BIBLIA DE LOS TRUCOS PARA WINDOWS E INTERNET.

By Ozharu & Sansuito

-ELIMINAR WINDOWS MESSENGER
Si no utilizas el Messenger seguramente querrás eliminarlo del sistema. La forma más sencilla de hacerlo es pulsado en el botón de inicio -> ejecutar:
RunDll32 advpack.dll,LaunchINFSection %windir%\INF\msmsgs.inf,BLC.Remove

Trucos para buscar en Google:

-Buscar serial en Google = **94fbr Mas Nombre del Programa en Google**

- Si quieres buscar una frase exacta, introdúcela entre comillas (""). Por ejemplo:
"diarios deportivos"

- Para encontrar páginas que incluyan determinadas palabras, pero no otras, deberemos incluir el signo '-' delante de las que no queremos buscar. Por ejemplo, para descubrir webs que incluyan la palabra 'tienda', pero no la palabra 'online': **tienda -online**

- Si pretendemos encontrar una determinada palabra u otra, usaremos 'OR' (o bien el símbolo '|' (AltGr+1). Por ejemplo, para buscar webs de en los que aparazca 'tienda' y 'zapatos', o bien:
'tienda' y 'pantalones':
tienda (zapatos OR pantalones)
tienda (zapatos | pantalones)

- Hay numerosas palabras (en español: 'a', 'de', 'el', ...; en inglés: 'to', 'of', 'the',...) que Google no tiene en cuenta en sus búsquedas, a no ser que lo indiquemos. Para ello, escribiremos el signo '+' delante de estas palabras. Por ejemplo, estas dos búsquedas no generan los mismos resultados:
el mundo
+el mundo

- Se puede hacer uso de comodines. Esto es, el símbolo '*' puede ser usado para sustituir a una palabra, y facilitar algunas búsquedas. Por ejemplo:
"los * años"
"los * * años"

- No es necesario distinguir las mayúsculas de las minúsculas. Estas dos búsquedas generan los mismos resultados:
Crtl+

- A: Abrir
- B: Buscar
- C: Copiar
- E: Seleccionar todo
- G: Guardar
- I: Ir a
- L: Reemplazar
- P: Imprimir
- U: Nuevo
- V: Copiar
- X: Cortar
- Y: Repetir
- Z: Deshacer

Datos personales a través de Internet

Cuando ofrezcan datos personales a través de Internet que se encuentren en una web cifrada aquellas cuya dirección comienza por https:// (y no http:// como habitualmente) y que tienen en la parte inferior de la ventana del explorador el icono de un candado cerrado.

Windows XP tiene un programa espia que permite a Microsoft seguir el rastro de un equipo en su sitio web.

Es un control ActiveX que le permite leer el HWID (Hardware ID) así como el MSID (Microsoft ID) del equipo lo cual permite a Microsoft conocer sus movimientos en su sitio.

Para eliminarlo, puede seguirse los siguientes pasos:

1.- Pulsar en "Menu Inicio" -> "Ejecutar..."
2.- Escribir en la caja de dialogo lo siguiente en función de la versión de Windows:

Para XP HOME EDITION
"regsvr32.exe -u c:\windows\system32\egwizc.dll"

Para XP Profesional
"regsvr32.exe -u c:\winnt\system32\egwizc.dll"

3.- Hacer clic sobre OK para validar. Se visualizará una ventana con:
"DllUnregisterServer en c:\windows\system32\egwizc.dll con éxito".

DESACTIVAR REINICIO AUTOMATICO

Windows XP al igual que Windows 2000, al producirse un error reinicia de forma automática el ordenador pero si por cualquier razón quieres desactivar dicha caracteística debes hacer lo siguiente:

Pulsa el botón Inicio luego Panel de control y seguidamente Sistema. Debes abrir la pestaña "Opciones avanzadas" y luego haz clic sobre Configuración. En la opción "Reiniciar automáticamente" desmarca esa casilla. Haz clic sobre Aceptar y de nuevo sobre Aceptar. A partir de ahora no solo no se reiniciará al producirse un error, sino que también tendrás la oportunidad de conocer un poco más sobre su causa y solucionar el problema que realmente ha hecho que Windows XP reinicie sin permiso tu PC.

CAMBIAR LA CLAVE DE INSTALACION DE WINDOWS XP

Durante la instalación de Windows XP, nos solicitarán lo siguiente: que le facilitemos la clave que verificará la autenticidad del producto. Teniendo en cuenta que cada clave de instalación del Win XP, irá asociada mediante el Windows Product Activation al hardware de la máquina, podemos encontrarnos ante la necesitad de realizar el cambio de la clave de instalación de nuestro Windows XP, previa a la activación del producto. En este supuesto, no se hará necesaria la reistalación de Windows XP. Podemos operar de la siguiente manera:

- Activamos Windows en el menú de Inicio.
- Seleccionamos la opción Teléfono.

- Pulsamos sobre "Cambiar clave de producto".
- Introducimos la nueva clave.
- Pulsamos sobre Actualizar.
- Al termino de estos pasos, ya solo nos falta activar el producto

Para borrar la clave anterior (si no funciona):

1. Ejecutar regedit y buscar la clave **HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\WPAEvents**
2. Abrir la clave oobetimer, borrar el valor hexadecimal CA, y cerrar regedit
3. Ir a Inicio, Ejecutar y escribir %systemroot%\system32\oobe\msoobe.exe /a
4. Nos aparecerá la pantalla de activación de Windows XP, seleccionar activación por teléfono, pulsar en Cambiar clave del producto e introducir la nueva clave y pulsar actualizar. (Las claves que comienzan por F o D han sido baneadas por Microsoft en el SP1)
5. Ejecutar de nuevo %systemroot%\system32\oobe\msoobe.exe /a, y con esto finalizará el proceso de activación.

PROGRAMAR EL APAGADO DE WINDOWS XP

Podemos apagar de una forma remota nuestro equipo, creando un archivo "apagadorremoto.js". Teniendo por contenido el siguiente texto:

(new ActiveXObject("Shell.Application")).ShutdownWindows();.

Seguidamente lo guardamos en donde nos parezca más oportuno. De este modo, podemos apagar nuestro equipo con solo hacer doble clic sobro el archivo creado con anterioridad. Pero también podemos programar el apagado de nuestro equipo con la siguiente utilidad: **Shutdown -t xx**

Teniendo en cuenta que xx es el tiempo en segundos que transcurre asta que se apaga nuestro equipo. Con buena lógica, esta opción se queda un poco coja, pues de este modo solo disponemos de un margen de maniobra de asta 99 segundos.

Para lograr que esto aumente podemos acudir al Programador de tareas indicando seguidamente la hora y el día en que queremos que se ejecute.

PROBLEMAS CON EL APAGADO DEL WINDOWS

Parece ser que en muchos equipos ATX en los que versiones anteriores de Windows apagaban automáticamente el sistema, en Windows 2k/XP no lo hacen, mostrando el mensaje "Ahora puede apagar el sistema" o incluso reiniciando en vez de apagarse, cuando en sistemas anteriores (Windows 9x-Me) lo hacía correctamente. Una posible solución a ese problema la encontraremos en el registro de Windows, hacemos clic en el botón inicio y luego en Ejecutar, escribimos regedit y pulsamos el botón Aceptar. Una vez se abra el registro nos desplazaremos por la siguiente clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

donde comprobaremos que el contenido de los valores alfanuméricos "PowerDownafterShutdown" y "ShutdownWithoutLogon" sea "1" y de lo contrario cambiaremos el valor por éste último. También revisaremos en la clave **HKEY_CURRENT_USER\Control Panel\Desktop** la existencia del valor alfanumérico "PowerOffActive" cuyo contenido deberá ser "1".

Si esto no soluciona el problema, iniciaremos la herramienta de administración del sistema, pulsando con el ratón derecho sobre Mi PC y seleccionando Administrar.

Dentro del administrador de dispositivos, comprobaremos que en en el apartado "Equipo" aparezca "Equipo ACPI compatible", "Equipo compatible con Advanced Configuration and Power Interface (ACPI), o "PC Estándar APM". En este último caso, dentro del menú Ver, seleccionaremos mostrar dispositivos ocultos y nos aseguraremos de que el elemento "NT ATM / Legacy Interfaz mode" no tenga un aspa roja, en cuyo caso tendríamos que acceder a sus Propiedades y habilitar el dispositivo.

Por último, comprobaremos que en las propiedades de energía, dentro del panel de control, en la pestaña "APM" se encuentre activada la opción:
"Habilitar la compatibilidad con la administración avanzada de energía".

CAMBIAR LA RESOLUCION DE PANTALLA CON UN DOBLE CLICK

Este truco te será muy últil en caso de que algún programa te pida que configures la pantalla con otro resolución distinta a la que hablitualmente utilizas, todo de forma mas rápida que si entraramos en las Propiedades de Pantalla.

El truco consistirá en realizar una llamada a: DESKCP16.DLL, pasándole los parámetros:
QUICKRES_RUNDLLENTRY
RHxRVxPC.
QUICKRES_RUNDLLENTRY: Indicamos a la DLL que queremos cambiar la resolución de la pantalla.
RH: Ancho (ej: 800)
RV: Alto (600)
PC: Profundidad del color en bits (ej. 32)
La llamada se realiza mediante RUNDLL.EXE, por lo tanto podemos crear un acceso directo e indicarle que tiene que ejecutar:
RUNDLL.EXE DESKCP16.DLL,QUICKRES_RUNDLLENTRY 800x600x32

Con el ejemplo anterior crearíamos un acceso directo que nos cambiaría la resolución de la pantalla a 800x600 y 32 bits de profundidad del color.

