física

- *Aplicación:* Formada por los programas que utilizamos para realizar tareas a través de Internet (navegador, lector de correo,...)
- *TCP / IP*: Son los protocolos en que se basa Internet.
- *Red física*: El medio físico a través del cual se transmiten los datos, p. ej. la línea telefónica, el cable,...

Para poder conectarse a esta red es necesaria una dirección IP, una serie de números en formato xx.xx.xx.xx, que identifica a cada ordenador conectado. Cada uno de estos números puede ir de 0 a 255. Además, cada ordenador dispone de una serie de puertos, numerados del 1 al 65535, que le permiten comunicarse con el resto de sistemas.

Así, para identificar una determinada conexión necesitaremos saber las direcciones IP de los dos ordenadores y los puertos que están utilizando. Así, por ejemplo, una conexión de un ordenador a un servidor de páginas web podría identificarse por

IP origen: 192.168.0.5
Puerto origen: 3127
IP destino: 192.168.0.23
Puerto destino: 80

Muchos de estos puertos están designados para ser utilizados por un determinado tipo de aplicación, p.ej. el puerto 80 es utilizado por los servidores de paginas web, el puerto 25 por los servidores de envío de correo,... Habitualmente, el sistema operativo mantiene una lista de los servicios asignados a cada puerto. En Windows 2000 o XP podemos encontrarla en `c:\WINDOWS\SYSTEM32\DRIVERS\etc\services`

Si queremos saber que puertos están en uso actualmente en nuestro ordenador existen diversas formas de hacerlo. La más sencilla es utilizando, desde la linea de comandos, la instrucción *netstat*. Esto nos mostrará la lista de conexiones que hemos activado desde nuestro ordenador.

```
C:\>netstat -n

Conexiones activas

Proto  Dirección local   Dirección remota  Estado
TCP    192.168.0.4:3632  62.193.199.204:80 ESTABLISHED
TCP    192.168.0.4:3748  207.46.107.85:163 ESTABLISHED
```

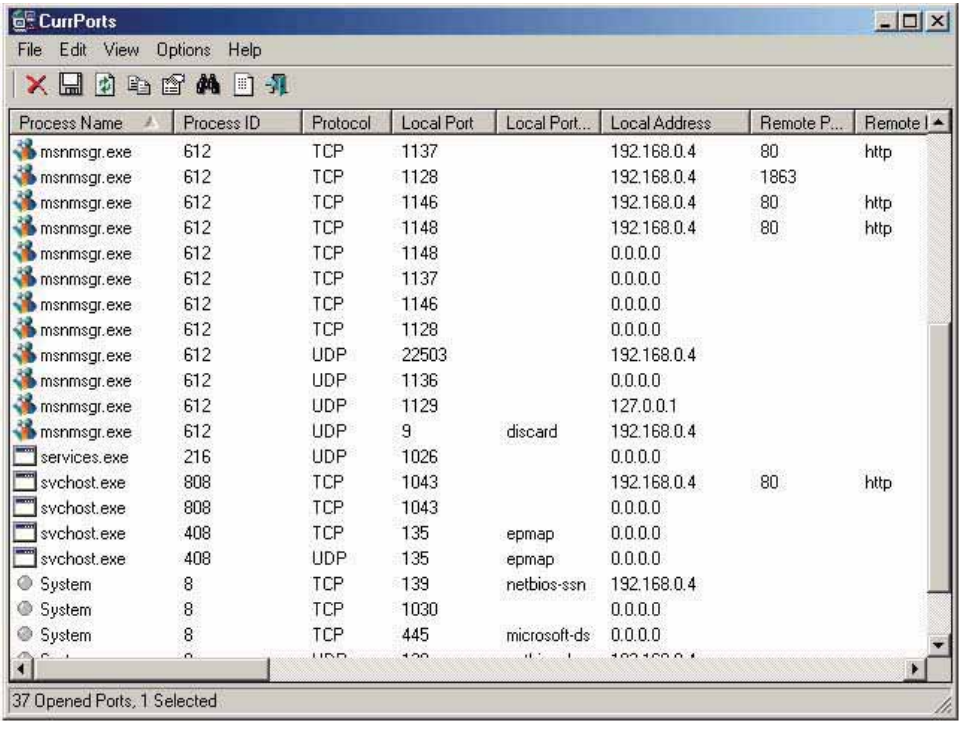
Si queremos ver la lista con todas las conexiones, incluidas las que están en escucha podemos utilizar el parametro -a

```
C:\>netstat -a

Conexiones activas

Proto  Dirección local   Dirección remota    Estado
  TCP    0.0.0.0:135     0.0.0.0:0           LISTENING
  TCP    0.0.0.0:445     0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1025    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1030    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1043    0.0.0.0:0           LISTENING
  TCP    0.0.0.0:1128    0.0.0.0:0           LISTENING
  ...
```

Nos interesan especialmente los puertos que están a la escucha (LISTENING), pues pueden ser un signo indicativo de que tenemos algún programa no autorizado en ese puerto. Además, si no están bien protegidos pueden ser un lugar de entrada para intrusos a nuestro ordenador.

Si queremos ver que aplicación es la que está usando cada uno de estos puertos, podemos utilizar el programa CurrPorts. Este nos mostrará de forma gráfica el uso de los puertos. De esta manera podremos saber si hay algún programa que no debería estar utilizando ningún puerto y lo está haciendo. Debemos tener especial cuidado y comprobar que no haya programas desconocidos en esta lista.

Para protegernos de posibles atacantes que intenten entrar en nuestro ordenador debemos utilizar un software como *cortafuegos* (*firewall*, en inglés). El *cortafuegos* es una aplicación que monitoriza el tráfico de red que entra y sale de nuestro ordenador y actúa sobre él, según una serie de reglas predefinidas. Por ejemplo, podemos indicarle que no deje pasar tráfico de red hacia nuestro ordenador o impedir que un determinado programa envíe datos hacia Internet.



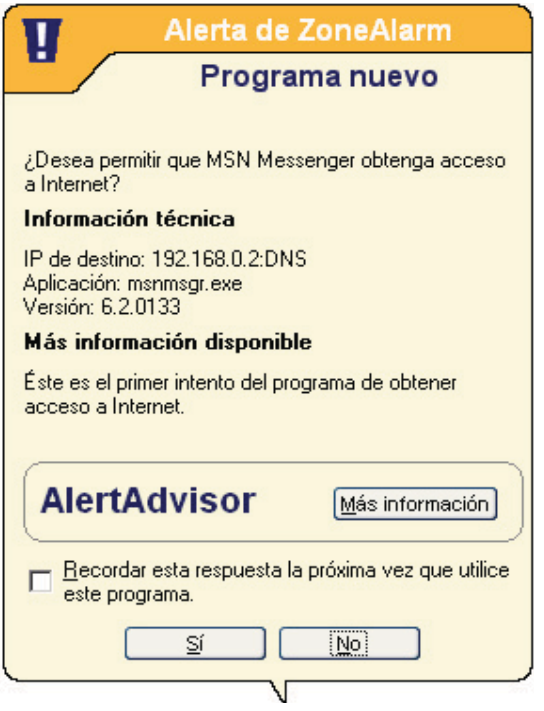
De esta manera, aunque tengamos un determinado puerto abierto, no se podrá acceder a él desde fuera de nuestro ordenador, ya que el *cortafuegos* impedirá el acceso. También podemos impedir que aplicaciones que no deberían hacerlo envíen datos sobre nuestro ordenador, como hacen algunos programas, que envían registros de las páginas web a las que accedemos o incluso registros de las teclas pulsadas en nuestro ordenador.

Existen diversos programas que implementan esta funcionalidad. Windows XP lleva incluido un *cortafuegos*, pero es bastante limitado y no dispone de algunas de las opciones avanzadas de las que disponen otros como Zone Alarm o Kerio Personal Firewall.

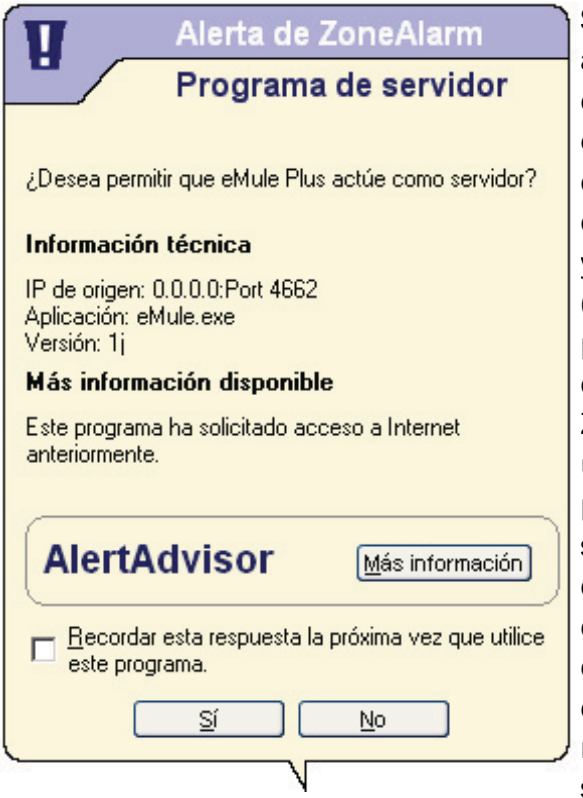
Zone Alarm

Zone Alarm es un cortafuegos gratuito que nos permite un buen control sobre el acceso a la red de nuestro ordenador. Una vez instalado quedará residente en la barra de tareas monitorizando la actividad de la red y avisándonos cuando se produzca un intento de acceder a nuestro ordenador o cuando se envíe información hacia la red.

Cuando Zone Alarm detecta que un programa intenta enviar información a través de la red nos mostrará una ventana como esta, en la que nos pedirá información sobre que acción tomar. Debemos tener especial atención con esta ventana para no dar permiso a alguna aplicación que no debería tenerlo. Para ello debemos comprobar que el nombre del programa que se nos muestra es conocido (p.ej. en este caso *MSN Messenger*) y, en ese caso, asegurarnos de que el programa necesita realmente acceder a la red. En el caso de *MSN Messenger* la respuesta es afirmativa en los dos casos por lo que podemos darle permiso para acceder a la red. Si no queremos que Zone Alarm nos vuelva a preguntar por los permisos de este programa deberemos marcar la opción de *Recordar esta*



respuesta. En caso de que no estemos seguro si debemos dar permiso a un programa podemos negarselo inicialmente y comprobar si todo funciona correctamente, en caso contrario, cuando nos vuelva a preguntar podemos permitir el acceso. Siempre podemos utilizar la opción *Más información* si no estamos seguros, donde se nos mostrará más información sobre las acciones a realizar.



Si un programa quiere actuar como servidor, es decir, ponerse a la escucha en nuestro ordenador para que otros ordenadores se conecten y poder recibir información (es el caso de algunos programas de compartición de ficheros), Zone Alarm nos mostrará una ventana como esta, pidiéndonos información sobre como actuar. Igual que en el caso anterior, debemos asegurarnos que conocemos el programa y que realmente este necesita actuar como servidor, antes de darle permiso para hacerlo. Ante la duda podemos utilizar la opción de *Más información*.

Kerio Personal Firewall

Este cortafuegos (en adelante KPF) ofrece una serie de opciones interesantes para usuarios avanzados, a costa de una menor facilidad de uso, además de no disponer de una versión en castellano.
Al igual que Zone Alarm, KPF detecta cuando una aplicación intenta enviar datos hacia la red y nos avisa de ello, debiendo tomar nosotros la decisión de permitirle o no hacerlo.

Algunas aplicaciones, para poder saltarse las protecciones impuestas por el cortafuegos, intentan ejecutar otros programas que si estén autorizados a comunicarse a través de la red. KPF permite detectar cuando un programa intenta ejecutar otros y nos pedirá confirmación para darle permiso para hacerlo. Esta es una opción de la que otros cortafuegos no disponen y que puede ser muy útil para evitar fugas de información.

KPF también permite comprobar que los ficheros que intentemos ejecutar no han sido modificados, de forma que estemos seguros de que el fichero es el que nosotros pretendemos ejecutar y no ha sido reemplazado por otro. Esto puede servirnos, además, como alerta ante un virus, pues podremos detectar si el virus ha modificado alguno de nuestros ficheros.