Como el cambio se realiza de una forma inmediata y sin pedir confirmación, busca en el manual de tu tarjeta gráfica y monitor las resoluciones que soportan

REINICIAR CON UN DOBLE CLICK

Para crear un acceso directo en el Escritorio y reiniciar el ordenador con doble clic debes seguir estos pasos:

Haz clic con el ratón derecho en una zona libre del Escritorio, selecciona Nuevo y Acceso directo.
Luego escribe shutdown.exe -r -t 00 y pulsa el botón Siguiente, escribe el nombre que quieras darle al acceso directo y clic en Finalizar.
A partir de ahora cada vez que hagas doble clic sobre dicho icono se reiniciará tu ordenador.
También puedes establecer un tiempo de espera antes de reiniciar, para que te de tiempo a cerrar los programas que tengas abiertos en este caso lo que debes poner es: shutdown.exe -r -t 12 siendo 12 los segundos que esperará para reiniciar.

BORRAR LOS DOCUMENTOS COMPARTIDOS DE MI PC

Para quitar de Mi PC la opción Documentos Compartidos debes seguir estos pasos:

Haces clic en el botón Inicio luego en Ejecutar y escribe Regedit, luego pulsa el botón Aceptar. Ahora vas a la rama del registro.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ MyComputer\NameSpace\Delegate Folders

Allí localizamos la rama {59031a47-3f72-44a7-89c5-5595fe6b30ee} y la borramos Reiniciar la PC.

QUITAR LAS FLECHAS DE LOS ICONOS DE ACCESO DIRECTO

Para quitar las flechitas a los iconos de acceso directo, solo teneis que seguir estos pasos:

- Haz clic en el botón "Inicio" y a continuación sobre "Ejecutar", escribe "Regedit" y pulsa el botón Aceptar.Una vez estés en el Registro debes desplazarte por la siguientes claves y borrar el valor IsShortCut de las dos claves:

HKEY_CLASSES_ROOT\lnkfile\IsShortCut
HKEY_CLASSES_ROOT\piffile\IsShortCut

- Una vez borrados estos valores llamados IsShortCut, bastará con reiniciar la máquina para no ver más esas flechitas.
- Reiniciar el Pc

MEJORAR LAS TRANSFERENCIAS EN RED DE ARCHIVOS

Windows normalmente limitará la cantidad de memoria RAM que el sistema podrá utilizar para las operaciones de entrada y salida de datos en conexiones de red, algo que podemos modificar mediante la edición del registro

La utilidad de este ajuste cuestionable para usuarios que no tengan instalado en el sistema algún tipo de servidor, ya que básicamente este ajuste mejora el rendimiento de entrada/salida del ordenador cuando se están realizando una cantidad grande de transferencias de archivos y operaciones similares.

Este ajuste no hará mucho en sistemas que no tengan grandes cantidades de memoria, pero sistemas con más de 256 Mb de RAM generalmente encontrarán una mejora en el rendimiento estableciendo este valor entre 16 y 32 Mb. El valor por defecto es 0.5Mb (512Kb). Para modificar el ajuste automático en esta configuración, iniciaremos la herramienta de edición del registro de sistema, con el comando “regedit.exe” en el menú Inicio/Ejecutar. Localizaremos la clave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management y crearemos o modificaremos el valor DWORD de nombre ?IoPageLockLimit? (sin las comillas) con un número, cuyo valor será equivalente al máximo de bytes que se utilizarán para las operaciones de entrada y salida, de forma que tendremos que multiplicar el número de megabytes x 1024 x 1024.

NOTA: Modificar este ajuste puede causar problemas de estabilidad con dispositivos de sistema, como problemas relacionados con OpenGL o SCSI, en cuyo caso volveremos al ajuste predeterminado.

MEJORAR EL ANCHO DE BANDA DEL XP PROFESSIONAL

Windows XP se reserva el 20% del ancho de banda disponible, con el fin de ejecutar aplicaciones especiales. La ?retención? se produce mediante el denominado el programador de paquetes QoS (Quality of Service ? Calidad del Servicio), encargado de la optimización de redes locales.

Sin embargo, para los usuarios privados, que sólo tienen un PC en casa, QoS no es una función necesaria; sino todo lo contrario. Windows XP reserva el 20% del ancho de banda aunque el usuario cancele la función QoS. También se puede optar por desintalar el Programador de paquetes QoS si no tenemos ninguna Red Local.

1. Entrar como administrador.
2. Inicio, ejecutar, escribid: gpedit.msc
3. Aparecen las directivas de grupo, id a Configuración de Equipo.
4. Plantillas Administrativas
5. Red (Network)
6. Programador de Paquetes Qos
7. Doble click en Limitar el ancho de banda reservado
8. Habilitarlo y poner el 0% en Límite de Ancho de Banda.
9. Aplicar y Aceptar
10. Id a propiedades red y comprobad que está marcado el Programador de Paquetes Qos.

ACELERAR APAGADO DEL XP

1) Editor de registro. Para ello pinchamos en INICIO -> Ejecutar: "regedit" (sin comillas) y le damos a enter. Entramos luego hasta el nivel **HKEY_CURRENT_USER -> Control Panel -> Desktop** y localizamos allí la clave **"WaitToKillAppTimeout"** y hacemos doble clic sobre ella.
A continuación cambiamos el valor de 20.000 (que ya trae por defecto) por el de 4.000. Ahora, y sin salir del editor, accedemos a **HKEY_LOCAL_MACHINE -> System -> Current Control -> Control**, para localizar de nuevo la clave **"WaitToKillAppTimeout"** y repitiendo la misma operación de antes cambiamos el valor de 20.000 a 4.000.

OPTIMIZAR GESTION DE MEMORIA RAM

Podemos realizar varios ajustes en el registro de Windows para optimizar el subsitema de memoria que utiliza Windows XP

Estos valores se encuentran bajo la clave:
KEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\MemoryManagement
y para su modificación será necesario iniciar la herramienta de edición del registro del sistema, con el comando "regedit.exe" desde el menú Inicio/Ejecutar. Activando el valor DisablePagingExecutive, evitaremos que los archivos ejecutivos de Windows XP sean paginados en el disco duro, consiguiendo que el SO y la mayoría de programas funcionen de forma más suave.

No obstante, para utilizar esta opción nuestro sistema deberá contar con una significativa cantidad de memoria RAM instalada en el sistema (más de 256 Mb) ya que este ajuste consume una parte sustancial de los recursos del sistema. Por defecto el contenido del valor es “0”, y para para activarlo lo cambiaremos a “1”.

ELIMINAR LA CONTRASEÑA DEL ASESOR DE CONTENIDOS DEL IExplorer

Proteger el acceso al asesor de contenidos mediante una clave resultará útil para que ninguno de los usuarios pueda modificar el nivel de seguridad establecido

Sin embargo, ¿qué pasa cuando olvidamos la clave?. Desinstalar y reinstalar Internet Explorer no servirá de nada porque la clave del supervisor del asesor de contenidos se encuentra en el registro. Para eliminarla iniciaremos el editor de registro de Windows, con el comando "regedit.exe" desde el menú Inicio/Ejecutar. Allí localizaremos la clave **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Windows\Current Version\Policies\Ratings,**
donde modificaremos el parámetro "key", que contiene, encriptada, la clave del asesor de contenido. Borrándolo este valor eliminaremos el password.

LIMPIAR ARCHIVO DE INTERCAMBIO AL APAGAR

Por defecto el archivo de intercambio de Windows XP siempre se mantiene en el disco duro, ocupando un espacio que puede sernos de utilidad, sobretodo en entornos de arranque dual

Para modificar este comportamiento, y que su contenido sea eliminado al apagar el sistema, iniciaremos la herramienta de edición del registro de sistema, con el comando “regedit.exe”, desde el menú Inicio/Ejecutar y localizaremos la clave
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\MemoryManagement.
Allí crearemos o modificaremos el valor DWORD “ClearPageFileAtShutdown” cuyo contenido será “1” eliminar el archivo de intercambio al pagar el sistema o “0” para mantenerlo.

MOSTRAR EL COMANDO ENCRIPTAR EN EL MENU CONTEXTUAL

Antaño, pulsando con el botón derecho del ratón sobre un archivo o carpeta mientras pulsábamos la tecla Mayús en particiones NTFS, el menú contextual que aparecía... nos ofrecía la opción de Encriptar y desencriptar el elmento. Sin embargo esta opción ha desaparecido, aunque solo en principio ya que si iniciamos la herramienta de edición del registro del sistema (“regedit.exe”) a través del menú Inicio/Ejecutar y localizamos la clave
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced,
comprobaremos que creando un nuevo valor de tipo DWORD llamado "EncryptionContextMenu” (sin comillas) y cuyo contenido sea 1, esta opción volverá al menú contextual que aparecerá al pulsar con el botón derecho del ratón sobre carpetas y archivos.

REFRESCAR EL CONTENIDO DE LA PANTALLA AL INSTANTE

Algunas veces, tras haber creado o eliminado un archivo o carpeta, nos habremos encontrado con que es necesario esperar unos segundos antes que estos cambios se muestren en el explorador...

Esto es debido a que Windows no refresca por defecto la pantalla continuamente. Ocasionalmente utilizamos la tecla F5 para redibujar el contenido de la pantalla, pero podemos modificar el registro para disminuir los tiempos de refresco. Para ello:

Iniciar el registro de Windows (regedit.exe)
Localizar la clave **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Update.**
Modificar el valor binario "UpdateMode" de "01" a "00".
Reiniciar Windows.