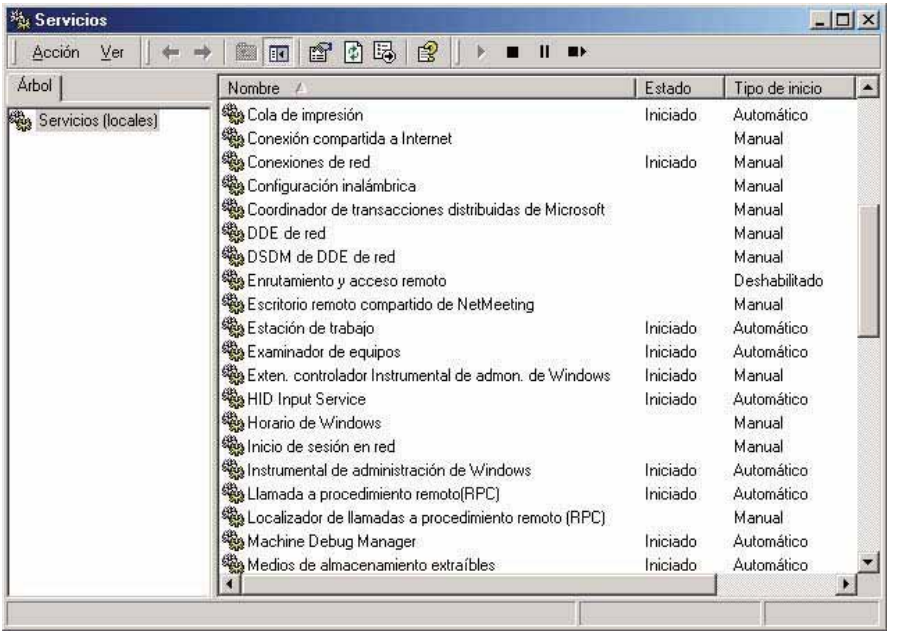
Finalmente, KPF nos ofrece también otra serie de opciones como la posibilidad de detectar ataques externos, la creación de zonas de confianza personalizadas y, en su versión avanzada el bloqueo de publicidad y ventanas emergentes en nuestro navegador.

Servicios

Los servicios son programas que se ejecutan al iniciar el ordenador, antes de que el usuario entre en el sistema. Normalmente, ofrecen alguna funcionalidad del sistema operativo al usuario o proveen acceso desde la red a algún programa, p.ej. un servidor de bases de datos.

Debemos tener controlados los servicios que se están ejecutando en nuestro ordenador, de modo que no malgastemos recursos con algo que no necesitamos u ofrezcamos acceso desde la red a nuestro ordenador sin la protección adecuada.

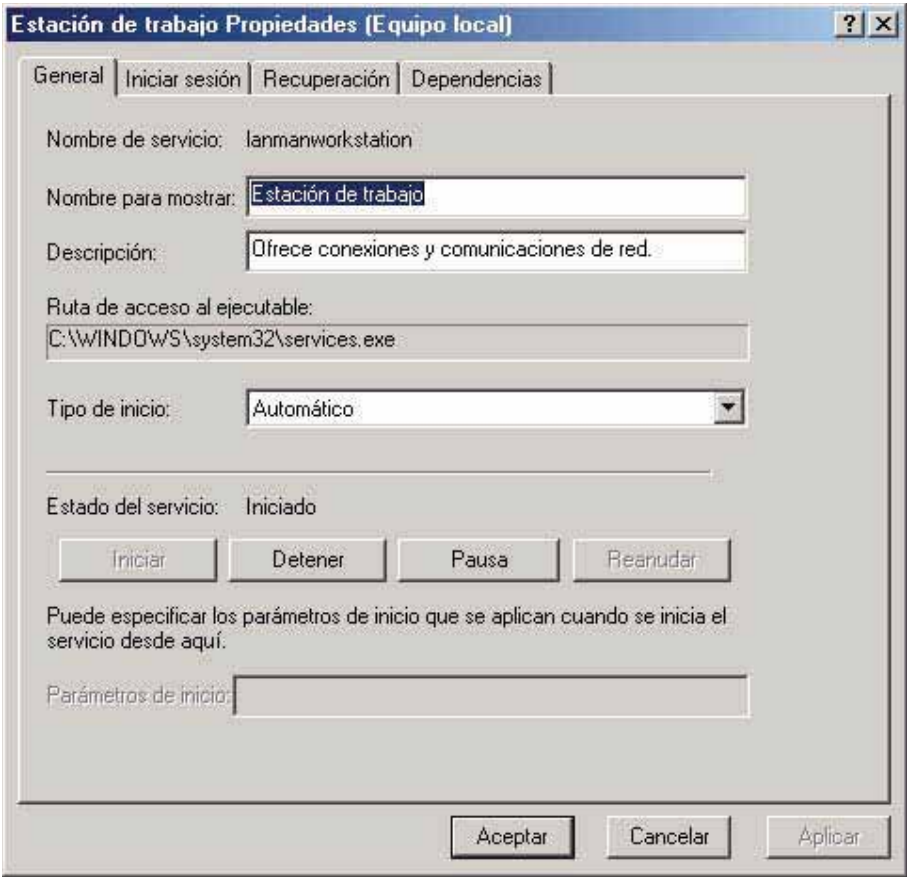
Para ver una lista de los servicios disponibles y su estado debemos ir a Inicio -> Ejecutar... y indicarle que ejecute *services.msc.* Se nos mostrará una pantalla con el listado de los servicios que se pueden ejecutar en nuestro ordenador.



Desde aquí podremos detener los servicios, pararlos, activarlos y especificar si deben arrancarse al iniciar el sistema. Podemos especificar tres estados diferentes para el tipo de inicio:

- *Automático*: el servicio se ejecutará al arrancar el sistema
- *Manual*: el servicio se ejecutará en el momento que Windows lo necesite
- *Deshabilitado*: el servicio no se ejecutará nunca

Para especificar el tipo de inicio pulsaremos con el botón derecho sobre el servicio que queremos modificar y iremos a la opción Propiedades. Allí podemos indicar el tipo de inicio que queramos.



Debemos tener especial cuidado al cambiar el tipo de inicio de algunos de los servicios, ya que esto podría hacer que nuestro ordenador no arrancase correctamente. Por ello, es especialmente importante conocer que hace cada uno de los servicios y saber si es seguro o no pararlo.

Mostramos aquí una lista de algunos de los servicios de Windows que es posible desactivar sin perder funcionalidad. Es recomendable desactivarlos uno a uno y comprobar que todo funciona correctamente después, en caso contrario deberemos volver a activarlo.

Lista de servicios

Nombre	*Descripción*	*Acción*
Actualizaciones automáticas	Permite la actualización automática de Windows	Desactivar solo si la vamos a hacer nosotros manualmente
Administrador de conexión automática de acceso remoto	Crea una conexión a una red remota cuando es necesario	Desactivar
Cliente de seguimiento de vínculos distribuidos	Envía notificaciones de movimientos de ficheros	Desactivar

Nombre	*Descripción*	*Acción*
Compatibilidad de cambio rápido de usuario	Permite que varias usuarios se conecten a la vez en el mismo ordenador	Desactivar si solo vamos a usar un usuario
Coordinador de transacciones distribuidas de Microsoft	Combina transacciones entre bases de datos, colas de mensajes…	Desactivar
DDE de red	Una reliquia de anteriores versiones	Desactivar
Enrutamiento y acceso remoto	Permite el acceso remoto	Desactivar
Escritorio remoto compartido de Netmeeting	Permite que alguien se conecte a nuestro ordenador través de Netmeeting	Desactivar
Examinador de equipos	Permite ver que ordenadores hay en la red	Desactivar si no vamos a conectarnos a ninguna red.
Firewall de Windows	Provee de un cortafuegos	Desactivar solo si vamos a instalar otro cortafuegos
Host de dispositivo Plug and Play universal	Permite autoconfigurar periféricos de este tipo (UPnP)	Desactivar si no tenemos ningún periférico UPnP

Nombre	*Descripción*	*Acción*
MS Software Shadow Copy Provider Service	Utilidad adicional para el uso de Microsoft Backup	Desactivar si no usamos Microsoft Backup
Portafolios	Permite el acceso remoto al portapapeles	Desactivar
Programador de tareas	Permite programar una tarea para que se ejecute de forma periodica	Desactivar si no necesitamos programar ninguna tarea
Registro remoto	Permite editar el registro de Windows desde otro ordenador	Desactivar
Servicio de alerta	Muestra determinadas alertas, como las del Monitor de rendimiento	Desactivar
Servicio de Fax	Permite el envío de fax	Desactivar
Servicio de Index Server	Indexa los contenidos de nuestro ordenador para hacer más rápidas las búsquedas	Se puede desactivar, consume muchos recursos
Telnet	Permite que se nos conecten a través del protocolo telnet	Desactivar
Temas	Administra los temas de escritorio	Se puede desactivar, ya que gasta muchos recursos

Mensajero

Desde la aparición de Windows NT, este lleva incluido un servicio que permite al usuario recibir mensajes del resto de ordenadores de la red. Igualmente también se nos ofrece el programa para poder enviar estos mensajes. Este servicio es conocido como *Mensajero* (en inglés, Messenger) y no tiene nada que ver con la aplicación de mensajería instantánea *MSN Messenger*.

El servicio *Mensajero* estaba pensado inicialmente para que el administrador pudiera enviar mensajes al resto de usuarios de la red, como por ejemplo, avisos de mantenimiento, recordatorios... El problema de este servicio es que por defecto está activado y puede ser accedido desde cualquier dirección de Internet. Los *spammers* han aprovechado esto para enviar su publicidad a cualquier ordenador que tuviera este servicio accesible.

Si no queremos recibir este tipo de mensajes deberemos desactivar este servicio.

Spim

Poco a poco nuestra cuentas de email se van llenando de correo basura, mensajes publicitarios enviados sin nuestro consentimiento, el conocido *spam*. Pero al parecer, los *spammers* no tienen suficiente con inundar nuestros buzones, ahora, además pretenden mandarnos su publicidad a través de los sistemas de mensajería instantánea, como *MSN Messenger*, *Yahoo Messenger*,...

Este nuevo medio de envío de publicidad, llamado *spim* (por relación con *spam* y *Instant Messaging* (mensajería instantánea)), consiste en el envío de mensajes comerciales a todas las personas posibles. Para ello, se utilizan programan que generan direcciones al azar donde se envía esta propaganda. Aunque hoy en día el uso de esta práctica todavía no está muy generalizado, es muy probable que poco a poco vaya aumentando, ya que cada vez el envío de *spam* se va a hacer más difícil y ello llevará a la generalización de otras técnicas para la distribución de publicidad.

Este nuevo tipo de marketing puede llegar a ser más molesto incluso que el *spam*, ya que habitualmente se recibe en el mismo momento en que se manda y interrumpe en mitad de lo que se esté haciendo. Por suerte, al tener que pasar todos los mensajes por un mismo servidor (el de *Microsoft*, el de *Yahoo* o el correspondiente en cada caso) es más fácil para los proveedores filtrar este tipo de mensajes y evitar molestias al resto de usuarios. También es posible para los servidores bloquearlos observando la cantidad de tráfico que envían, ya que sólo un programa automático es capaz de enviar tal cantidad de mensajes en tan poco tiempo.

Por parte del usuario es también más fácil el bloqueo de estos mensajes. Simplemente debemos indicar a nuestro cliente de mensajería que solo queremos recibir mensajes de gente que esté en nuestra lista de contactos, de esta forma evitaremos que cualquier desconocido nos asalte con publicidad.

Referencias

Dirección de descarga de CurrPorts
http://www.nirsoft.net/utils/cports.html

Dirección de descarga de la versión gratuita de Zone Alarm
http://download.zonelabs.com/bin/free/es/download/znalm.html

Dirección de descarga de Kerio Personal Firewall
http://www.kerio.com/kpf_download.html

Artículo acerca del spim
http://barrapunto.com/article.pl?sid=04/03/04/1447227

Tutorial de TCP/IP
http://www.faqs.org/rfcs/rfc1180.html

Listado de puertos utilizados por aplicaciones de Microsoft
http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref_net_ports_ms_prod.mspx

Artículo sobre publicidad a través del Mensajero de Windows
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q330904

Manual de Zone Alarm
http://www.almendron.com/zonealarm/mza.htm

[Capítulo 3]

Navegador

Cambiar el navegador: Firefox

Existen multitud de razones por las que no es deseable utilizar *Internet Explorer* para navegar a través de Internet sino otros navegadores. Es especialmente recomendable el uso de *Firefox*, un navegador de código abierto. *Firefox* es el heredero de *Netscape Navigator*, un navegador que tuvo un uso masivo hasta que fue superado por *Internet Explorer*. En 1998 Netscape publicó gran parte del código de *Netscape Communicator* y se creo una organización llamada *Mozilla* para desarrollar esta aplicación. Poco después se abandonó todo el código existente para reescribir el navegador desde cero. En estos años se han hecho grandes avances en el desarrollo de *Firefox* y hoy en dia es, probablemente, el más avanzado de los navegadores existentes.

Porqué debería usar Firefox en lugar de Internet Explorer?

- **Mejor soporte de estándares:**
  Firefox soporta más estándares y lo hace mejor que *Explorer*. De esta forma, cualquier página que este bien construida se verá correctamente en *Firefox*, lo cual no siempre sucede con *Explorer*, que además suele implementar extensiones propietarias que ningún otro navegador soporta.

- **Seguridad:**
  Firefox es mucho más seguro que *Internet Explorer* ya que está pensado, desde un principio, para ofrecer la máxima seguridad al usuario. Por ello, no permite la instalación o ejecución de código bajado de Internet sin el consentimiento del usuario así como tampoco el uso de controles *ActiveX*, una de las causas más habituales de los fallos de seguridad de *Internet Explorer*. Además, *Firefox* no implementa el concepto de zonas del que dispone *Explorer*, de forma que trata todo el contenido al que puede acceder como potencialmente peligroso, sin darle la posibilidad de otorgarle más permisos, otro de los fallos habituales de *Explorer* del que se aprovechaba mucho código malicioso para cambiar de zona y conseguir más privilegios.

- **Multiplataforma:**
  Firefox no solo funciona bajo *Windows*, sino que además también lo hace bajo *Linux*, *Mac OS X* y *Solaris*. Además, está disponible en multiples idiomas, como puede ser castellano, catalán, gallego y muchos otros.

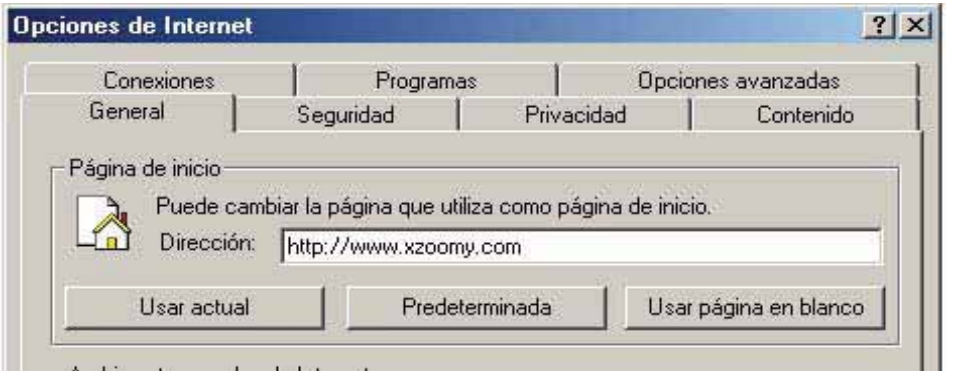
- **Extensible y adaptable:**
  Firefox provee de diversos métodos para cambiar la funcionalidad y la apariencia del navegador. A través de las extensiones podemos conseguir nuevas funciones del navegador, como bloqueo de publicidad o pequeños juegos. También podemos cambiar la apariencia del navegador mediantes los Temas, los conocidos *skins* que permiten cambiar desde los iconos hasta cualquier otro detalle del navegador.

- **Garantía de reembolso:**
  Además de todo esto, *Firefox* es gratuito y ocupa menos de 5 Mb, por lo que no perdemos nada por probarlo. Es probable que una vez lo hayamos probado ya no queramos volver nunca más a usar Internet Explorer.

Hijack

Una método utilizado por algunas páginas para aumentar el número de visitas que reciben es el *browser hijacking*, que consiste en el uso de técnicas para modificar algunos aspectos de nuestro navegador, como, por ejemplo, nuestra página de inicio o la de búsqueda.

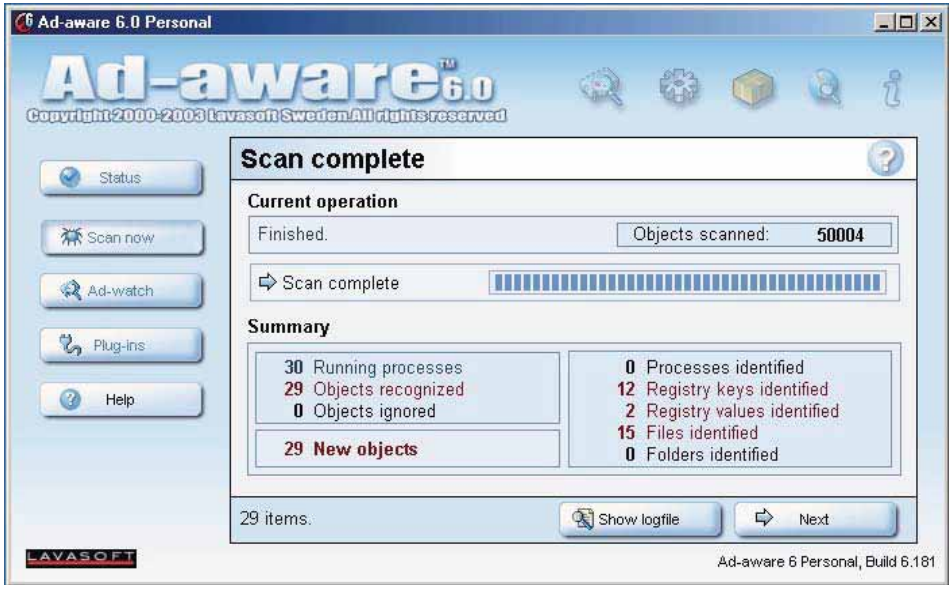
Qué se consigue con esto? Por una parte, aumentar el tráfico que recibe esa página, cosa que hará aumentar los beneficios por publicidad gracias a los *banners* que contendrá. Otras páginas lo utilizan para rastrearnos y espiar las páginas que visitamos, para crear perfiles sobre nosotros.



Existen diferentes tipos de técnicas para lograr estos objetivos. La menos peligrosa consiste en añadir un link a nuestros favoritos con el objetivo de que lo visitemos. También suelen modificar la página de inicio, de forma que cada vez que iniciemos el navegador iremos a parar a su sitio. Otros sitios más agresivos modifican nuestra página de búsqueda de modo que nuestro buscador por defecto será el suyo; algunas incluso nos harán creer que el buscador utilizado habitualmente (Google, Yahoo,...) funciona correctamente, pero los resultados ofrecidos no serán correctos, apuntando en su mayoría a su página. Finalmente, las más peligrosas llegan a modificar el

registro de Windows, a deshabilitar las opciones de Internet o a instalarnos programas de forma que cuando reiniciemos el ordenador los cambios que han hecho se mantengan. Para poder recuperar nuestro navegador, en un principio nos servirá el mismo programa que utilicemos para eliminar el spyware, por ejemplo *Ad-Aware* o *SpyBot* .

En caso de que con estos programas no consigamos recuperar el control de nuestro navegador podemos utilizar otros más avanzados como *Hijack This*, cuyo uso es más complicado pero nos asegurará el borrado de cualquier hijacker.



Parásitos

Cuando navegamos por Internet podemos encontrarnos miles de parásitos que intentan entrar en nuestro ordenador, normalmente a través de nuestro navegador, para lograr su propósito: instalarse en nuestro sistema. El objetivo de todos estos parásitos suele ser que veamos publicidad (a veces, incluso, redirigiendo las peticiones de páginas que hacemos hacia su propio servidor) o recopilar datos sobre nuestros hábitos de navegación.

Existe una manera sencilla y eficaz de evitar que la mayoría de estos bichos entren en nuestro sistema y es a través del fichero HOSTS. Cómo funciona este método? En primer lugar deberemos saber como funciona el sistema de DNS. En Internet cada servidor se identifica por su dirección IP, una serie de números que vienen a ser equivalentes al número de teléfono del servidor. Pero nosotros estamos acostumbrados a escribir una dirección textual; aquí es donde entra en juego el DNS. El DNS es el sistema encargado de convertir una dirección (p.ej. www.elligre.tk) en su correspondiente dirección IP (69.93.4.26). Así, solo nos falta saber que la dirección 127.0.0.1 corresponde siempre a nuestro propio ordenador, el que estemos utilizando en ese momento.

El fichero HOSTS le indica al sistema operativo la dirección IP correspondiente a ciertas direcciones textuales. Si en este fichero le indicamos 127.0.0.1 como dirección IP de un cierto sitio, el navegador no será capaz de encontrar ese sitio, ya que lo intentará buscar en nuestro ordenador local y no encontrará nada. Así, podemos aprovechar para bloquear todos aquellos sitios a los que no queramos acceder.

Para conseguir esto simplemente deberemos bajarnos el fichero HOSTS de alguna de las siguientes páginas:

http://www.mvps.org/winhelp2002/hosts.htm
http://www.everythingisnt.com/hosts.html
http://pgl.yoyo.org/adservers/

y deberemos guardarlo en el directorio `c:\windows\system32\drivers\etc` (puede ser diferente si tenemos el sistema operativo instalado en otro directorio). A partir de ese momento navegaremos más seguro y más rapidamente, sin tener que ver tanta publicidad en nuestro navegador.

Alguno de estos ficheros HOSTS solo bloquea la publicidad y no el resto de parásitos, por ello el más recomendable es el que está disponible en el primero de los links. De todas maneras, podemos probar cual nos gusta más, ya que cada uno bloquea sitios diferentes.

Cookies

Qué son las cookies?

El protocolo HTTP, que es el que usa nuestro navegador, es un protocolo sin estado, es decir, que no guarda ninguna información entre una petición de una página y la siguiente. Esto impide al servidor saber si quien pide una página es el mismo que ha pedido otra anteriormente, lo que provoca que el servidor no tenga manera de guardar preferencias o datos similares para personalizar las páginas que se le piden.

Por ejemplo, en el buscador Google podemos personalizar las búsquedas indicandole en que idioma queremos buscar o cuantos resultados queremos visualizar por pantalla. Como se consigue esto? A través de las *cookies*.

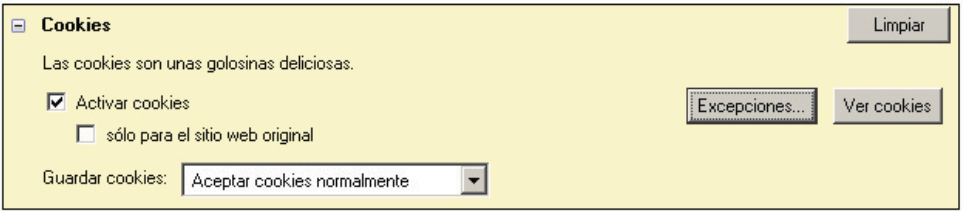
Las *cookies* son unas pequeñas cadenas de texto que nos envía el servidor la primera vez que nos conectamos a él. Esta cadena nos identifica ante el servidor, ya que cada vez que pedimos una página a ese servidor se envía de vuelta la *cookie*, de forma que pueda saber quien somos.

El problema de las cookies

Esto puede ser bueno en determinadas páginas, pero presenta un problema cuando se usa indebidamente. Muchas empresas de publicidad instalan *cookies* en nuestro ordenador sin avisarnos, de forma que pueden conocer que páginas visitamos y de este modo enviarnos publicidad personalizada. Hay que tener en cuenta que las *cookies* no pueden dañar nuestro ordenador (como haría un virus), pero pueden dañar nuestra privacidad si son usadas incorrectamente

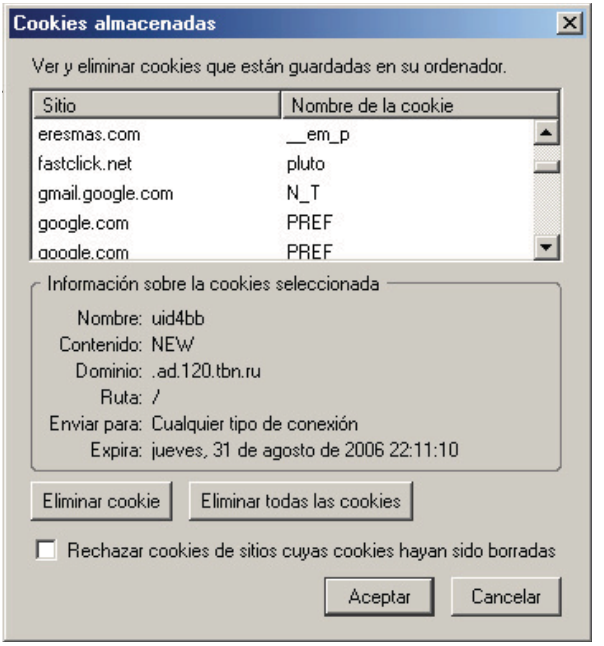
por parte del servidor; no todas las *cookies* son malas y algunas son muy útiles.

La forma más sencilla de librarse de ellas es desactivándolas en nuestro navegador o bien configurando que sitios permitimos que nos envíen cookies y cuales no. Para ello, en Firefox podemos ir al menú Herramientas -> Preferencias y allí ir a la opción de Privacidad, donde encontraremos el apartado Cookies.



Desde allí podemos desactivarlas o establecer excepciones, de forma que podremos indicarle al navegador las páginas de las que no queremos recibir *cookies*. Es recomendable, además, activar la opción *Sólo para el sitio web original*, para evitar que diferentes sitios web puedan enviarse sus *cookies* entre ellos

También podemos ver todas las *cookies* que ya tenemos en nuestro ordenador si pulsamos en la opción *Ver cookies*. Desde allí podremos borrarlas individualmente o todas de una vez.



Debemos tener cuidado con las *cookies* que borramos, ya que al eliminar algunas de ellas podemos perder la configuración personalizada o la entrada automática (sin tener que introducir el usuario y la contraseña) en alguna de las webs que visitemos habitualmente. Por ello, es recomendable borrar solo aquellas que sean procedentes de sitios que no conocemos o que sepamos que no vamos a visitar con frecuencia.

HTTP Seguro

El protocolo HTTP, usado al navegar por Internet, envía todos los datos a través de la red en forma de texto. Esto implica que cuando estamos accediendo a cualquier página web todo lo que enviamos y recibimos puede ser leído por todos los ordenadores por donde pasan los datos (los de nuestro ISP, los del ISP de la página a la que accedemos, los nodos intermedios,...)