RESTRINGIR LAS APLICACIONES QUE LOS USUARIOS PUEDEN EJECUTAR

Windows proporciona la posibilidad de restringir las aplicaciones que los usuarios pueden ejecutar en una estación de trabajo:

Para ello, iniciaremos la herramienta de edición del registro de sistema, con el comando "regedit.exe", desde el menú Inicio/Ejecutar y localizaremos la clave:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.
Alli crearemos o modificaremos el valor DWORD "RestrictRun" (sin comillas) con el valor "1" para activar la restricción o "0" para desactivarla. Acto seguido tendremos que definir las aplicaciones cuya ejecución estará restringida ya que por defecto la ejecución de todas estará permitida. Para ello nos trasladaremos hasta la clave:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun
e introduciremos valores alfanuméricos cuyo nombre serán números consecutivos y como contenido tendrán los nombres de los ejecutables de cada aplicación.

RESTRINGIR EL ACCESO AL EDITOR DEL REGISTRO DEL SISTEMA

Para obtener la posesión sobre una rama del registro o restringir el acceso a la misma, abriremos el editor de registro de sistema, con el comando "regedit.exe" desde el menú Inicio/Ejecutar y localizaremos la clave cuyas propiedades queramos modificar.

En el menú Editar o desde el menú contextual que aparece al pulsar con el botón derecho del ratón seleccionaremos la opción Permisos, que abrirá un cuadro de diálogo con los diferentes permisos de acceso existentes para los usuarios del sistema sobre esa rama.

Pulsaremos sobre el botón Avanzada y nos trasladaremos hasta la pestaña Propietario. En el cuadro de diálogo "Cambiar Propietario" seleccionaremos la cuenta que tomará posesión de rama y pulsaremos sobre Aplicar. Igual que si de una carpeta en el explorador de Windows se tratara, confirmaremos si queremos reemplazar el propietario del resto de claves y ramas que cuelgan de la seleccionada.

SUSTITUIR ARCHIVOS EN USO

"inuse.exe" es una herramienta que antaño formaba parte del kit de recursos de Windows 2000, y que con la liberación de Windows XP Microsoft ha decidido ponerla a disposición de forma gratuita. Su cometido es permitir la sustitución de archivos que estén en uso por parte del Sistema Operativo y que de otra manera no podrían ser sustituidos. Su sintaxis es:
INUSE origen destino /y

Origen especifica el nombre del archivo actualizado
Destino especifica el nombre del archivo existente que será reemplazado
/y elimina la petición de confirmación para reemplazar el archivo.

Nota: los cambios no surtirán efecto hasta que reiniciemos el ordenador.

WINDOWS MESSENGER BAJO UN ROUTER O FIREWALL

Si nos conectamos a Internet a través de un Firewall o un router habremos comprobado que algunas de las características de Windows Messenger no funcionan de forma correcta. Para solucionar este problema tendríamos que configurar en el firewall o router el uso de los siguientes puertos:

Videoconferencia, audio, video y llamadas de PC a teléfono: Puertos UDP 5004-65535. Debido a

que el envío de flujos se aloja dinámicamente en este rango de puertos, tendremos que encontrar la manera de abrir todos ellos.
Application Sharing y WhiteBoard: Puerto TCP 1503

Transferencia de archivos: Puertos TCP 6891-6900. Estos puertos permiten hasta 10 transferencias simultáneas por usuario. Si únicamente abrimos el puerto 6891, el usuario únicamente podrá realizar una única transferencia simultánea.
Asistencia Remota: Puerto TCP 3389

COMO ACTIVAR Y DESACTIVAR LA TECLA WINDOWS

Windows XP ofrece la posibilidad de desactivar la tecla Windows que se encuentra entre las teclas "Ctrl" y "Alt" la Winkey, es fácilmente identificable por la banderita de Windows.
En algunas ocasiones puedes ser interesante desactivarla, sobre todo si juegas con tu PC y sin querer pulsas esta tecla ya sabes lo que ocurre, para activarla o desactivarla sigue estos pasos:
Pulsa sobre el botón Inicio y luego en Ejecutar, escribe regedit y pulsa el botón Aceptar.
Ahora vete abriendo las siguientes claves:
HKEY_CURRENT_USERS/oftware/Microsoft/ Windows/CurrentVersion/Policies/Explorer.
Allí crearemos o modificamos el valor DWORD NoWinKeys con el valor "1" para desactivar el uso de la tecla y "0" para activarla de nuevo.
Si no existe la entrada NoWinkeys debemos crearla tal como se indica en la figura y asignarle el valor "0" para deshabilitarla o "1" para habilitarla.
Si ya está creada la entrada entonces solo debemos cambiar el valor "0" o "1".

COMO CONSEGUIR EJECUTAR PROGRAMAS ANTIGUOS EN WINDOWS XP

Si una aplicación antigua te crea problemas al ejecutar Windows XP, puedes configurar las propiedades de compatibilidad de forma manual para que el programa se ejecute en un modo diferente, como Windows 95, o con una configuración de pantalla y de resolución distintas. Para establecer las propiedades de compatibilidad de un programa debes seguir estos pasos:

Haces clic con el ratón derecho en el archivo ejecutable o en el acceso directo del programa al archivo ejecutable y, a continuación, haces clic en Propiedades.
Activa la casilla de verificación Ejecutar este programa en el modo de compatibilidad. Dale a la lista, selecciona un sistema operativo en el que se ejecute el programa sin problemas.
Si fuera necesario, cambia también la configuración de pantalla y la resolución, o deshabilita los temas visuales de Windows XP.
Ejecuta el programa de nuevo cuando hayas terminado de cambiar la configuración. Ajusta los valores de compatibilidad de nuevo si el programa todavía no se ejecuta sin problemas: un programa que presente problemas en Windows 2000 puede no tener ninguno en Windows 98.

COMO IMPEDIR QUE LOS USUARIOS DEL EQUIPO REALICEN DESCARGAS DESDE INTERNET

Windows XP ofrece la posibilidad de impedir que los usuarios de un mismo equipo, realicen descargas de archivos desde Internet, para ello tenemos que recurrir al registro de Windows de la siguiente forma:

Hacemos clic en el botón Inicio y luego en Ejecutar
Escribimos Regedit y pulsamos el botón Aceptar.
Ahora en el registro nos desplazamos por las siguientes claves:

HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Internet Settings/Zones

Al abrirse la última entrada de Zones veremos varias carpetas, la que nos interesa es la carpeta 3.
Ahora hacemos clic sobre la carpeta nº 3 y en el panel derecho veremos los valores que tiene asociados.
Buscamos el valor 1803 hacemos doble clic sobre él, en la ventana que nos muestra escribimos el número 3 y pulsamos el botón Aceptar. La próxima vez que alguien intente descargar algo desde Internet recibirá un mensaje de aviso de que la seguridad no le autoriza a descargar ese archivo.
Aclaración: Esta restricción solo afecta al usuario al que se le ha hecho la restricción, y lógicamente hay que hacer este truco desde la propia cuenta de usuario a restringir.

CREAR UN DISCO DE RESTABLECIMIENTO DE CONTRASEÑAS

Si estás ejecutando Windows XP Profesional como usuario local en un entorno de grupo de trabajo, puedes crear un disco de restablecimiento de contraseñas para iniciar sesión en el equipo cuando olvides la contraseña. Para crear el disco, sigue estos pasos:

Haz clic en Inicio, en Panel de control y, a continuación, en Cuentas de usuario.
Haz clic en tu nombre de cuenta.
Debajo de Tareas relacionadas, haces clic en Prevenir el olvido de contraseñas.
Sigue las instrucciones del Asistente para contraseña olvidada con el fin de crear un disco de restablecimiento de contraseña.
Guarda el disco en un lugar seguro, ya que cualquiera que lo utilice puede tener acceso a su cuenta de usuario local.

CREAR UN ICONO PARA APAGAR RÁPIDAMENTE EL PC

Puedes hacer que tu PC se apague con doble clic, para ello deberás crear un icono que te permita hacer esta función, para realizar este truco sigue estos pasos:

Haz clic con el ratón derecho en una zona libre del Escritorio y luego selecciona Nuevo y Acceso directo.
En la ventana del acceso directo debes escribir shutdown -s -t 00 y pulsa el botón Siguiente, después le pones el nombre que quieras al acceso directo y pinchas el botón Finalizar.
Si quieres dejar algo de tiempo para cerrar las aplicaciones debes poner esto shutdown.exe -s -t 12 de esta forma dejarás un margen prudencial de 12 segundos para apagar el PC.

DESACTIVAR LAS VENTANAS DE AVISO

Mientras estás utilizando Windows XP, el sistema te va mostrando distintas ventanas de aviso en la parte inferior junto al Reloj, estas ventanas que a veces son molestas se pueden eliminar de la siguiente forma:

Haces clic en el botón Inicio y luego en Ejecutar, una vez te muestre el cuadro ejecutar escribe la palabra Regedit y pulsa el botón Aceptar.
Cuando aparezca el Editor del Registro "Regedit" desplázate por la siguiente cadena
HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Advanced

Pulsa sobre la opción Edición de la barra de herramientas y luego Nuevo, y Valor DWORD con ello aparecerá una nueva ventana.
Escribe EnableBalloonTips y pulsa la tecla Intro.
Reinicia Windows y no volverás a ver esas ventanitas tan molestas algunas veces.

DESHABILITA LOS SERVICIOS INNECESARIOS

Al iniciarse, Windows XP ejecuta muchos programas que permanecen cargados en segundo plano, consumiendo recursos del sistema y haciendo que todo sea un poco más lento, y que a veces son innecesarios. Estos programas consumen bastante memoria. Para deshabilitar estos servicios sigue estos pasos:

Hacemos clic en el botón Inicio, después en Ejecutar y escribimos services.msc.
En la ventana que aparece hacemos clic con el ratón derecho sobre el servicio que deseamos deshabilitar.
Elegimos Propiedades
En la opción Tipo de Inicio seleccionamos Deshabilitado y listo de esta forma habremos deshabilitado los servicios que consideremos oportuno con el consiguiente ahorro de memoria.