Cuando navegamos por páginas con información confidencial como, por ejemplo, nuestro correo electrónico o la página de nuestro banco, no queremos que esa información pueda ser leída por nadie, por lo que no nos interesa utilizar el protocolo HTTP habitual, sino el protocolo HTTP seguro, que permite, además de ocultar la información que se transmite, asegurar que la página a la que nos conectamos es quien dice ser y no ha sido suplantada por otra.

Cómo funciona HTTP Seguro?

HTTP Seguro (a partir de ahora, HTTPS) funciona gracias a la criptografía, que permite asegurar mediante una serie de funciones matemáticas el origen y la ocultación de los datos. Por suerte, no necesitamos saber como funciona matemáticamente el sistema, ya que el navegador se encargará automáticamente de ello.

Cada servidor que quiera implementar HTTPS debe disponer de un certificado, una especie de DNI digital, que nos indica todos sus datos y la clave que permite cifrar todo lo que enviamos y recibimos del servidor. Estos certificados son emitidos por una serie de compañías a nivel mundial, que garantizan la identidad del propietario del certificado.

Cómo utilizar HTTPS?

Vamos a ver un ejemplo práctico del uso de HTTPS. Para ello, entraremos en la web de un banco cualquiera, en este caso Sabadell Atlántico y veremos como utilizar el protocolo seguro.

La primera diferencia entre el protocolo normal y el seguro es el uso de https para indicar que la conexión debe ser segura. Si queremos acceder a nuestro banco la dirección para mostrar la página principal es http://www.sabadellatlantico.com.

El problema de esta página es que la información enviada cuando intentemos conectarnos podría ser leída por otras personas y que no podemos asegurar el origen de la página, pues podría haber sido suplantada por alguien para intentar conseguir códigos de acceso al banco. Por ello, vamos a utilizar HTTPS para acceder a la página. En lugar de la dirección anterior, en esta ocasión cambiaremos el http del inicio por https, de forma que nos quedará https://www.sabadellatlantico.com y nos mostrará la misma página en modo seguro.

La segunda diferencia que encontramos en la página es que el navegador nos muestra la dirección con el fondo de color amarillo, para así poder distinguir las páginas normales de las seguras.

Finalmente, también se muestra un pequeño candado en la barra de la dirección y, si hacemos doble-click sobre él, se nos mostrará una ventana con información sobre la página actual, donde podremos comprobar la autenticidad del sitio y que la conexión ha sido cifrada de forma que nadie pueda leer nuestros datos. Podremos, Incluso, ver el certificado de la página para hacer comprobaciones más exhaustivas.

Es muy recomendable comprobar esta información cada vez que accedamos a una página segura, ya que el simple hecho de usar HTTPS no garantiza la autenticidad del origen de los datos, sino que debemos comprobarla personalmente. A pesar de eso, si la identidad del certificado no coincide con la de la página que estamos visitando el navegador nos avisará y nos mostrará una ventana con información, avisándonos de lo que sucede y preguntándonos si realmente queremos visitar la página.

ATENCIÓN

Acceder a un servidor en modo seguro no nos garantiza la fiabilidad de la operación que realicemos. Antes de realizar alguna compra a través de Internet es recomendable informarse acerca de la empresa que nos ofrece el producto. Normalmente, bastará con una simple búsqueda del nombre de la empresa en Google y allí podremos ver si hay alguna queja sobre su funcionamiento.

Referencias

Dirección de descarga de Firefox
http://www.difundefirefox.com/

Dirección de descarga de extensiones para Firefox
http://update.mozilla.org/extensions/

Dirección de descarga de temas para Firefox
http://update.mozilla.org/themes/

Dirección de descarga de HijackThis
http://tomcoyote.com/hjt/

Artículo muy completo acerca de las cookies
http://www.cookiecentral.com/faq/

[Capítulo 4]

Correo electrónico

Cambiar el lector de correo: Thunderbird

Igual que en el caso del navegador, no es recomendable utilizar el lector de correo que lleva incorporado Windows, *Outlook Express*, ni tampoco su hermano mayor, *Outlook*, que suele venir incluido en *Microsoft Office*, sino algún otro sustituto como puede ser *Thunderbird*. Este es un lector de correo de los mismos creadores de *Firefox* y que, por lo tanto, dispone de muchas de sus mismas características: mayor seguridad, código abierto, gratuito, multiplataforma, extensible...

Porqué debería usar Thunderbird en lugar de Outlook?

En primer lugar, *Thunderbird* ofrece mucha más seguridad que *Outlook*. A principios de 1999 vio la luz el virus *Melissa*, el primer virus con una gran expansión que utilizaba el correo electrónico para reproducirse. Al abrir un archivo que llevaba adjunto el mensaje el virus se ejecutaba y se enviaba a si mismo a las primeras 50 entradas de la libreta de direcciones de *Outlook*. Al año siguiente apareció el famoso virus ILOVEYOU, que también utilizaba las direcciones de *Outlook* para enviarse al ejecutar un fichero adjunto al mensaje.

En 2001, el virus *Nimda* aprovechaba una vulnerabilidad en *Outlook* para ejecutarse sin necesidad de interacción por parte del usuario. No era necesario abrir ningún fichero adjunto, el simple hecho de visualizar el mensaje ya ejecutaba el virus. Aunque estos son los más conocidos no son los únicos virus que existen que utilizan *Outlook* para propagarse.

Otra razón para usar *Thunderbird* es el filtro que incorpora para detectar el correo basura, *spam* que suele llenar nuestros buzones con mensajes comerciales indeseables, y del que hablaremos después más detalladamente. También dispone de otra serie de opciones para proteger nuestra privacidad, como la desactivación de la visualización de imágenes en mensajes sospechosos de ser *spam*.

Finalmente, *Thunderbird* nos facilita la migración desde *Outlook* o desde *Outlook Express*, ya que permite importar todos los datos desde estos dos programas o desde versiones anteriores de *Netscape*.

Correo basura

Conocemos como *spam* o "correo basura" aquellos mensajes no deseados o no solicitados que llegan a nuestra cuenta de correo. Habitualmente, consisten en publicidad de productos poco o nada legales o en esquemas para hacerse rico rapidamente.

Los *spammers*, como se conoce a la gente que envía este tipo de correos, utilizan esta técnica porque es una manera muy barata y rápida de hacer llegar el mensaje a muchísima gente. Al no ser el *spammer* el que carga con los gastos de enviar esos correos, sino que suelen ser o bien los usuarios que los reciben o bien el servidor desde donde se envían, pueden enviar millones de mensajes al mismo tiempo. Uno de los últimos métodos utilizados por los *spammers* es el uso de ordenadores infectados por virus, de los cuales toman el control remotamente y desde donde envían el *spam*. Existen, incluso, organizaciones que venden listas con las direcciones de estos ordenadores listos para ser usados como plataformas de envío masivo de mensajes.

El problema para el usuario es que, hoy en dia, el *spam* suele superar en número a los mensajes que sí le interesan, de forma que tiene que borrar una gran cantidad de mensajes que no quiere leer para llegar al correo genuino. Todo esto, además, vigilando de no perder entre todo este *spam* mensajes realmente importantes. Según algunos estudios, un tercio del correo electrónico enviado en Estados Unidos es *spam*, aunque hay quien considera este porcentaje muy bajo y dependiendo del servidor podría llegar a tasas del 98% del correo recibido.

Para conseguir direcciones de correo donde poder enviar sus mensajes, los *spammers* suelen recorrer las páginas web, mediante programas conocidos como *bots*, buscando palabras que coincidan con el formato de una dirección de correo (es decir, cualquier cosa que se parezca a nombre@servidor.com). Para impedir que los spammers puedan encontrar así nuestra dirección podemos utilizar una serie de técnicas distintas:

- Distorsionar deliberadamente nuestra dirección, de forma que quien quiera escribirnos pueda hacerlo, pero un *bot* utilize una dirección erronea por no saber interpretarla. Por ejemplo, si nuestro correo es minombre@example.com podríamos transcribirlo como minombreQUITAR@ESTOexample.com. Esto debemos hacerlo siempre que nuestra dirección vaya a aparecer publicada en cualquier sitio (un foro, un comentario en alguna página,...)

- Utilizar dos cuentas diferentes, nuestra cuenta habitual, cuya dirección solo proporcionaremos a gente de confianza, y una cuenta en un servidor gratuito para todos los sitios que nos pidan una dirección de correo para podernos registrar. De este modo, si nos envían spam a esa dirección no la recibiremos en nuestra cuenta personal.

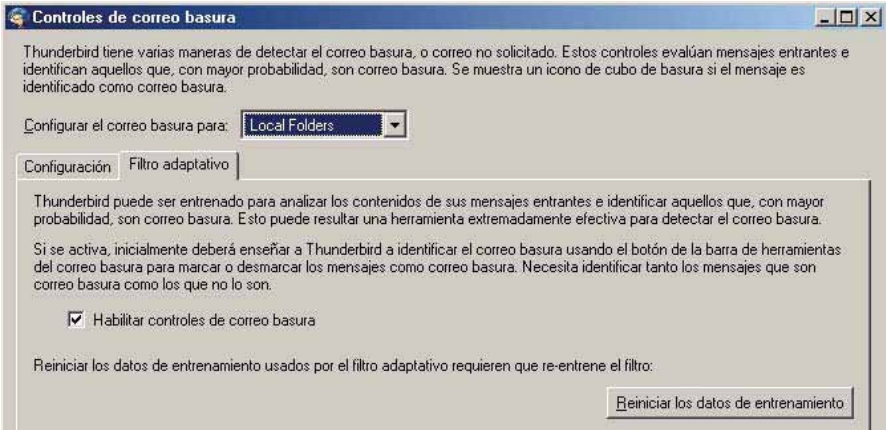
- Muchas de estas direcciones se consiguen pidiendo la dirección para que nos envíen algo a nosotros o a algún amigo (felicitaciones "electrónicas", chistes,...). No debemos dar nuestra dirección ni la de nadie en ninguno de estos sitios si no es de total confianza.

- En caso de que recibamos *spam* en nuestra cuenta no debemos responder nunca al mensaje recibido, ya que la dirección de origen suele ser falsa. Aunque muchos de estos correos suelen llevar una dirección donde podemos darnos de baja, no debemos hacerlo nunca ya que de esta manera confirmaríamos al spammer que nuestra dirección de correo realmente existe y que además hemos leído el mensaje que nos ha enviado, con lo cual nos convertimos en un objetivo deseado para que nos envíen más correo de este tipo.

Detectando el correo basura automáticamente

Thunderbird dispone de una herramienta para clasificar el correo electrónico, de forma que puede detectar automáticamente y con una gran probabilidad de acierto si un mensaje es *spam* o es un correo legítimo. Para ello utiliza un algoritmo conocido como *filtro bayesiano*, que consiste en conocer la probabilidad de que una palabra aparezca en un mensaje corriente y en uno de *spam*. De este modo, examinando las palabras de un mensaje y conociendo sus diferentes probabilidades será capaz de distinguir entre un tipo y otro.

Para activar este filtro debemos ir al menú *Herramientas -> Controles de correo basura*



y en el apartado *Filtro adaptativo* marcamos la opción *Habilitar controles de correo basura* para todas las cuentas que tengamos.

Una vez activado deberemos entrenar a *Thunderbird* para que reconozca que mensajes son correo basura y cuales son correo legítimo.

Para ello utilizaremos el botón *Basura* de la barra de tareas en caso de que encontremos un mensaje de *spam* y queramos clasificarlo como tal.

Utilizaremos el botón *No es correo basura* en caso de que *Thunderbird* nos clasifique algún correo incorrectamente como *spam*.

Una vez hayamos entrenado suficientemente al programa, este será capaz de clasificar correctamente los correos que recibamos y puede moverlos directamente a una carpeta especial si así se lo indicamos, para que ni siquiera tengamos que verlos.

En caso de que activemos esta última opción es recomendable revisar una vez por semana la carpeta de correo basura, de forma que no perdamos algún correo importante al haber sido mal clasificado.

Phishing

Una modalidad de timo usada en Internet es el envío de emails que simulan provenir de nuestro banco o de alguna tienda de Internet, como Amazon. Suelen avisar de que nuestra contraseña puede haber sido comprometida, que están validando a los usuarios o nos piden que confirmemos algún cargo que se ha hecho a nuestra nombre. Para ello necesitan que entremos en nuestra cuenta y nos ofrecen un enlace que permite entrar directamente en ella.

Este enlace nos va a redirigir a una página creada por el timador, con un aspecto lo más parecido posible al original, pero controlada por él, de forma que cuando introduzcamos nuestro número de cuenta o DNI y la contraseña asociada, estos no irán a parar al banco o tienda, sino al timador que dispondrá de ellos y podrá acceder a nuestra cuenta como si fuéramos nosotros.

Estos correos suelen estar escritos en formato HTML y simulan con gran fidelidad el look corporativo del banco o tienda, por lo que puede resultar sencillo que el usuario caiga en la trampa sin darse cuenta.