DESHABILITAR PROGRAMAS QUE ARRANCAN CON EL INICIO DE WINDOWS

En la mayoría de los casos con el paso del tiempo vamos instalando e instalando programas y muchos de ellos arrancan con el inicio de Windows, haciendo que el sistema se vuelva pesado y tarde mucho en mostrar el escritorio, pues bien hay una forma de hacer que estos programas no arranquen con el inicio de Windows.

- Hacemos clic en el botón Inicio y luego en Ejecutar.
- Tecleamos MSCONFIG y pulsamos el botón Aceptar.
- En la ventana que nos muestra hacemos clic sobre la pestaña Inicio y ahí es donde desactivamos los programas que no queremos que se carguen al arrancar Windows, de esta forma reduciremos el tiempo de arranque del sistema operativo.
- Luego pulsamos el botón Aceptar y listo, la próxima vez que reiniciemos el SO, tardará menos tiempo en mostrarnos el Escritorio.

DESOCULTAR PROGRAMAS INSTALADOS QUE NO APARECEN EN AGREGAR/QUITAR PROGRAMAS

Microsoft ha eliminado del programa de instalación del sistema la posibilidad de que el usuario especifique los componentes de Windows que serán instalados. Podemos observar que si vamos a la opción de "Agregar o quitar componentes de Windows" dentro del "Panel de control" no veremos la lista completa de aplicaciones que podemos añadir o eliminar.

Podremos solucionar este problema accediendo a la carpeta "c:\windows\inf" y allí localizaremos el archivo "sysoc.inf" que podremos abrir con el bloc de notas. Si observamos la sección [Components], encontraremos que algunos de los elementos contienen las palabras "hide" o "HIDE" y por esta razón no se muestran bajo el panel "Agregar o quitar componentes de Windows".

```
[Version] Signature = "$Windows NT$"
DriverVer=02/22/2002,9.3.3202.0
[Components]
NtComponents=ntoc.dll,NtOcSetupProc,,4
WBEM=ocgen.dll,OcEntry,wbemoc.inf,hide,7
Display=desk.cpl,DisplayOcSetupProc,,7
Fax=fxsocm.dll,FaxOcmSetupProc,fxsocm.inf,,7
NetOC=netoc.dll,NetOcSetupProc,netoc.inf,,7
iis=iis.dll,OcEntry,iis.inf,,7
AccessOpt=ocgen.dll,OcEntry,optional.inf,HIDE,7
```

Pinball=ocgen.dll,OcEntry,pinball.inf,HIDE,7
MSWordPad=ocgen.dll,OcEntry,wordpad.inf,HIDE,7
[...]

Sustituiremos la cadena "hide" por una coma ",". Acto seguido salvaremos el archivo, volveremos a ejecutar el panel "Agregar o quitar componentes de Windows" y comprobaremos que aparecen listados para su instalación o desinstalación, componentes que hastan entonces permanecían ocultos.

ELIMINAR AUTOMÁTICAMENTE LOS ARCHIVOS TEMPORALES DE INTERNET

Puedes configurar tu navegador para que elimine automáticamente los archivos temporales cada vez que cierres tu navegador, para configurar esta opción sigue estos pasos:

Abre tu navegador Internet Explorer, y haces clic en el Menú Herramientas y luego en Opciones de Internet.
Pulsa en la pestaña Opciones avanzadas y busca la opción "Vaciar la carpeta archivos temporales de internet cuando se cierre el explorer"
Finalmente pulsa sobre el botón Aceptar y a partir de ahora cada vez que cierres el Explorer automáticamente te eliminará los archivos temporales.

EVITAR LA ACTIVACIÓN DE WINDOWS XP

Como es bien sabido Windows XP debe ser activado después de su instalación, porque de lo contrario dejará de funcionar a los 30 días. Hasta este punto todo correcto, se instala Windows XP, se activa y listo, pero el problema viene una vez que por cualquier circunstancia hay que formatear el PC o reinstalar Windows, que nuevamente tenemos que activarlo, para evitar esto debemos hacer lo siguiente:

Una vez que se activa Windows XP por primera vez, se guarda un archivo en nuestro PC, este archivo debemos copiarlo y guardarlo muy bien para la siguiente vez que borremos el disco duro y así evitaremos la activación nuevamente.
Sigue estos pasos para buscar y guardar el archivo que guarda las configuraciones del hardware y la activación de tu copia de Windows XP.
Haces clic con el botón Inicio y a continuación en Ejecutar.
Escribe wpa.dbl y pulsa el botón Aceptar, después de unos segundos aparecerá el archivo en el cuadro buscar.
Ahora fíjate bien donde está el archivo (normalmente estará en el directorio Windows), copia este archivo en un disquete o en cualquier otro lugar del disco duro donde esté a salvo de errores y lo puedas conservar hasta que lo necesites.
La próxima vez que formatees el disco duro, o por cualquier otra causa necesites activar tu copia de Windows XP simplemente copia el archivo que acabas de guardar al directorio Windows, reinicias y listo ya está activada nuevamente tu copia de Windows XP.

OCULTAR EL BOTÓN APAGAR EL SISTEMA DEL BOTÓN INICIO

Si tu ordenador es utilizado por varios usuarios, en una misma sesión, puede que desees desactivar el botón de Apagar el sistema que aparece al pulsar el botón inicio, si este es tu caso sigue estos pasos para ocultar dicho botón:

Pulsa sobre el botón Inicio y luego en Ejecutar, escribe Regedit y pulsa el botón Aceptar. Ahora buscaremos las siguientes claves:
HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/Explorer.

Creamos o modificamos el valor del tipo DWORD NoClose con el contenido "1" para ocultar el botón del menú inicio o "0" para mostrarlo. Aunque siempre estará disponible desde el administrador de tareas.
Si no está creada la clave que será lo más probable debes crearla y darle el nombre NoClose y luego debes darle el valor "1" o "0" según tus necesidades, tal como hemos explicado en el paso 3.

PANTALLA CLÁSICA DE BIENVENIDA AÑADIR UN MENSAJE

Este truco solo es válido si tienes configurado el arranque de Windows con la pantalla de inicio clásica. Para poder añadir un mensaje a la pantalla de bienvenida debes seguir estos pasos:

Entra en Windows como Administrador y luego pulsa el botón inicio y Ejecutar
Escribe regedit y pulsa el botón Aceptar.
Ahora te desplazas por las siguientes claves:
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/CurrentVersion/Winlogon
Ahora en el panel de la derecha haces clic con el ratón derecho y seleccionas Nuevo y luego Valor alfanumérico, luego le pones el nombre LogonPrompt y pulsa la tecla Intro.
Si haces doble clic sobre la entrada que acabas de crear podrás escribir el mensaje que quieras que muestre al arrancar Windows en la pantalla de bienvenida, luego Aceptas y cierras todas las ventanas que tengas abiertas, reinicias el equipo para comprobar que el mensaje que has puesto aparece en la pantalla de bienvenida.

TECLAS

Estas son algunas combinaciones del Teclado utilizadas por Windows XP. Con estas combinaciones de teclas accederás rápidamente a cada función.

- Tecla Windows + Tecla D: Minimizar o restaurar todas las ventanas
- Tecla Windows + Tecla E: Windows Explorer
- Tecla Windows + Tecla F: Búsqueda de archivos
- Tecla Windows + Ctrl + Tecla F: Buscar en equipo
- Tecla Windows + Tecla F1: Ayuda
- Tecla Windows + Tecla R: Ejecutar
- Tecla Windows + Tecla mayúsculas + Tecla M: deshacer minimizar ventanas
- Tecla Windows + Tecla L: Bloqueo de la estación de trabajo
- Tecla Windows + Tecla U: Administrador de utilidades
- Tecla Windows + Tecla Pausa: Sistema

UN ICONO PARA CADA LIBRERÍA DLL

Si encuentras aburrido el icono que representa los archivos ".dll" de las librerías dinámicas, podemos configurar el registro para que cada uno de estos archivos muestre su propio icono, si bien no todos ellos incluyen uno, por lo que éstos se mostrarán con el icono de tipo "tipo desconocido". Para realizar este truco debes seguir estos pasos:

Comenzaremos haciendo clic en el botón Inicio y luego en Ejecutar, ahora escribimos Regedit y pulsamos el botón Aceptar.
Ahora nos desplazamos por las siguientes claves:
HKEY_CLASSES_ROOT\dllfile\DefaultIcon
Ahora modificaremos el contenido del valor (Predeterminado) con %1 (sin comillas. Si queremos volver al ajuste predeterminado, modficaremos el contenido con la cadena **"%SystemRoot%\System32\shell32.dll,-154.** De la misma forma se comportan los archivos .cpl que representan los applets del panel de control. Para que cada uno de estos

archivos muestre su icono dentro del explorador de Windows, localizaremos la cadena **HKEY_CLASSES_ROOT\cplfile** y añadiremos una subclave DefaultIconcuyo valor (Predeterminado) estableceremos en %1. Reiniciaremos el sistema para aplicar los cambios.

VELOCIDAD DE DESCARGA EN LA TRANSFERENCIA DE ARCHIVOS

Windows XP nos brinda la oportunidad de ver en gráficos la velocidad en la transferencia de archivos, bien sea cuando descargamos algo de la red, como archivos o páginas web, o bien cuando somos nosotros los que hacemos de servidor y están descargando algo de nuestro ordenador. La forma de obtenerlo es la siguiente:

Hacemos clic con el ratón derecho sobre una zona libre de la barra de tareas, junto al botón inicio y luego sobre Administrador de tareas.
Seguidamente se abrirá el Administrador de tareas, ahora hacemos clic sobre la pestaña Funciones de Red y es en este gráfico donde se muestra nuestra actividad en la red.

CAMBIAR LA CARPETA PREDETERMINADA DEL EXPLORADOR DE WINDOWS

El explorador de Windows de forma predeterminada, se abre mostrando la carpeta Mis documentos. Para cambiar los valores predeterminados y que se muestren todas las unidades y carpetas de nivel superior, sigue estos pasos:

Haces clic en en el botón Inicio, luego seleccionas Programas, Accesorios, después, haces clic en Explorador de Windows y, a continuación, haces clic en Propiedades.
En el campo Destino, en el que aparece **%SystemRoot%\explorer.exe**, agregas lo que falta para que en la línea aparezca **%SystemRoot%\explorer.exe /n, /e, /select, C:**
Haces clic en Aceptar.
Ahora, cuando abras el Explorador de Windows podrás elegir de todas las carpetas y unidades, y no sólo de Mis documentos.

VOLVER AL INICIO CLÁSICO DE WINDOWS

Al comenzar a trabajar con Windows XP muchas veces hechamos de menos el menú de inicio clásico de Windows, pues bien Windows XP tiene una opción con la que se puede volver a obtener el menú clásico de Windows, para ello sigue estos pasos:
Haces clic con el ratón derecho sobre la barra de inicio, junto al botón Inicio. Seleccionas Propiedades
Haz clic sobre la pestaña Menú Inicio y marca la casilla Menú inicio clásico.
Acepta para que se apliquen los cambios y listo, ahora cuando pulses sobre el botón Inicio volverás a ver el menú clásico de Windows.

FRAGMENTAR RÁPIDO

Todos sabemos que los discos se fragmentan cada tanto. A medida que vamos borrando archivos, aparecen pequeños agujeros en nuestro disco rígido. El problema es que Windows ve estos agujeros como espacio libre para guardar datos. Y lo peor es que, si el espacio disponible es menor que el tamaño del archivo por almacenar, Windows guardará lo que entre y pondrá el resto en algún otro lejano lugar del disco rígido. ¿El resultado? Con el tiempo, mayor tardanza para acceder a los archivos y programas.

Windows ejecuta una "regla" cuando hace esto. La cantidad de espacio libre tiene que ser de 512 KB o más. Lo que hemos encontrado es un pequeño cambio en el Registro que nos permitirá subir este límite para forzar a Windows a que busque un hueco más grande donde poner los datos.

Vamos a llevar este límite a 2 MB. Para ello abrimos Regedit y nos dirigimos a:
[HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Control\ File System].
Creamos un nuevo valor DWORD con el nombre **ConfigFileAllocSizer** y le colocamos el valor 2048 en decimal. Cerramos todo, reiniciamos y listo. ¡Ojo! Nuestro disco se quedará sin espacio más pronto, por lo que tendremos que volver a desfragmentarlo cada tanto.

PROBLEMAS CON LAS FUENTES

Si tenemos fuentes en el sistema aparentemente instaladas de forma correcta, pero que no aparecen en la carpeta Fuentes, esto puede ser debido a que la clave Fonts en el registro haya sido borrada o esté dañada

En primer lugar moveremos el contenido de la carpeta C:\WINDOWS\FONTS a una carpeta vacía, abriendo la carpeta, seleccionando todas las fuentes y después copiándolos a la nueva carpeta.
Una vez hecho iniciaremos la herramienta de edición del registro de sistema, con el comando "regedit.exe" desde el menú Inicio/Ejecutar. Allí localizaremos y eliminaremos los contenidos de la clave **HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Fonts** (para equipos Windows 9x) o
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Fonts
(Para equipos Windows NT-2000-XP). Una vez hecho esto, reiniciaremos el sistema, reinstalaremos las fuentes desde el panel de control/Fuentes seleccionando en el menú Archivo la opción Instalar nueva fuente añadiendo las fuentes que previamente copiamos al directorio temporal.

RESTRICCIONES PARA EL ESCRITORIO ACTIVO

Algunas de las características del escritorio activo de Windows pueden ser controladas y deshabilitadas de forma individual a través del registro...
Para ello iniciaremos la herramienta de edición del registro de sistema, con el comando "regedit.exe" desde el menú Inicio/Ejecutar y localizaremos la clave:
HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ ActiveDesktop.
Allí crearemos o modificaremos los valores DWORD existentes, cuyo contenido será "1" para activar la restricción de configuración de esos elementos o "0" para desactivar la restricción:

- "NoChangingWallpaper" Deshabilita la posibilidad de cambiar el papel tapiz.
- "NoAddingComponents" Deshabilita la posibilidad e añadir componentes.
- "NoDeletingComponents" Deshabilita la posibilidad de eliminar componentes.
- "NoEditingComponents" Deshabilita la posibilidad de editar componentes.
- "NoHTMLWallPaper" Deshabilita el uso de archivos diferentes de mapas de bits (.bmp) como fondo de escritorio.

VERSIÓN DE WINDOWS XP

Si en algún momento decidieras actualizar tu versión de Wndows XP, y no conoces la versión que tienes en tu PC, lo puedes averiguar de la siguiente forma:
Abres una ventana de MS-DOS desde el botón Inicio, luego todos los programas, Accesorios y finalmente sobre la entrada Símbolo del sistema. Una vez se abra la ventana de MS-DOS, teclea la palabra Ver y pulsa la tecla Intro, en unos segundos te mostrará la versión actual de Windows XP.

CAMBIAR LA LETRA DE LA UNIDAD

Para cambiarle la letra de unidad a un dispositivo en Windows XP, iniciaremos la consola de administración de sistema, pulsando con el ratón derecho sobre Mi PC y seleccionando Administrar. Una vez allí, seleccionaremos el Administrador de discos y haremos clic con el ratón derecho sobre el dispositivo al que queramos cambiarle la letra de unidad, seleccionando la opción Cambiar letra de unidad y ruta y especificando la nueva letra de unidad que queramos darle.

REINSTALAR WINDOWS MEDIA PLAYER

Para reinstalar Windows Media Player, si por cualquier circunstancia se estropeó o simplemente no funciona, sigue estos pasos:

Desde el botón Inicio haz clic en Ejecutar... escribe o copia esta línea **rundll32.exe setupapi,InstallHinfSection InstallWMP64 132 c:\windows\inf\mplayer2.inf**
(OJO! se supone que XP está en la unidad C:\ en caso contrario cambia a la ruta correcta, te pedirá el CD de XP).
Ahora vuelve otra vez a Inicio, Ejecutar... y escribe o copia **rundll32.exe setupapi,InstallHinfSection InstallWMP7 132 c:\windows\inf\wmp.inf**
(OJO! se supone que XP está en la unidad C:\ en caso contrario cambia a la ruta correcta, te pedirá el CD de XP), cuando finalice, reinicia el sistema.

FIJAR EL ARCHIVO DE PAGINACIÓN

Durante la instalación del sistema y dependiendo de la cantidad de memoria, se establece automáticamente el tamaño del archivo de paginación. Para alterar su ubicación y su tamaño, o prescindir de él:
Pulsaremos con el botón derecho del ratón sobre el icono Mi PC seleccionando sus Propiedades.
En la pestaña Avanzada pulsaremos el botón configuración situado en el apartado Rendimiento y dentro en la pestaña Avanzada pulsaremos sobre el botón Cambiar modificando los tamaños mínimos y máximo así como la unidad en la que se establecerá.

INHABILITAR OPCIONES DE WINDOWS

Este truco permitirá deshabilitar algunas aspectos del explorador para que nadie pueda tener acceso a tu computadora. Abre el editor del registro de windows (regedit.exe),y luego ve a la clave(carpeta):
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Una vez ahí puedes crear los siguientes valores que te describiré a continuación: Primero siempre efectúa el siguiente paso para cada Valor que vallas a crear; Click en Edición\Nuevo\Valor DWORD. Te aparecerá en el costado derecho de la pantalla un nuevo valor DWORD. Luego le pones uno de los siguientes nombres a dicho valor:

- NoClose: Deshabilita el comando "Apagar el sistema" del menú inicio
- NoFavoritesMenu: Deshabilita el menú "Favoritos" del menú inicio
- NoFind: (Deshabilita el comando "Buscar" del menú inicio)
- NoRecentDocsMenu: Deshabilita el menú "Documentos" del menú inicio
- NoRecentDocsHistory: Complemento de el truco anterior para deshabilitar totalmente el menú "Documentos"; este complemento no permite que aparezcan accesos directos en la carpeta recent
- NoRun: Deshabilita el comando "Ejecutar" del menú inicio
- NoSetFolders: Deshabilita los comandos "Panel de control" e "Impresoras" del menú Configuración que esta en el menú inicio
- NoSetTaskbar: Deshabilita los comandos "Barra de tareas y Menú inicio" del menú Configuración que esta en el menú inicio

- NoFileMenu: Deshabilita el menú "Archivo" del Explorador de Windows
- NoViewContextMenu: (Deshabilita los menús que aparecen cuando hacemos click con el boton derecho del ratón; exepto los de la barra de tareas
- NoTrayContextMenu: (Deshabilita los menús que aparecen cuando hacemos click con el boton derecho el ratón en la barra de tareas)
- NoDesktop: Esconde todos los iconos del escritorio

Para que todo esto funcione; luego de nombrar los valores se debe hacer doble click sobre ellos y escribir "1" para habilitar la acción ó "0" para deshabilitarla. Ademas se debe reiniciar el equipo para que los cambios tengan efecto.

SUPRIMIR LA ANIMACIÓN DE LAS VENTANAS

La animación de las ventanas al maximizar y minimizar puede retardar el trabajo del sistema, sobre todo si escasea la memoria RAM y trabajamos con varios programas al mismo tiempo.
Se puede eliminar esta animación de la siguiente forma:
Acuda a la clave HKEY_CURRENT_USER del registro, y sucesivamante a las subclaves Control Panel, Desktop y WindowsMetrics. Saldrán unos cuantos valores que no debe tocar, más bien al contrario, se debe añadir la siguiente entrada: MinAnimate, siendo su valor cero.