Thunderbird piensa que este mensaje es correo basura

Asunto: Citibank's official notice

De: Citibank cuse-billing12@citibank.com

Fecha: 22/07/2004 7:58

A: madeleine@arane.com

citi

Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

A member of citigroup

Copyright © 2004 Citicorp

in 1926 Paranormal Auctions select location from in 1894

Como ejemplo, podemos ver este correo donde se informa que el software utilizado por el banco está siendo actualizado y que es necesario que entremos en nuestra cuenta para verificar nuestros datos. Para ello, ofrecen un supuesto enlace que parece apuntar a la página de Citibank, pero que gracias a la manipulación de la dirección en realidad apunta a http://200.246.11.135:3127/cit/index.htm que corresponde a una máquina que está bajo el control del timador.

Como protegernos del phishing?

Debemos tener en cuenta que es muy poco probable que nuestro banco nos envíe un correo electrónico para verificar nuestros datos o para informarnos de algún cargo a nuestra cuenta. Aun así, existe la posibilidad de que alguno de estos correos sea realmente de nuestro banco, pero debemos asegurarnos de ello y tomar una serie de precauciones antes de actuar:

- Tener en cuenta que el correo puede ser falso por lo que deberemos comprobarlo por algún otro medio

- Comprobar que el correo está bien escrito, sin faltas de ortografía, bien redactado y es coherente. Los *phishers*, muchas veces, ni siquiera se preocupan de preparar bien sus mensajes o de escribirlos correctamente.

- No acceder nunca a la página mediante el enlace que nos ofrecen. Es mucho más seguro acceder a través del navegador y escribir nosotros mismos la dirección para entrar.

- En caso de duda ponernos en contacto telefónico con la entidad para comprobar la autenticidad y veracidad del mensaje recibido.

Cadenas

Con cierta regularidad recibimos en nuestros buzones electrónicos mensajes enviados en cadena por conocidos nuestros donde se nos advierte de supuestos peligros, de supuestos virus o se nos pide nuestra colaboración para algún tipo de proyecto.

Estos correos, conocidos como *hoaxes*, suelen ser enviados con la mejor intención, pero resultan casi siempre falsos, como una especie de leyenda urbana distribuida por Internet.

Podemos distinguir un mensaje de este tipo porque suele anunciar grandes desgracias en caso de que no lo reenvíes a un cierto número de personas, no suelen ir firmados, nos prometen regalos por parte de alguna compañía o nos ofrecen alguna información poco creíble. Algunos ejemplos de este tipo de correos son:

- Envía este email a 10 personas y un niño recibirá un dolar por cada mensaje
- Nokia esta haciendo promoción de sus móviles. Envía este email a 800 personas y recibirás un móvil gratuito
- Hay un virus muy peligroso. Busca cierto fichero en tu disco y si existe borralo
- Reenvía esta cadena a 15 amigos o te quedaras calvo en menos de una semana

No debemos reenviar nunca estos correos puesto que, con ello, lo único que conseguimos es saturar el tráfico de la red y llenar los buzones de nuestros conocidos de mensajes que probablemente no les interesen. En caso de duda, podemos consultar la página Rompecadenas para saber si un correo es de este tipo.

Privacidad del correo

Normalmente consideramos que los correos electrónicos que enviamos son como una carta, van guardado dentro de un sobre y nadie puede leerlos. Esto no es cierto, ya que estos correos viajan como texto plano (es decir, texto visible a simple vista) por lo que pueden ser vistos por cualquier sistema por donde pasen. Debemos tener en cuenta que, muchas veces, los mensajes no viajan directamente al servidor del destinatario, sino que pasan por diversos servidores intermedios antes de llegar a su destino. Podemos verlo en las cabeceras de un correo real:

```
Received: from 205-158-62-26.outblaze.com
([205.158.62.26] helo=spf4.us.outblaze .com) by xxxx
with esmtp (Exim 3.35 #1 (Debian)) id 1AWFK5-0004pF-00
for <xxx@xxx.com>; Tue, 16 Dec 2003 14:33:14 +0100

Received: from web60809.mail.yahoo.com
(web6080.mail.yahoo.com [216.155.196.72]) by
spf4.us4.outblaze.com (Postfix) with SMTP id
9E99D1BA1EE for <xxx@xxx.com>; Tue, 16 Dec 2003
13:38:21 +0000 (GMT)

Received: from [213.0.240.13] by
web60809.mail.yahoo.com via HTTP; Tue, 16 Dec 2003
14:38:03 CET
```

Cada una de las lineas *Received* indica un servidor por donde ha pasado el correo, de forma que cualquiera de los servidores puede haber leído el contenido del mensaje enviado.

Además, si utilizamos el protocolo IMAP para leer el correo, este suele quedar almacenado en el servidor, donde el administrador puede leerlo facilmente. Esto desde luego no es legal pero es difícilmente detectable.

También existe la posibilidad, en caso de estar utilizando una cuenta de correo otorgada por la empresa en que trabajamos, que esta esté controlada, es decir, que se monitorice el uso de esta e incluso el contenido de los emails enviados y recibidos. La legalidad de este tipo prácticas no está demasiado clara, habiendo incluso sentencias judiciales contradictorias.

De forma similar al correo tradicional, el remitente de un correo electrónico es muy fácil de falsificar. Si queremos cambiar el remitente de una carta tan solo debemos escribir la dirección que nos interese en el reverso del sobre; de igual manera podemos modificar el remitente de un correo electrónico. La mayoría de programas de correo permite cambiar la cabecera y indicar la dirección que nosotros queramos, y aunque se puede saber si el remitente ha sido falseado este es un proceso complicado y que puede no llevarnos a descubrir el verdadero remite.

Cómo podemos proteger nuestro correo?

Para resolver el problema de la falta de privacidad y de la autenticación se utiliza la firma digital; esta permite confirmar que quien envía el mensaje es quien dice ser y/o cifrar el mensaje de forma que solo su destinatario pueda leerlo. Existen diversos sistemas de firma digital, entre ellos los más conocidos y utilizados son S/MIME y los basados en OpenPGP.

Los programas de firma digital permiten dos funciones principales: la firma y el cifrado de los mensajes.

La firma permite garantizar que el origen del mensaje es el correcto y que el contenido del mensaje no ha sido modificado.

El cifrado permite que solo el destinatario pueda leer un determinado mensaje. Habitualmente se combina con la firma, de forma que solo el destinatario correcto verá el contenido del mensaje y podrá saber que no ha sido manipulado y además podrá garantizar por quien ha sido enviado.

Cómo funciona la firma digital

Para conseguir la seguridad requerida en el correo electrónico se utilizan una serie de funciones matemáticas, englobadas dentro del campo de la criptografía. Existen varios conceptos clave para entender como funciona todo el sistema:

- **Criptografía de clave simétrica:** Los sistemas de clave simétrica utilizan una misma clave para cifrar y descifrar, de forma que tanto el emisor como el receptor del mensaje deben ponerse de acuerdo previamente en la clave a utilizar. El mensaje a enviar se divide en bloques de igual tamaño y a cada uno de estos bloques se le aplica la misma función de cifrado. El receptor aplica la función de descifrado a cada uno de los bloques recibidos y obtiene el mensaje original. Ejemplos de este tipo de algoritmos son *DES*, *Blowfish* o *AES-Rijndael*.
- **Criptografía de clave asimétrica:** Los sistemas de clave asimétrica utilizan claves distintas para cifrar y para descifrar. De esta forma, se pretende evitar el problema de que los comunicantes tengan que acordar previamente una clave. Cada uno de ellos dispone de un par de claves, una pública, que permite cifrar y verificar firmas y una privada, que permite descifrar y firmar. La clave pública se puede distribuir a cualquier persona y la clave privada es la que debe mantenerse en secreto. Si "A" quiere enviar un mensaje a "B" debe cifrarlo con la clave pública de "B", de forma que este solo podrá ser descifrado con la clave privada de "B". Ejemplos de este tipo de algoritmos son *RSA* o *ElGamal*.

- **Funciones resumen (hash):** Las funciones resumen hacen corresponder un mensaje de longitud arbitraria a otro de longitud fija (el *hash*, normalmente más pequeña). Esta función debe cumplir dos condiciones: ha de ser difícil encontrar dos mensajes diferentes cuyo *hash* sea el mismo y dado el *hash* ha de ser imposible conocer el mensaje original.

El inconveniente de los sistemas de clave asimétrica es que son mucho más lentos que los de clave simétrica, por lo que se suelen cifrar los mensajes con un clave simétrica aleatoria (clave de sesión) que se cifra con un sistema de clave asimétrica para darla a conocer al otro participante de la conversación. De este modo, en lugar de cifrar todo el mensaje (que potencialmente puede ser muy extenso) con la clave pública solo cifraremos una clave de sesión, lo cual nos ahorrará mucho tiempo.

La mejor forma de entender como funciona todo esto es ver un ejemplo: supongamos que "A" quiere enviar un mensaje cifrado a "B". Para ello deberá hacer:

1. Crear una clave aleatoria K
2. Cifrar el mensaje original M con la clave K obteniendo M'
3. Cifrar la clave K con la clave pública de B, obteniendo K'
4. Enviar M' y K' a B

Cuando B reciba M' y K' deberá hacer:

1. Descifrar K' con su clave privada, obteniendo K
2. Descifrar M' con la clave K, obteniendo M

Este proceso se complica si además de enviar el mensaje cifrado se quiere enviar también firmado, pues entonces también entran en juego la clave privada y la pública de A.

Si "A" quiere enviar un mensaje firmado a "B" (de forma que B puede asegurar que A ha escrito ese mensaje y que el contenido no ha sido modificado) deberá hacer:

1. Hacer un resumen del mensaje M, obteniendo H
2. Cifrar H con su clave privada, obteniendo H'
3. Enviar M y H' a B

Cuando B reciba M y H', para comprobar que ha sido enviado por A deberá hacer:

1. Hacer un resumen de M, obteniendo J
2. Descifrar H' con la clave pública de A, obteniendo H
3. Si H es igual a J la firma es correcta

Finalmente, si A quiere enviar a B un mensaje cifrado y firmado deberá realizar los siguientes pasos:

- Primero se debe firmar el mensaje:
  1. Hacer un resumen del mensaje M, obteniendo H
  2. Cifrar H con su clave privada, obteniendo H'
  3. Juntamos M y H' obteniendo N
- Después se debe cifrar N:
  1. Crear una clave aleatoria K
  2. Cifrar el mensaje N con la clave K obteniendo N'
  3. Cifrar la clave K con la clave pública de B, obteniendo K'
  4. Enviar N' y K' a B

Y B para leer el mensaje y comprobar que ha sido escrito por A deberá hacer:

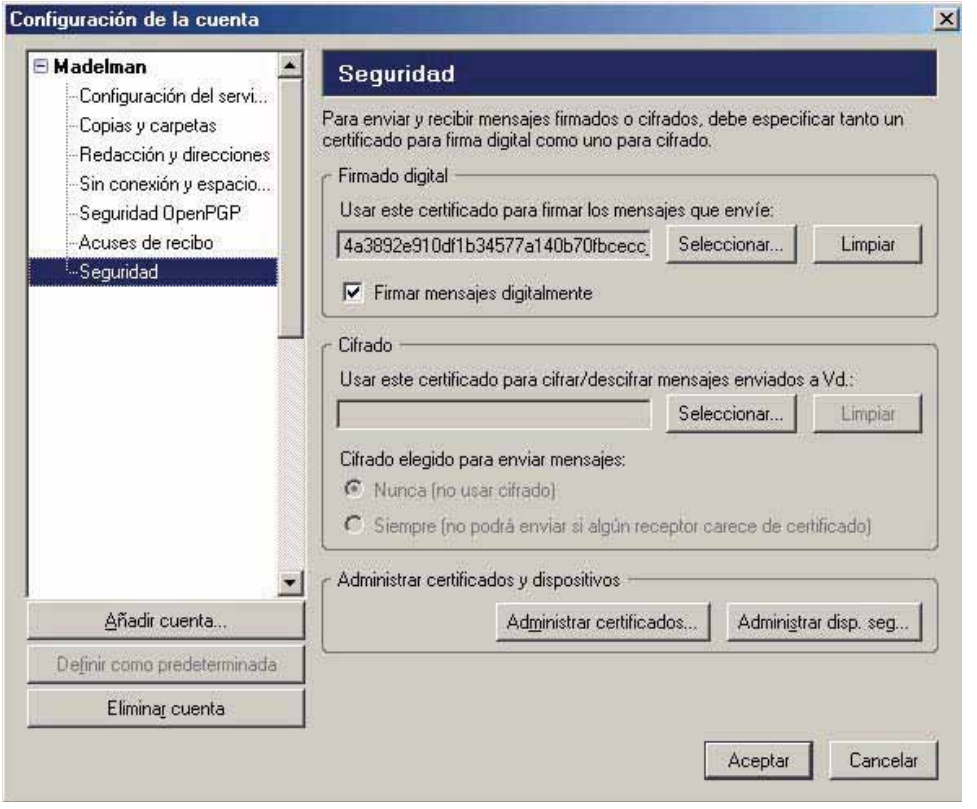
1. Descifrar K' con su clave privada, obteniendo K
2. Descifrar N' con la clave K, obteniendo N
3. N está compuesto por M y H'
4. Hacer un resumen de M, obteniendo J
5. Descifrar H' con la clave pública de A, obteniendo H
6. Si H es igual a J todo ha sido correcto

Automatizando el proceso

La teoría matemática detrás de este proceso es complicada, por suerte existe una serie de programas como GPG que se encarga de realizar todos estos pasos por nosotros automáticamente. Además, también se comprime el mensaje que queremos enviar para reducir el espacio que ocupa y aumentar la seguridad. Otra medida que utiliza GPG es la petición de una contraseña antes de poder usar la clave privada, de forma que nadie pueda usar nuestra clave privada sin conocer esta contraseña.