Cómo conservar los mails en Outlook Express 6.0

Encontré esta solución después de trabajar con muchas PCs a lo largo de mi carrera y de recibir quejas por la pérdida de e-mails y de la base de datos de los correos electrónicos de los usuarios a los que les reparaba la PC. A veces, a causa del ataque de virus o del formateo del disco rígido, no se salva la base de los mails, la cual está alojada en la carpeta **[C:\Windows\Aplication Data\Microsoft\Andress Book] (Libreta de direcciones).**
Los mails recibidos están contenidos en **[C:\Windows\Application Data\Microsoft\Outlook Express].**
El truco consiste en lo siguiente:
Seleccionamos esas dos carpetas y las guardamos en un disquete de 3 ½, siempre y cuando nuestros mails no superen el tamaño de 1,44 MB.
Cuando terminemos de instalar la nueva configuración de Windows, abrimos Outlook Express y vamos a [Archivo/Importar/Mensajes o Libreta de direcciones]. En el menú que aparece, seleccionamos [Archivos de Outlook 4, 5] (o la versión que estemos usando). Luego, elegimos la identidad principal, buscamos la carpeta que bajamos al disquete de 3 ½, y hacemos clic en [Aceptar]. Si todo sale bien, aparecerá una ventana que nos preguntará si queremos importar todas las carpetas o sólo una (por ejemplo, la Bandeja de entrada).

Mail sin abrir Outlook Express 6.0

Este truco nos resultará muy útil si no queremos abrir Outlook Express (o el cliente predeterminado de correo) para crear un mensaje nuevo. Hay que hacer clic en [Inicio/Ejecutar], escribir mailto: y, luego, hacer clic en [Aceptar] o presionar [Enter]. De esta manera, se abrirá el mensaje nuevo sin tener que ejecutar el programa de correo.

Disco de inicio en Windows XP

Para crear un disco de arranque de forma sencilla ,deberemos seguir estos pasos:
Doble clic sobre [Mi PC].
Clic derecho sobre la unidad A: que debe contener un disquete. En las opciones de formateo, se debe marcar la casilla de verificación para crear un disco de inicio. De esta forma, hemos creado un disco de inicio que podrá sacarnos de más de un apuro en el futuro.

Deshabilitar el reporte de errores

Si hay una característica de Windows XP de la que podemos prescindir, ésta es el reporte automático de errores. Cada vez que un programa se cuelga, el sistema nos pregunta si queremos enviar un informe a Microsoft. Creemos que éste es uno de los peores momentos de la historia de la informática y, en general, es absolutamente inútil, salvo para Microsoft, que algún día podrá mejorar su sistema operativo. En fin, para deshabilitar el reporte de errores, hay que seguir este camino:
[Panel de control/Sistema/Opciones avanzadas/Informe de errores/Deshabilitar el informe de errores].

Configurar Rendimiento en Windwos XP

La interfase Luna de Windows XP puede volver un poco lenta alguna máquina con un procesador viejo, con poca memoria o sin una buena placa de video. Es innegable que el sistema es mucho más vistoso de esta forma... pero no es recomendable tenerlo en máquinas muy viejas. Por suerte, las opciones visuales se pueden configurar por separado. Por ejemplo, podemos elegir si queremos sombra bajo los menúes, sombra debajo del puntero, estilos visuales en ventanas, etc. Para configurar esto, hay que dirigirse a las propiedades de Mi PC (haciendo clic derecho) y elegir la solapa [Opciones avanzadas]. Allí, vamos a [Rendimiento/Configuración]; se abrirá el cuadro de diálogo que se ve en la imagen. Acá podremos habilitar o deshabilitar cualquiera de las casillas o elegir alguna de las opciones predeterminadas, para mejor rendimiento o la apariencia.

Arranque automático de discos

Una novedad de XP bien recibida por algunos –aunque no tanto por otros– es la que permite la reproducción automática de CDs, aunque éstos no tengan autorun. Esta característica hace un poco lenta la lectura, ya que primero lee el CD completo para analizar el tipo de archivos que contiene. Por ejemplo, si es un CD con imágenes, nos mostrará opciones de tratamiento de imágenes. Vale aclarar que lo mismo sucede tanto con CDs como con cualquier tipo de disco extraíble. Estas opciones se pueden personalizar:

Debemos abrir el cuadro de diálogo [Ejecutar], escribir gpedit.msc y pulsar [Aceptar].
Aparecerá el editor de directivas de grupo.
Acá debemos dirigirnos a [Configuración del equipo/Plantillas administrativas/Sistema].
Seleccionamos la opción [Desactivar Reproducción automática]; doble con un clic sobre ella.
En el cuadro de diálogo que aparece, seleccionamos [Habilitar].

Por más que suene confuso, el procedimiento es correcto: estamos "habilitando la desactivación".

Accesos superdirectos

Y seguimos encontrándole nuevos usos a la archiconocida barra de vínculos de Explorer. Antes de empezar, los que no la conozcan, sepan que la barra de vínculos del Explorador de Windows e Internet Explorer, se activa desde [Ver/Barras de herramientas/Vínculos] y se encuentra dentro de la misma carpeta FAVORITOS, en \Documents and settings\usuario\Favoritos. Nuestro primer agregado a esta barra consistirá en arrastrar el ícono de Internet Explorer desde la barra de inicio rápido hasta la misma barra de vínculos (si presionamos CTRL al mismo tiempo, estaremos creando una copia). Con este nuevo ícono, será posible abrir una nueva ventana de Internet Explorer rápidamente: ¿qué les parece? Luego pueden hacer clic derecho sobre el ícono y cambiar el nombre por "e", por ejemplo: para que no ocupe tanto lugar.
Otra idea es colocar un acceso directo a Winamp; luego, podrán seleccionar un conjunto de archivos de música y arrastrarlos y soltarlos sobre el ícono del programa para escucharlos. Por alguna extraña razón, esto no funciona no bien se termina de agregar el ícono de acceso directo del programa: hay que cerrar y volver a abrir la ventana del explorador. En caso contrario, Windows entenderá que quieren agregar los archivos a la barra de herramientas.
Por último, otra posibilidad muy interesante es agregar el acceso directo de DropStuff (una aplicación integrante del paquete StuffIt Deluxe). De esta forma, podrán seleccionar un grupo de archivos que quieran comprimir y arrastrarlos sobre ese ícono, para que se conviertan en un archivo ZIP o SIT en ese mismo directorio.

Cambio rápido de usuario

Windows XP brinda soporte un muy bueno para múltiples cuentas de usuario. Por ejemplo, es posible cambiar de usuario sin cerrar la sesión y mantener la conexión a Internet y los programas abiertos. Para aprovechar esto, es recomendable tener activado el Cambio rápido de usuario, ya que, por lo general, no viene configurado de manera predeterminada en Windows. Esta característica permite, mediante las teclas **[WINDOWS] + L**, acceder a la pantalla de bienvenida para elegir otro usuario. Si nuestro teclado no tiene la tecla [WINDOWS], podemos acceder a esta característica desde [Inicio/Cerrar sesión].

Para activar el Cambio rápido de usuario, es preciso dirigirse a [Inicio/Panel de control/Cuentas de usuario] y, en la ventana que aparece, hacer clic en [Cambiar la forma en que los usuarios inician y cierran sesión]. Acá hay que marcar dos opciones: **[Usar la pantalla de bienvenida]**

Atajos de teclado para Windows XP

- La lista definitiva con todos los atajos de teclados para Windows XP.
  [WIN] + R: cuadro de diálogo Ejecutar
- [WIN] + F: buscar
- [WIN] + M: minimizar todas las ventanas
- [WIN] + D: mostrar el Escritorio/Restaurar vista
- CTRL + ESC: mostrar el menú Inicio.
- CTRL + Clic: selecciones múltiples
- SHIFT + Clic: selecciones múltiples de elementos dentro de un rango
- CTRL + C: copiar la selección al Portapapeles
- CTRL + X: cortar la selección al Portapapeles
- CTRL + V: pegar el contenido del Portapapeles
- CTRL + Z: deshacer la última acción

- CTRL + E: seleccionar todo
- F5: actualizar el contenido de la ventana
- CTRL + W: cerrar ventana
- CTRL + H: ver el Historial
- CTRL + I: ver Favoritos
- CTRL + R: actualizar

Configuración de sistema en Windows XP

Veamos cómo sacarle un peso de encima a nuestra computadora, optimizando los recursos que ya tenemos a mano. Siga los siguientes pasos:

1. Para acceder a las herramientas de configuración del sistema, vamos a **[Inicio/Programas/Accesorios/Herramientas del sistema/Información del sistema].** Una vez abierta la ventana de [Información del sistema] de Microsoft, vamos a **[Herramientas/Programas de configuración del sistema].**

2. Si nuestro sistema operativo es Windows Millennium, tardaremos mucho en encontrar las utilidades del System Config, porque tendremos que pasar por la ayuda del sistema. Sin embargo, podemos acceder escribiendo "msconfig" en el menú [Ejecutar].

3. En la solapa [General], podemos setear qué tipo de inicio queremos y elegir qué archivos del proceso se ejecutarán cuando Windows arranque. Si tenemos Windows Me o XP, también podemos usar [Iniciar Restaurar Sistema], para que el sistema vuelva al estado anterior.

4. En System.ini encontramos el residuo de los sistemas de 16 bits; están incluidos en los sistemas de 32 bits de Windows 95/98/Me/XP, para conservar la compatibilidad con las aplicaciones viejas. El archivo System.ini tiene información sobre drivers, sobre DLLs y sobre passwords necesaria para iniciar el sistema. Se puede activar o desactivar algo de Sistem.ini desde esta solapa.