En nuestro caso vamos a utilizar la función integrada en Thunderbird, basada en S/MIME. Para ello, en primer lugar, necesitamos conseguir nuestro certificado de usuario. Podemos conseguir uno gratuitamente en http://www.cacert.org. Allí nos daremos de alta y el sistema nos enviará un correo a nuestra dirección para comprobar nuestra identidad; posteriormente, podremos descargarnos el certificado, que quedará instalado en nuestro navegador. Una vez instalado, podremos exportarlo desde el navegador (en primer lugar, para hacer una copia de seguridad) e importarlo en nuestro programa de correo.
Otra opción, en el caso de España, es utilizar el certificado que nos ofrece la Fábrica Nacional de Moneda y Timbre, que también sirve para presentar la declaración de Hacienda a través de Internet y otras gestiones con la Administración. Este certificado se puede conseguir en http://www.cert.fnmt.es

Para utilizar este certificado en Thunderbird, una vez lo hayamos exportado desde nuestro navegador, vamos al menu *Herramientas* -> *Configuración de cuentas* y entramos en la opción *Seguridad*. Desde allí entramos en *Administrar certificados* donde nos permitirá importar nuestro certificado.



Posteriormente debemos configurar nuestra cuenta para que use este certificado para firmar los mensajes que enviemos. Para ello, una vez importado el certificado, lo seleccionamos en la opción de Firmado digital y marcamos la opción *Firmar mensajes digitalmente*

Una vez lo tengamos activado todos los mensajes que enviemos se firmaran digitalmente y nuestros contactos podrán comprobar que el correo recibido es legítimo. Para ello necesitarán tener nuestra clave pública, que les deberemos proporcionar nosotros y que podemos obtener exportándola desde el navegador (recordando siempre de no distribuir nuestra clave privada a nadie bajo ningún concepto).

Cuando alguien nos envíe un correo electrónico firmado podremos comprobar si es válido o no. Thunderbird muestra un icono como este

si el mensaje está firmado pero no se ha podido comprobar la autenticidad del firmante, habitualmente porque no disponemos de su clave pública. En caso de que sí dispongamos de su clave pública Thunderbird comprobará la identidad y si esta es correcta mostrará el icono

con lo que podemos estar seguros de que el mensaje es de quien dice ser y que el contenido no ha sido modificado por nadie. También podemos hacer servir estos certificados para enviar correo cifrado, de forma que solo su destinatario pueda leerlo.

Referencias

Artículos sobre la privacidad del correo en el trabajo
http://www.baquia.com/com/20001221/art00032.html
http://www.informatica-juridica.com/trabajos/el_uso_del_correo_electronico_en_el_trabajo.asp

Artículos con información sobre el virus ILOVEYOU
http://www.virusprot.com/Vi00012a.html
http://www.vsantivirus.com/loveletter.htm

Artículo con información sobre el virus NIMDA
http://www.hispasec.com/unaaldia/1061

Artículos con información sobre la proporción de spam
http://www.theregister.co.uk/2004/04/20/idc_spam_survey/
http://it.slashdot.org/article.pl?sid=04/04/20/1558244&tid=111

Cómo evitar el spam
http://www.rickconner.net/spamweb/avoiding.html

Información sobre el spam
http://spam.abuse.net/overview/

Grupo de trabajo contra el phishing
http://www.antiphishing.org/

Artículo sobre el phishing
http://www.consumer.es/web/es/especiales/2004/09/22/109261.php

Información sobre las cadenas en el correo electrónico
http://www.rompecadenas.com.ar/

Introducción al funcionamiento PGP
http://www.pgpi.org/doc/pgpintro/

[Capítulo 5]

Seguridad de los datos

Copias de seguridad

Más tarde o más temprano, todo aparato electrónico tiene tendencia a fallar. Siendo el ordenador un aparato electrónico, compuesto además de innumerables piezas electrónicas, la probabilidad de que alguna de ellas se estropee es relativamente alta. Si tenemos suerte, el fallo podrá repararse simplemente sustituyendo la pieza averiada pero, en otros casos, la reparación puede ser imposible o puede haber afectado tanto a nuestros datos que estos sean irrecuperables. Es en esos momentos cuando es más necesario tener copias de seguridad de todos nuestros datos, de forma que podamos recuperarlos rápidamente y sin problemas.

Desgraciadamente, el tener copias de seguridad no es un hecho habitual entre la mayoría de los usuarios, que solamente toman la determinación de hacer estas copias una vez han sufrido en sus propias carnes la perdida total y completa de datos importantes, momento a partir del cual realizan las copias regularmente.

Es importante tomar conciencia de la necesidad de las copias de seguridad antes de sufrir alguno de estos problemas que nos pueden hacer perder horas y horas de trabajo y que podían haber tenido fácil solución con unas pequeñas medidas de prevención.

Planeando las copias de seguridad

En un ordenador personal tenemos dos tipos de ficheros: reemplazables e irreemplazables.

Los ficheros reemplazables son aquellos de los cuales disponemos una copia. Habitualmente, estos son los ficheros del sistema operativo y de los diversos programas que hayamos ido instalando (siempre que dispongamos del original desde donde los instalamos o estos estén libremente disponibles en Internet para su descarga legal).

Los ficheros irreemplazables son aquellos de los que no disponemos de ninguna copia ni ninguna manera sencilla de recuperar su contenido en caso de borrado accidental. Normalmente estos ficheros serán los datos generados por los programas que utilicemos (documentos de texto, imágenes tomadas de nuestra cámara digital, hojas de cálculo con nuestra contabilidad,...)

Nuestro objetivo deberá ser convertir los ficheros irreemplazables en ficheros reemplazables. Para conseguirlo deberemos tener copias de seguridad de estos ficheros de forma que podamos recuperarlos en caso de pérdida.

Para tener unas buenas copias de seguridad deberemos plantearnos las siguientes preguntas:

Qué?

Cuáles son los ficheros que realmente nos interesa mantener? Hoy en dia son habituales los discos duros de 80 Gb, 120 Gb o incluso más capacidad. Es evidente que no podemos hacer una copia de todos los ficheros almacenados en ellos, así que deberemos decidir cuales son los ficheros importantes.

Cuándo?

Con que frecuencia debemos hacer copias de seguridad de los datos? Idealmente, deberíamos hacer una copia cada vez que modifiquemos el fichero. Esto es difícil, así que deberemos decidir una cierta frecuencia (dos días, una semana,...) teniendo en cuenta que si perdemos información durante ese período necesitaremos reintroducirla en el sistema.

Dónde?

En que tipo de sistema de almacenamiento vamos a guardar nuestras copias de seguridad? Para un usuario doméstico hay tres tipos de formatos disponibles: CD, DVD o disco USB. Si grabamos los datos en CD deberemos tener en cuenta que su capacidad es de tan solo unos 700 Mb, por lo que tal vez necesitaremos muchos CDs para copiar todos nuestros datos. Es un formato ideal, por ejemplo, para grabar una colección de ficheros MP3, ya que son datos que, en principio, no variarán.

Si los grabamos en DVD dispondremos de mucho más espacio para guardar los datos y, hoy en dia, el precio de una grabadora de DVD ya no es impedimento para su adquisición.

Finalmente, los discos USB habituales disponen de entre 256 Mb y 1 Gb de espacio en caso de que utilicemos los conocidos como *pendrive.* Existen también discos duros externos conectables por USB, en los cuales podemos llegar a disponer de la misma capacidad que en nuestro disco interno y a un precio asequible.

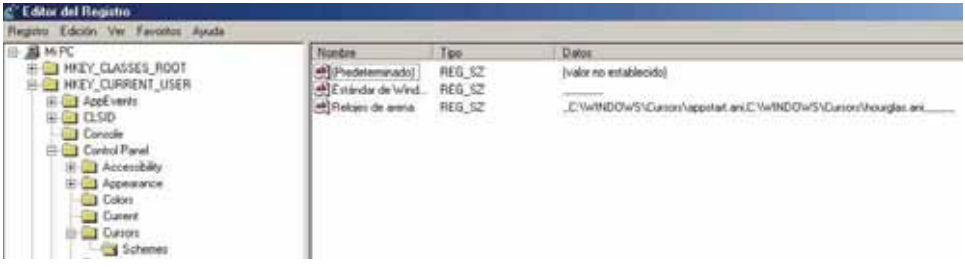
Deberemos escoger, además, donde vamos a guardar estas copias de seguridad una vez realizadas. Idealmente, estarán guardadas en una caja fuerte a prueba de fuego. Esto no suele ser posible en la mayoría de los casos, por lo que deberemos guardarlas en un sitio alejado del ordenador y protegido de posibles robos.

Es muy útil también disponer de un sistema de rotación de las copias, de forma que podamos recuperar no solo la última versión sino, también alguna de las anteriores. Para ello, no debemos sobreescribir los ficheros cada vez que realicemos la copia de seguridad sino que deberemos ir rotando entre diferentes medios según la frecuencia que nos interese. Por ejemplo, si realizamos las copias diariamente en CD regrabables podemos disponer de un CD regrabable para cada día de la semana, convenientemente etiquetado. Así, si lo necesitamos seremos capaces de recuperar datos de hasta una semana de antigüedad, lo cual puede ser útil en caso que hayamos hecho modificaciones en algún fichero y no podamos recuperar los datos originales.

El registro de Windows

Mucha de la información necesaria para el funcionamiento de Windows se guarda en el registro. El registro es una base de datos donde se centraliza la configuración del sistema, del hardware del que disponemos y de muchas aplicaciones. En las versiones antiguas de Windows esta información se guardaba en ficheros de texto (normalmente, con extensión INI) y cada aplicación los guardaba en diferentes directorios, lo que complicaba buscar el que nos interesaba para modificarlo. A partir de Windows 95 se implementó este nuevo sistema que permite editar los datos que contiene desde un único sitio.

El registro está organizado en una serie de carpetas y subcarpetas donde se almacenan las claves y el valor que tienen. Esta estructura lógica es muy parecida a un sistema de ficheros, donde las claves se corresponden a los nombres de los ficheros y los valores al contenido de ese fichero. De ese modo, podemos acceder al valor de una clave navegando hasta la subcarpeta donde está la clave y visualizando su valor.



Para poder editar el registro disponemos de dos herramientas, regedit.exe y regedt32.exe, aunque es bastante peligroso editar directamente el registro, ya que corremos el riesgo de equivocarnos, modificandolo de forma que podemos dejar el sistema en un estado

inestable o incluso inservible, llegando a tener que reinstalar el sistema operativo. Existe el riesgo, además, de que el registro quede corrupto, ya sea a causa de un programa defectuoso o de un apagado incorrecto de nuestro ordenador, de forma que no sea posible recuperarlo. Por ello, es adecuado realizar copias de nuestro registro habitualmente. Para hacerlo podemos utilizar ERUNT, que nos permite realizar una copia de todo el registro y posteriormente restaurarlo desde DOS o desde la Consola de Recuperación de Windows. Este programa nos permite planificar copias diarias del registro de forma que podemos volver a estados anteriores cuando lo necesitemos.

Del mismo autor es NTREGOPT, que permite optimizar el espacio que ocupa nuestro registro. Cuando instalamos y desinstalamos muchos programas se crean y se borran claves en el registro, pero el espacio que ocupan estas claves puede no recuperarse totalmente. NTREGOPT funciona creando un nuevo registro que contiene solo las claves existentes sin el espacio vacío que hayan podido dejar las borradas, aprovechando mejor el espacio en disco que ocupa el registro.

Otra causa de problemas en el registro son los programas que crean claves en él que después no son borradas. Esto provoca que el registro se llene de claves repetidas o innecesarias. Existen diversos programas que nos permiten la limpieza del registro, como Easy Cleaner, aunque debemos tener especial cuidado con el uso de estos programas porque podemos borrar sin querer claves que son necesarias para el buen funcionamiento de nuestro ordenador.

Finalmente, existen toda una serie de "trucos" que podemos aplicar a nuestro ordenador para cambiar alguna de sus funcionalidades a través de modificaciones en el registro. Hay una lista bastante completa de estas modificaciones en Winguides.

Borrado seguro de datos

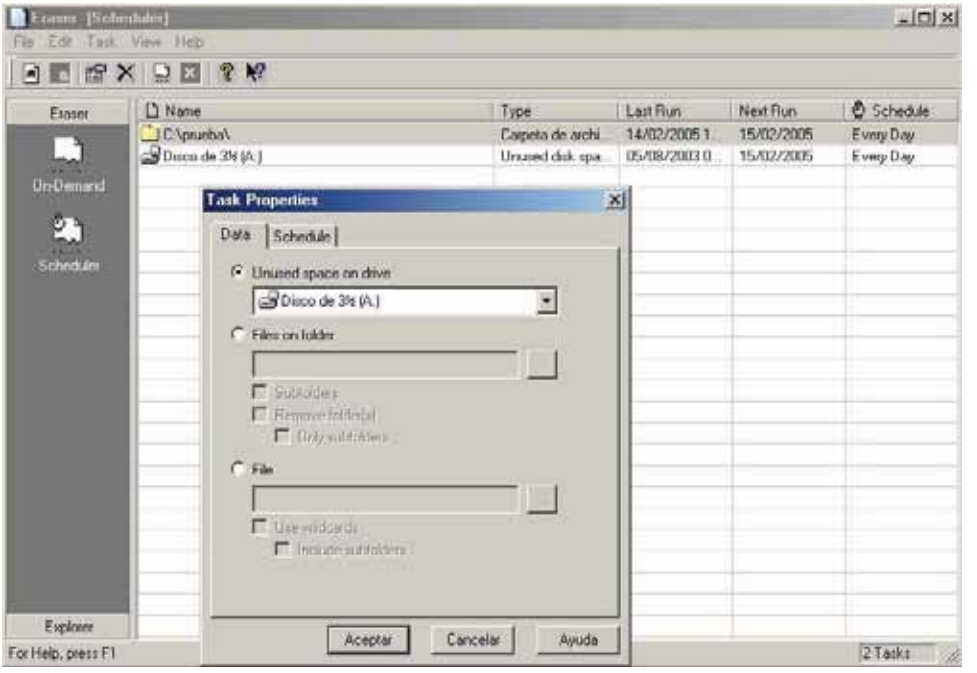
Muchas veces no nos planteamos la cantidad de información que podemos estar proporcionando en cualquier momento. Por ejemplo, en el momento de vender nuestro ordenador, un disco duro o de lanzar un disquete o un CD a la basura nos estamos arriesgando a que nuestros datos estén a disposición de quien quiera (y pueda) leerlos. Según un estudio hecho por dos estudiantes del MIT, la mayoría de discos duros que se venden a través de eBay contienen información privada del vendedor. De los 158 discos que compraron, 69 contenían ficheros recuperables y 49 contenían ficheros con información personal (cartas de amor, números de tarjetas de crédito, pornografía.)

Podemos pensar que un simple formateo del disco duro impedirá que los datos almacenados en este puedan ser recuperados, pero resulta bastante sencillo recuperar archivos que hayan sido borrados de un disco y algunos programas permiten deshacer el formateo de una determinada unidad.

Existen incluso métodos para recuperar los datos de los discos aunque estos hayan sido sobreescritos. Aunque las técnicas para conseguir extraer esa información no están al alcance de cualquiera, podemos localizar diversas empresas especializadas en recuperación de datos a través de Internet que disponen de las herramientas para ello. Esto nos puede ser útil en el caso que se estropee alguno de nuestros discos o hayamos borrado alguna información y no tengamos copia de seguridad de los datos. Hay que tener en cuenta que la tarifa que cobran por estos servicios es considerablemente elevada por lo que solo será una opción a tener en cuenta si los datos son realmente importantes y necesarios.

Si queremos asegurarnos de no estar distribuyendo información privada debemos sobreescribir los datos de forma que no sea posible recuperarlos de ningún modo. Para ello, es necesario realizar diversas pasadas de escritura sobre cada uno de los sectores donde se almacena la información, algunas con datos aleatorios y otras con datos fijos.

Para simplificar la tarea lo más sencillo es utilizar algún programa como Eraser o un disco de arranque como DBAN, que nos permitirán eliminar la información de forma sencilla.



Eraser nos permite borrar ficheros individuales, carpetas completas y/o el espacio sin usar de cualquier unidad de disco. Además, también permite programar la tarea para que se realice con una determinada frecuencia, con lo que no tendremos que preocuparnos de tener información comprometida en algún lugar de nuestro ordenador.

De todas formas, si la información que contiene nuestro disco es muy importante y queremos asegurarnos de que nadie pueda acceder a ella, lo mejor es destruir fisicamente ese disco. Para ello, deberemos abrir el disco duro y asegurarnos de destruir los platos que contiene de forma que no puedan ser leídos, por ejemplo, sumergiéndolos en ácido o destruyéndolos en una fundición. Esta es la mejor solución hoy en día; teniendo en cuenta el precio de un disco duro, si este contiene datos realmente confidenciales no merece la pena arriesgarse por el poco dinero que podemos obtener en su venta.

También deberíamos asegurarnos de que los disquetes o los CDs que lanzamos a la basura no puedan ser leídos por nadie si contienen datos confidenciales. Para los disquetes podemos seguir el mismo método que con el disco duro o simplemente abrir la carcasa de plástico, extraer el disco magnético de su interior y cortarlo en trozos lo más pequeños posible. Para destruir los CDs podemos envolverlos con un trapo o un papel y romperlos en trozos pequeños. Si hacemos estos, debemos procurar no tirar todos los trozos en la misma basura para dificultar aun más su posible recuperación.

Protección ante la copia de datos en discos USB

En un domicilio particular será un poco extraño, pero en un empresa es habitual que haya un ordenador que contenga datos confidenciales y que no deben salir de ese ordenador (nóminas, facturación, planos, diseños industriales...) Si estos datos son importantes es de suponer que se habrán tomado medidas para que nadie pueda copiarlos, como por ejemplo, no conectar ese ordenador a la red, desactivar la disquetera, no dar permiso a los usuarios para utilizar la grabadora de CDs (de alguna manera habrá que hacer copias de los datos, pero nunca deberá hacerlas un simple usuario).

Pero no debemos pasar por alto un detalle, la aparición de discos duros que se conectan a través del puerto USB. Estos discos tienen una gran capacidad de almacenamiento (128, 256, 512 Megabytes e incluso superiores) y no tenemos ningún mecanismo para evitar que alguien pueda conectarlos a ese ordenador y utilizarlos (aparte de desactivar fisicamente los puertos USB, cosa que no es posible en muchas placas base).

Si disponemos de Windows 2000 o Windows XP existen un par de soluciones sencillas, la primera en caso de que no se haya instalado aun ningún disco de este tipo y la segunda en caso de que ya se haya instalado alguna vez.

Si no se ha instalado ningún disco USB

Debemos quitar todos los permisos a los ficheros:

```
c:\windows\Inf\Usbstor.pnf
c:\windows\Inf\Usbstor.inf
```

Para ello iremos a las propiedades del fichero y en la pestaña *Seguridad* denegamos todos los permisos para todos los usuarios.

Si ya se ha instalado algún disco USB

Debemos editar el registro de Windows y buscar la siguiente carpeta:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
```

y editar la clave Start para ponerle el valor 4.

En caso de que queramos una solución más general existe un programa llamado DeviceLock que nos permitirá controlar que usuarios pueden acceder a cada tipo de dispositivo y no permitirá el uso de dispositivos externos (tanto USB como Firewire u otros).

Referencias

Artículo sobre la información encontrada en discos duros usados
http://news.bbc.co.uk/1/hi/technology/2676461.stm

Diferencias entre regedit y regedt32
http://support.microsoft.com/default.aspx?kbid=141377

Dirección de descarga de ERUNT y NTREGOPT
http://home.t-online.de/home/lars.hederer/erunt/index.htm

Dirección de descarga de EasyCleaner
http://personal.inet.fi/business/toniarts/ecleane.htm

Modificaciones del registro de Windows
http://www.winguides.com/registry/

Dirección de descarga de Eraser
http://www.heidi.ie/eraser/default.php

Dirección de descarga de DBAN
http://dban.sourceforge.net/

Dirección de descarga de DeviceLock
http://www.protect-me.com/dl/

Cómo desactivar el uso de discos USB
http://support.microsoft.com/default.aspx?scid=kb;en-us;823732

[Capítulo 6]

Seguridad física

Keyloggers

Una manera de capturar las teclas que se pulsan en un ordenador es instalando un *keylogger*. Este es un sistema que registra todas las teclas que pulsamos, de forma que, posteriormente, podrán ser leídas por el atacante, ya sea directamente en el ordenador o bien enviadas de forma remota (p.ej. por correo electrónico). De esta forma, ni tan solo es necesario el acceso físico a nuestro ordenador para obtener los datos.

Esto permite a un atacante leer todos los datos que introducimos, tales como contraseñas, números de cuenta bancaria, correos, conversaciones en chats, etc... Es evidente el alto riesgo que esto supone para nuestra seguridad y para nuestra privacidad.

Existen dos tipos de *keyloggers*:

- los basados en hardware, como por ejemplo *KeyGhost*. Estos se conectan entre el teclado y el ordenador, por lo que el atacante necesitará disponer de acceso físico a nuestro sistema, tanto para instalarlo como para recuperar los datos.

- los basados en software, como *Ghost Keylogger*, que se instalan como cualquier otro programa. Suelen incorporar muchas características, como el envío automático de los datos al atacante, la realización de capturas de pantalla a intervalos regulares,...

Detectar este tipo de programas puede resultar bastante difícil, ya que suelen utilizar técnicas para ocultarse y no ser descubiertos. Además, algunos virus y *spyware* llevan incorporados *keyloggers* para poder robar información del usuario.

Para detectar los que están basados en software podemos utilizar programas como *KL-Detector* o *Anti-Keylogger*, que se basan en detectar si algún archivo crece de forma continuada cuando pulsamos teclas. De esta forma, pueden saber si algún programa está guardando las pulsaciones que realizamos en nuestro teclado. Los *keyloggers* hardware no pueden ser detectados por software, así que necesitaremos comprobar que nuestro teclado está conectado directamente al ordenador y no con algún artilugio desconocido entre ellos.

ATENCIÓN

No siempre el uso de un *keylogger* tiene que ser perjudicial. Podemos utilizarlo como un sistema de copias de seguridad de todo aquello que escribimos, lo cual puede ser muy útil para escritores, estudiantes realizando un trabajo o cualquiera que tenga que escribir grandes cantidades de texto.
Lo importante es que seamos nosotros quienes lo hayamos instalado y seamos conscientes de que está instalado y registrando nuestra actividad.

Ordenadores portátiles

En caso de que dispongamos de un ordenador portátil deberemos tener más precauciones con él que con un ordenador de escritorio, pues este es más vulnerable.

En primer lugar, deberemos tomar las medidas adecuadas para que el ordenador no pueda ser robado. La primera medida básica para esto es no perder nunca de vista el ordenador, a no ser que esté en un lugar completamente seguro. En caso de que estemos en un lugar poco seguro, deberemos intentar alejarnos lo menos posible de él. Si estamos en algún lugar público donde sean frecuentes los robos, no deberemos soltarlo nunca, llegando, si es necesario a llevarlo colgado al cuello y cruzado, de forma que no nos lo puedan quitar por el método del tirón.

Cuando estemos trabajando con él en algún lugar público o semi-publico podemos optar por utilizar cables de seguridad, como los de tipo *Kensington*. Estos cables son de acero y permiten amarrar el portátil a la mesa, de forma que nadie podrá llevarse el ordenador, existiendo modelos que incorporan alarma para avisarnos de un intento de robo. Para ello, es necesario que el portátil disponga de la correspondiente ranura para acoplar este tipo de cables, aunque hoy en día es habitual que la mayoría lo incorporen.

Para el caso de que perdamos o nos roben el portátil será útil que hayamos realizado unas cuantas acciones preventivas, tanto para impedir el acceso a los datos por parte del ladrón como para disponer nosotros de esos datos. En primer lugar, es más que aconsejable tener activada la contraseña tanto de arranque como la del sistema operativo. Esto detendrá, como mínimo al ladrón inexperto, pero no evitará que alguien con conocimientos acceda al ordenador. Por ello la mejor opción es guardar todos nuestros datos cifrados, existiendo multitud de programas que realizan esta función e incluso algunos que vienen con el propio sistema operativo. No debemos confiar en la protección que nos puedan ofrecer los programas de ofimática (Word, Excel,...) cuando guardamos los ficheros con contraseña, ya que estas son fáciles de descubrir.

Idealmente, guardaremos también todos nuestros datos en un sistema aparte, ya sea almacenándolos externamente a través de Internet o bien mediante un disco duro USB que mantendremos alejado del ordenador cuando no estemos utilizándolo para evitar que nos roben los dos simultaneamente.

Además, debemos estar preparados para poder hacer una denuncia. Para ello, tendremos apuntado el fabricante, el modelo y el número de serie de nuestro ordenador, además de guardar copia de la factura de compra. De este modo, podremos realizar fácilmente la denuncia ante la policía y, en caso, de que el ordenador sea encontrado podremos recuperarlo mucho más rápidamente al poder aportar pruebas de que el ordenador es realmente nuestro.

Es importante realizar cuanto antes la denuncia a la policía en caso de robo, pues puede llegar a facilitar mucho la recuperación de nuestro portátil y de la información que contiene.

Seguridad en una red desconocida

Si disponemos de un portátil y nos desplazamos frecuentemente con él, es fácil que necesitemos conectarnos a la red interna del sitio donde estemos (trabajo, universidad...) Debemos tener en cuenta, en ese caso, tanto la seguridad de nuestro portátil como la de la red donde vamos a acceder.

Siempre que nos conectemos a una red desconocida o poco confiable debemos asegurarnos de tener activo nuestro cortafuegos, con todos los puertos posibles cerrados al exterior. Además, tendremos que asegurarnos que el cortafuegos está configurado para protegernos de ataques desde esta red, ya que a veces estos, por defecto, solo nos protegen de ataques procedentes de Internet. Es importante también que no tengamos activado la compartición de ficheros de Windows si no la necesitamos y, en caso de que esta sea necesaria, debemos protegerla con una buena contraseña.

Además, nunca debemos acceder a servicios inseguros (cualquiera que envíe nuestra contraseña sin cifrar a través de la red, como POP3 o FTP) cuando estemos en una red no confiable, ya que es muy sencillo para un atacante ver todos los datos que circulan por esta red. Lo mejor en estos casos será acceder solo a servicios que funcionen a través de SSL, como HTTPS o POP3 + SSL.

También es importante tener en cuenta la seguridad de la red donde accedemos. Por ello, debemos comprobar siempre que nuestro ordenador no está infectado con un virus o un gusano que pueda entrar en esta red e infectar al resto de ordenadores, además de procurar no saturar el ancho de banda disponible con transferencias de grandes ficheros si no es imprescindible, como detalle de cortesía hacia los demás usuarios de esa red.

Redes inalámbricas

Desde hace un tiempo las redes inalámbricas se están poniendo de moda debido a la facilidad de instalación de estas y la comodidad de no tener que instalar cable hasta cada uno de los ordenadores que queremos conectar.

El problema de este tipo de redes es su falta de seguridad, al estar el medio físico por el que viajan los datos al alcance de todo el mundo; es decir, cualquiera, tan solo situándose en la zona de cobertura de la red inalámbrica puede escuchar lo que se está transmitiendo. Por lo tanto, solo debemos poner nuestra tarjeta de red inalámbrica en modo *escucha* y darnos un paseo por la calle para encontrar cientos de redes inalámbricas desprotegidas y de fácil acceso.

Para solucionar este problema se propuso el estándar WEP (*Wired Equivalent Privacy*) que transmite los datos cifrados a través de la red. Pero este protocolo es demasiado débil y está mal diseñado, por lo que resulta realmente sencillo descubrir cual es la clave que se utiliza y, por tanto, acceder a la red y registrar los datos que circulan por ella. Existen incluso programas que lo hacen de forma automática y muy sencilla, como Airsnort.

Por ello, se han propuesto otros protocolos como WPA (*Wi-Fi Protected Access*) que mejoran la seguridad de WEP, aunque tampoco son infalibles. Es por ello que debemos tomar una serie de precauciones al instalar una red inalámbrica:

- Activar siempre el protocolo WPA o, en su defecto, el protocolo WEP. Aunque estos sean débiles es mejor tenerlos activados para dificultar la tarea a un posible atacante.

- Activar el filtrado por MAC (la dirección física de la tarjeta de red inalámbrica), de forma que solo puedan conectarse al punto de acceso aquellas tarjetas a las que nosotros demos permiso.

- Usar un sistema de autenticación, como NoCatAuth.

- Usar antenas que emitan solo en la dirección que nos interesa.

- A ser posible, separar completamente la red inalámbrica del resto de la red. Instalar un cortafuegos y dar permiso solo a aquello que necesitemos.

ATENCIÓN

El desarrollo de la banda ancha y las tecnologías inalámbricas han propiciado la aparición de comunidades conectadas a través de este tipo redes, a veces ofreciendo servicios propios y otras simplemente conexión a Internet.
Si nos interesa el tema podemos ponernos en contacto con la comunidad de nuestra ciudad, donde nos informarán oportunamente.

Algunos ejemplos de estas comunidades:

http://www.barcelonawireless.net
http://www.madridwireless.net
http://www.zaragozawireless.org

Referencias

Keylogger basado en hardware
http://www.keyghost.com/

Keylogger basado en software
http://www.keylogger.net/

Dirección de descarga de KL-Detector
http://dewasoft.com/privacy/kldetector.htm

Dirección de descarga de AntiKeylogger
http://www.anti-keylogger.net/

APÉNDICE A: Cómo desinstalar completamente Explorer y Outlook

Internet Explorer y Outlook Express son dos de los componentes más temidos de Windows, al ser la mayor puerta de entrada a virus, gusanos, spam y demás basura que puebla Internet.

Aunque es una operación complicada y peligrosa, tenemos la opción de desinstalarlos completamente de nuestro sistema. No es recomendable realizar este proceso si no sabemos muy bien lo que estamos haciendo, pues existen muchas probabilidades de dejar nuestro sistema inservible. Si a pesar del aviso queremos desinstalarlos debemos saber que existen dos maneras de realizar la operación, una sencilla y una complicada.

La sencilla consiste en adquirir el programa XPLite. Este nos automatizará toda la tarea, además de permitirnos desinstalar muchas otras cosas como servicios innecesarios, drivers inútiles, DirectX... El inconveniente es que el programa es de pago, pero ofrece una versión de prueba gratuita. La complicada consiste en borrar nosotros a mano los ficheros y claves del registro necesarios.

Desinstalación de Outlook.

Borramos del registro las siguientes claves:

```
HKEY_LOCAL_MACHINE/Software/Microsoft/Outlook Express
HKEY_LOCAL_MACHINE/Software/Microsoft/WAB
HKEY_CURRENT_USER/Identities
HKEY_CURRENT_USER/Software/Microsoft/Outlook Express
HKEY_CURRENT_USER/Software/Microsoft/WAB
```

```
HKEY_LOCAL_MACHINE/Software/Microsoft/Active Setup/
      Installed Components/
      {44BBA840-CC51-11CF-AAFA-00AA00B6015C}
HKEY_LOCAL_MACHINE/Software/Microsoft/Active Setup/
      Installed Components/
      {7790769C-0471-11D2-AF11-00C04FA35D02}
```

Borramos del directorio `c:\windows\system32\dllcache` los ficheros:

```
Inetcomm.dll
Msoeacct.dll
Msoert2.dll
Msoe.dll
Msoeres.dll
Msimn.exe
Oeimport.dll
Oemiglib.dll
Oemig50.exe
Setup50.exe
Wab.exe
Wabfind.dll
Wabimp.dll
Wabmig.exe
Csapi3t1.dll
Directdb.dll
Wab32.dll
Wab32res.dll
```

Estos son copias de seguridad que hace Windows para poder restaurarlos.
Ahora debemos borrar los mismos ficheros que en el paso anterior pero en sus directorios originales. La mejor forma de encontrarlos es mediante la función de Buscar ficheros. Cuando intentemos borrarlos, Windows nos pedirá que introduzcamos el CD original para poder restaurarlos. Nosotros le decimos que no queremos restaurarlo y continuamos con el proceso.

Desinstalación de Internet Explorer.

El proceso a utilizar es muy similar al anterior, cambiando simplemente los ficheros a borrar. En primer lugar borramos `c:\windows\ system32\dllcache\iexplore.exe` y después borramos `c:\Archivos de Programa\Internet Explorer\ iexplore.exe`.

Este proceso ha sido probado en un sistema con Windows 2000 y ha funcionado correctamente. De todas maneras, no es recomendable realizarlo si no estamos muy seguros de lo que estamos haciendo.

Referencias

OLEXP: Cómo quitar y volver a instalar manualmente Outlook Express
http://support.microsoft.com/default.aspx?scid=KB;ES-ES;Q263837&

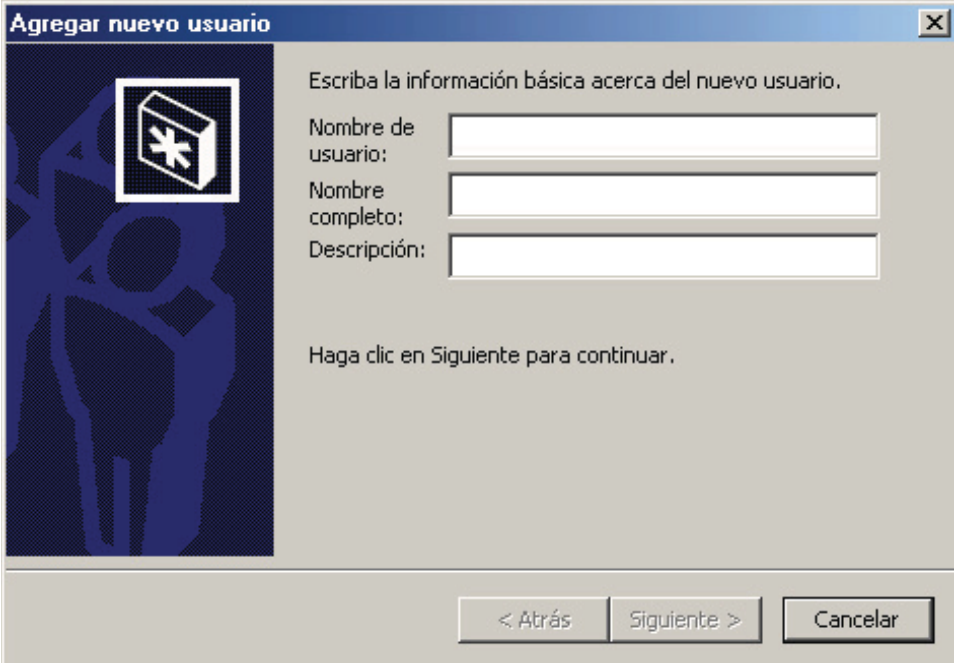
Como desinstalar Internet Explorer 6
http://support.microsoft.com/kb/293907/es

Cómo desinstalar Internet Explorer 5
http://support.microsoft.com/kb/217344/es

APÉNDICE B: Creación de diversos usuarios

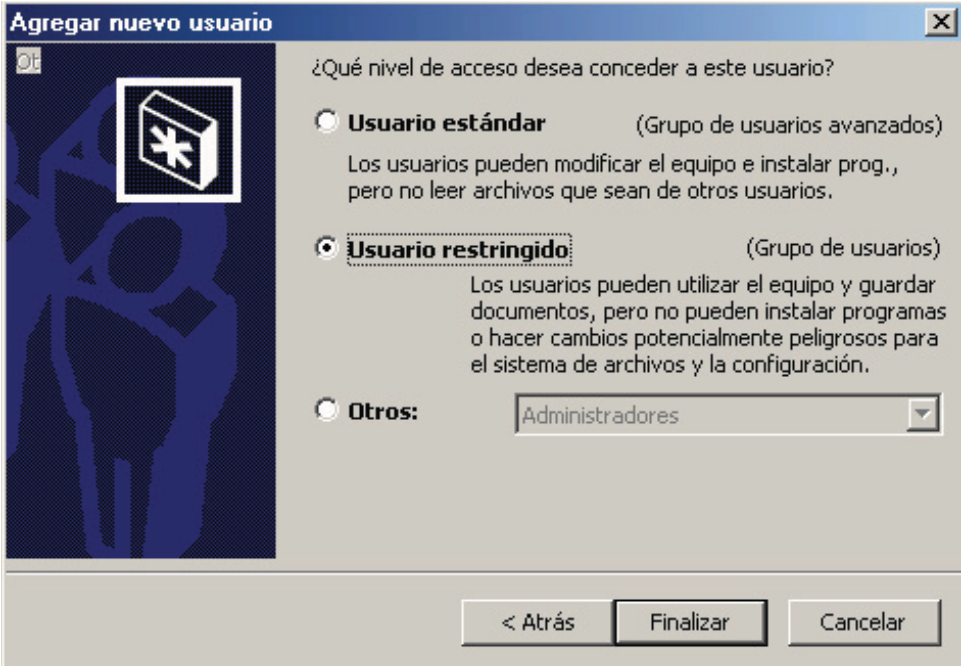
Una de las razones por las que existen tantos problemas de seguridad en los sistemas con Windows instalado es que este, por defecto, nos crea un usuario con permisos de Administrador, es decir, un usuario con permiso para hacer cualquier cosa en el ordenador: instalar programas, borrar ficheros,...

Esto facilita a cualquier virus o *spyware* la instalación en nuestro sistema, pues es capaz de sobreescribir los ficheros necesarios para instalarse. Para evitar esto podemos crear otros usuarios con los que trabajaremos de forma habitual, utilizando el usuario Administrador solo cuando sea imprescindible, por ejemplo para instalar programas.



Para crear otro usuario iremos a la opción *Usuarios y contraseñas* del *Panel de control.* Allí le indicaremos que queremos agregar un nuevo usuario, proporcionándole el nuevo nombre de usuario y la contraseña.

Posteriormente, el sistema nos pedirá que tipo de usuario queremos crear. Le indicaremos que queremos un Usuario restringido, de este modo habremos creado un usuario que no será capaz de modificar la configuración del sistema y que estará más protegido ante virus y otros programas malignos.



En caso de que necesitemos instalar algún programa o algún tipo de hardware, deberemos iniciar la sesión con el usuario Administrador o con algún otro que tenga permisos de Administrador y una vez lo tengamos instalado cerraremos la sesión y utilizaremos el usuario restringido.

Referencias

Por qué no debe trabajar en el equipo como administrador
http://www.microsoft.com/windows2000/es/professional/help/windows_security_whynot_admin.htm