5. Al igual que Sistem.ini, Win.ini fue reemplazado por el registro; pero todavía tiene un fin. Hay que evitar realizar cualquier cambio en este archivo, a menos que sepamos muy bien lo que vamos a hacer. Muchas de las configuraciones que guardamos se pueden editar más fácilmente desde el Panel de control.

6. Los archivos VXD son drivers de dispositivos que administran los recursos del sistema. De esta forma, Windows funciona suavemente y sin problemas. No deberíamos involucrarnos (o tocarlos), a menos que sufriéramos repetidamente las típicas "pantallas azules" de cuelgue o que supiéramos de qué problema se trata y cómo resolverlo.

7. La sección [Inicio] es la más utilizada de las solapas del programa de configuración del sistema, y es aquí donde debemos desactivar cualquier programa que intente encenderse al mismo tiempo que Windows. Para removerlo, sólo debemos quitarle la tilde.

8. La solapa [Entorno] nos permite controlar las variables del entorno y los detalles del Path, que generalmente se encuentra en Config.sis y en Autoexe.bat, en el programa de configuración del sistema de Windows 98 o ME. La solapa [Internacional], por su parte, permite modificar las opciones de lenguaje, cambiar el código de país, y algunas cosas más.

¡Y dale con los drivers no firmados!

Cómo configurar Windows XP para evitar advertencias.

Windows XP incorporó un sistema de firma digital para los controladores (o drivers). Para que un controlador sea aceptado por Windows XP sin problemas, éste debe poseer un certificado digital que lo hace compatible con Microsoft. Supuestamente, esto garantiza que no tendremos problemas con el software. Si queremos instalar un driver no firmado, podemos hacerlo... pero Windows nos advertirá con un cartel de error que esto puede traernos problemas. En realidad, nadie puede asegurarnos esto: ni siquiera el mismo Windows.

Lo malo es que con cada nuevo hardware que instalemos, aparecerá un molesto ícono para "quitar el hardware con seguridad", ya que el sistema lo considerará "peligroso para la estabilidad". Para deshabilitar el control de controladores no firmados, hay que hacer clic derecho en el ícono de [Mi PC] y elegir [Propiedades]. Una vez allí, en la solapa [Hardware], hacemos clic sobre el botón [Firma de controladores]. En donde se nos pregunta [¿Qué acción desea que realice Windows?], conviene seleccionar [Ninguna: instalar el software sin pedir mi aprobación]. De esta manera, no volveremos a recibir la advertencia.

Personalizar carpetas en Windows XP Como modificar la configuración de las carpetas en Windows XP

Windows XP también permite personalizar las carpetas, aunque de una manera más avanzada. Para acceder a este cuadro de diálogo, vamos al menú [Ver/Personalizar carpeta] de la carpeta que queremos modificar. Aparecerá un cuadro de diálogo donde podremos elegir qué tipo de contenido contendrá la carpeta (Video, Imágenes o Música), y qué imagen se mostrará en la carpeta. Las carpetas MIS IMÁGENES y MI MÚSICA son ejemplos de carpetas personalizadas, aunque éstas no pueden repersonalizarse.

¡Alerta! ¡Presionaste la tecla!

Si ya estamos cansados de cometer errores cada vez que presionamos accidentalmente la tecla , o si nos volvemos locos tratando de escribir los números hasta que nos damos cuenta de que sin querer habíamos desactivado el teclado numérico, es hora de saber que Windows tiene una función para ayudarnos. Entrando en las opciones de accesibilidad del Panel de control y seleccionando la opción [ToggleKeys], recibiremos una alerta sonora cada vez que presionemos alguna de esas molestas teclas.

Abrir las carpetas en el Explorador

Como abrir por defecto las carpetas con el explorador de Windows. Podemos determinar que todas las carpetas se abran por defecto mediante el Explorador de Windows. De esta forma, tendremos las dos ventanas: las carpetas y los archivos a la derecha, y el árbol a la izquierda. Para hacer este cambio tenemos que abrir cualquier carpeta y elegir el menú [Ver/Opciones de carpeta]. En la solapa [Tipos de archivo] buscamos [Carpeta] y hacemos clic en el botón [Editar]. En [Acciones] veremos que open está en negrita, lo que indica que es la acción predeterminada. Nosotros debemos hacer clic sobre [Explore] para seleccionarla, y luego sobre el botón [Predeterminada]. Ahora Explore aparecerá en negrita. Sólo hay que hacer doble clic en cualquier carpeta para probarlo.

¿Dónde están Mis Documentos?

Donde almacena Windows XP todos los documentos. Por defecto, Windows guarda todos los archivos en la carpeta MIS DOCUMENTOS, a menos que especifiquemos otra ubicación. Generalmente, esta carpeta se encuentra en el directorio raíz de la unidad en la que tenemos instalado Windows. Si contamos con múltiples usuarios en nuestra computadora, cada uno tiene su propia carpeta MIS DOCUMENTOS, ubicada en **C:\DOCUMENTS AND SETTINGS\USUARIO\MIS DOCUMENTOS.**

Personalizar los Favoritos

La carpeta FAVORITOS de Windows puede sernos de gran utilidad, principalmente porque es de fácil acceso desde cualquier cuadro de diálogo de apertura o guardado de archivos, desde el menú [Inicio] o desde los menúes [Favoritos] de Outlook y del Explorador de Windows. El sistema operativo de las ventanas utiliza esta carpeta sobre todo para almacenar las páginas web favoritas de Internet Explorer. Lamentablemente, no puede ser compartida con otros exploradores, de modo de tener una única ubicación de favoritos; pero sí puede utilizarse para guardar archivos, carpetas o accesos directos, y facilitarnos así la exploración.

En primer lugar, vamos a crear una forma más rápida de agregar archivos y accesos directos a esta carpeta. Para ello, realizaremos un acceso directo a la carpeta FAVORITOS en la carpeta SENDTO de Windows. Ésta guarda todas las opciones que aparecen en el menú [Enviar a] al hacer clic derecho en un archivo.

Si utilizamos versiones anteriores a Windows XP, estas carpetas se encuentran en la ubicación C:\WINDOWS. En Windows XP, en cambio, están en **C:\DOCUMENTS AND SETTINGS\%USUARIO%.**

Si no encontramos la carpeta SENDTO, es posible que no tengamos habilitada la opción para ver archivos ocultos. Para habilitarla, hay que seleccionar [Herramientas/Opciones de carpeta] y luego la opción [Ver/Mostrar todos los archivos y carpetas ocultos].

A continuación, seleccionemos la carpeta FAVORITOS y la arrastramos con el botón derecho del mouse hasta la carpeta SENDTO. Cuando la soltemos, aparecerá un menú contextual, en el cual tendremos que seleccionar [Crear íconos de acceso directo].

Si ahora entramos en la carpeta SENDTO, veremos que se ha creado un nuevo archivo: Acceso directo a Favoritos. Vamos a probar si funciona. Dirijámonos hacia alguna carpeta que contenga algún archivo o carpeta que queramos agregar a los [Favoritos]. Para enviarlo a [Favoritos], primero vamos a crear un acceso directo al elemento (no queremos mover la ubicación del objeto original). Para ello, hacemos clic derecho sobre él y seleccionamos la opción [Crear acceso directo]. Ahora sí, hacemos clic derecho sobre el acceso directo recientemente creado y seleccionamos [Enviar a/Acceso directo a Favoritos]. El acceso directo ya se habrá movido a esta carpeta.

Mostrar MI PC en el Escritorio

Si instalamos Windows XP desde cero (Disco Formateado) no la actualización, por defecto, Windows nos muestra el Escritorio vacío, sólo con la Papelera de reciclaje. Para solucionar esto, hacemos clic derecho en el Escritorio y seleccionamos [Propiedades]. Allí nos dirigimos a la solapa [Escritorio] y hacemos clic en [Personalizar Escritorio]. En la nueva ventana podemos elegir los íconos que queramos, tanto el de MI PC como el de Internet Explorer y demás.

Inhabilitar el beep Molesto de los Errores en Windows XP

Para inhabilitar el beep (el sonido que hace Windows al encontrar un error), abrimos el Editor de Registro y vamos a [HKEY_CURRENT_USER\Control Panel\Sound]. Allí hacemos doble clic en la clave [Beep] y cambiamos su valor a [no].

Inhabilitar servicios innecesarios

Personalizar los programas de inicio en Windows XP. Al iniciarse, Windows ejecuta muchos programas que permanecen cargados en segundo plano, y que a veces son innecesarios. Estos programas suelen consumir memoria útil. Para personalizar los programas para el inicio, nos dirigimos a [Inicio/Ejecutar] y tipeamos services.msc. En la ventana que aparece, hacemos clic derecho sobre el servicio que deseamos inhabilitar y elegimos [Propiedades]. En la opción [Tipo de inicio] (Startup type) seleccionamos [Deshabilitado] (Disabled).

Programitas que se cargan al Inicio II

La otra opción para evitar que ciertos programas innecesarios se carguen al iniciar Windows XP es muy fácil, en el cuadro [Ejecutar] escribimos MSConfig, alli se nos abrirá el programa de configuración de Sistema, luego solapa [Inicio] y alli podemos destildar lo que creamos podemos prescindir al arrancar Windows, esto no significa que luego no podamos utilizar dichos programas.

Remover los documentos compartidos

Cómo quitar la opción Documentos Compartidos en Windows XP. Para quitar de MI PC la opción [Documentos Compartidos] (Shared Documents), abrimos el Editor de Registro y nos dirigimos a la rama
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\DelegateFolders].
Allí localizamos la rama **{59031a47-3f72-44a7-89c5-5595fe6b30ee}** y la borramos. Reiniciamos y ¡listo!

Habilitar la defragmentación del booteo

Windows XP incluye una nueva opción, que es la habilidad para defragmentar el área de booteo.

Esto ubica todos los sectores de booteo juntos para un inicio más rápido. Para habilitarla o inhabilitarla, hacemos lo siguiente:

Iniciamos el Editor de Registro y vamos a la rama
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction].
Seleccionamos la opción [Enable] de la derecha, y cambiamos su valor a Y para habilitarlo, o a N para inhabilitarlo.

Mensaje al inicio de Windows

Esto puede ser útil para dejar recordatorios, que se mostrarán al iniciar XP. Si queremos que, al iniciar, Windows nos muestre un mensaje con el texto que deseemos, debemos hacer lo siguiente:

Abrimos el Editor de Registro y vamos a la rama
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon].
Ahí modificamos el valor de legalnoticecaption con el título del mensaje y legalnoticetext con el texto del mensaje. Luego reiniciamos la computadora.

Acelerar la exploración en Windows XP

Cómo recorrer el disco rápidamente. Para poder explorar el disco rígido más rápidamente, debemos hacer lo siguiente:

Abrimos el Editor de Registro ([Inicio/Ejecutar] y escribimos “regedit”), y nos dirigimos a la rama
[HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Explorer/RemoteComputer/NameSpace].
Allí veremos una rama con el nombre “{D6277990-4C6A-11CF-8D87-00AA0060F5BF}”.

Esta rama le especifica a Windows que busque tareas programadas. Si lo deseamos, podemos hacer un backup antes de realizar algún cambio, en caso de querer recuperar la configuración.

Administración de memoria

Cómo administrar la memoria en Windows XP. Las claves que les mencionamos a continuación sirven para poder mejorar la administración de memoria y dar un poco más de velocidad a ciertos procesos. Todas las claves se encuentran en:

[HKEY_LOCAL_MACHINE/System/CurrentControlSet/SessionManager/MemoryManagement]

DisablePagingExecutive: cuando esta clave está habilitada, previene que los archivos “ejecutivos” sean enviados al archivo de paginación del disco rígido, lo que hace que el sistema operativo y los programas respondan más rápido. Recomendamos realizar esto sólo si tienen una gran cantidad de memoria RAM (más de 128 MB), ya que esto consume muchos recursos del sistema. Por defecto, viene inhabilitado, y para habilitarlo deben cambiar su valor de 0 a 1.

LargeSystemCache: este seteo (que, por defecto, viene habilitado en Windows 2000 Server) le pide al sistema operativo que lleve todo, menos 4 MB (que se mantienen por si necesita hacer caching del disco), de la memoria del sistema al sistema de caché de archivos. El principal efecto

de esto es permitir que el kernel del sistema operativo esté cacheado, lo que aumenta la velocidad de respuesta. Este parámetro es dinámico, y si se llega a necesitar más de 4 MB para hacer cacheo de disco por alguna razón, el espacio ocupado será liberado. Tengan en cuenta que, en ciertos casos, habilitar esta opción puede causar una reducción en la performance de ciertas aplicaciones que tienen usos intensos. Por ejemplo, en el caso de SQL Server, que tiene su propio sistema de cacheo de memoria, o de Internet Information Server, el cual funciona mejor con la mayor cantidad de memoria RAM disponible.

IOPageLockLimit: esta opción brinda un aumento de velocidad en las operaciones de entrada/salida cuando está haciendo gran cantidad de transferencias de archivos u operaciones similares. Se recomienda para sistemas que poseen mucha RAM (así que ni se molesten si no tienen más de 128 MB). Con un valor de entre 8 y 16 MB, notarán un aumento de performance. Esta clave requiere que estemos en bytes, por lo que deben multiplicar la cantidad de megabytes que quieran por 1024 y, luego, poner ese valor. Y sí, con éste hay que probar hasta encontrar el mejor.

Agregar tapas a las carpetas

Con este truco, podremos reconocer fácilmente las carpetas que queramos en Windows XP. Una de las nuevas opciones que tiene Windows XP es la posibilidad de agregar una imagen a la carpeta, para poder reconocerla cuando investigamos el disco. Utilizamos esta opción cuando copiamos un álbum (en el formato WMA), y nos permite asignarle a la carpeta la tapa del CD creado.

Si queremos asignarle una imagen a una carpeta que no contenga CDs, o que tenga un CD pero hecho por nosotros en MP3, podemos personalizarla y elegir la imagen, pero esto lleva tiempo si son varias carpetas. Una alternativa mucho más simple es copiar la imagen que queremos a la carpeta por modificar, y renombrar el archivo a FOLDER.JPG. Así, Windows XP asignará automáticamente esa imagen a la carpeta.

Reglas Básicas para la Seguridad de tu plataforma Windows como usuario conectado a Internet.

1- Actualizar a la última Release (Edición) de la última plataforma publicada para usuarios del OS MS-Windows http://www.microsoft.com (XP Pro o Corporativo recomendado)ya que es mucho mas estable que sus predecesoras.

IMPORTANTE: Es extremadamente peligroso dejar este archivo en XP : uplddrvinfo.htm. Vayan a C:\Windows\PCHEALTH\HELPCTR\SYSTEM\DFS y borren el archivo uplddrvinfo.htm

2- Hacer Update (Es gratuito) del sistema http://www.windowsupdate.com visitar ese link y bajarse las actualizaciones disponibles - Deshabilitar el sistema de Update automático. Ahorrarás recursos y Microsoft te enviará un mail cuando necesites actualizar. (Ver siguiente punto)

3- Para estar al día con la seguridad de tu Windows: www.microsoft.com/security suscribirse al boletín de seguridad de Microsoft - Envía un mail vacio a: securbas@microsoft.com y sigue los pasos.

4- Instalar un Firewall Profesional - Los "Pro" tienen la opción de setear el filtrado de protocolos y

puertos a gusto de cada uno, en cambio el común viene por Default - Zonealarm Plus (nuevo) Instalar y configurar completamente, salpimentar a gusto.

ZoneAlarm Pro v3.5.169 Final

5- Deshabilitar *servicios* inútiles o puertos abiertos desde Services. Desde Administración del sistema se deshabilita por ejemplo Netbios,Unpnp,Telnet...

b Deshabilitar *programas* que se cargan inutilmente desde el inicio con: http://www.vtoy.fi/jv16/programs/RegCleaner.exe y mucho mas se puede hacer, pero ojo que manipular el registro y no saber, puede tener efectos nocivos para el OS.

6- Instalar Antivirus, actualizar, configurarlo y escanear, que monitoree actividad maliciosa en background* (*En tiempo real y files que se ejecutan) e e-mails. Recomendado: Symantec Norton Antivirus 9.0 2003

7- Instalar Antitroyano, actualizar, configurarlo y escanear, que monitoree en background*. Recomendado The Cleaner www.microsoft.com - *Ejecutar TCActive! –

8- Instalar P.G.P 8.0 Final version. Solo el Plugin del Outlook Express y Pgp key management, Con ello podras encriptar y firmar emails entre amigos, ademas de mailearse y que ningun admin de ISP o intruso te lea información importante.

9- Steganos Security Suite 4.15
Plataforma de seguridad en español: Disco rígido protegido, borrado seguro, esteganografía, bloqueo de pc, codificador/decodificador y administrador de contraseñas.

10- Norton System Works 2003 http://www.symantec.com - Instalar, configurar y dar un service completo - One button ckeckup, Ejecutar Norton System Works apretar Begin Scan, abajo a la derecha de la pantalla Inicial del programa. Al finalizar: Begin Fix

Reglas Bàsicas Generales para Windows XP

1-Mails: No ejecutar archivos atachados y tratar de manejarse solo con mails en texto plano, no HTML. No contestar mails de desconocidos desde el Outlook ya que damos a conocer nuestra posición en la red a través de la dirección IP. Recomendacion ; Mirar primeramente los E-Mails desde www.mail2web.com ingresando tu Login y password alli los que tienen atach los eliminas directamente desde el servidor y luego bajas solo los que te interesan (El servicio de Mail2web es gratuito y ni siquiera te piden registrarte).

2- No escribir sobre cosas personales ni dato alguno a desconocidos (pueden serle utiles para un futuro hackeo) http://derecho-internet.org/teoria.php?teoria_id=38 que aparecen por IRC, ICQ, E-Mails, Webchat, Teléfono, en la calle, en los sueños... Si los das procurate de que sea alguien de confianza y asegurate de que la seguridad de su pc este en buen estado. No aceptes archivos en IRC, ICQ, FTPs, URL, de nadie desconocido que pueden ser un backdoor o troyano.

3- Instruir a la persona "de confianza" (Cuidado con el hack local mas que nada por empleados desleales o compañeros de trabajo) que le dejes la pc a cargo: Hermanos, empleados, parientes y amigos, coméntale los riesgos poniendolo al tanto de estas básicas para que nadie se aproveche de él en la net, más si recién comienza a navegar por la net. Educar principalmente a las secretarias, tanto con el telefono como la pc y la data que da de la empresa, su entorno o componentes.

4- Elegir buenas contraseñas http://www.cybsec.com/Claves.pdf de mas de 8 dígitos alfanuméricas, no usar por ejemplo el mismo login que el password o cosas como nombre de pila o comunes: 123456, " tu birthday " , 111222, "mascota", nataliateamo, admin, tu nick... o nombre de hija/o agus32, pablo82, etc

5- Siempre instalar los programas en modo Custom y no Standar, elegir cada componente a instalar. No instalar programas con Spyware, por ejemplo Kazaa y generalmente todos "famosos" freeware Chequear pc con Ad-aware 5.83 Plus Español

6- Huir de esos sitios web que te ofrecen descargar boludeces ejecutables!!! Lo mas probable es que bajes programas troyanizados, haya scripts malignos y files con viejos virus.

7- Cambia los passwords de tus sitios, casillas de mails y conexión cada cierto tiempo. No solo los administradores de tu ISP ven tus pass día a día, sino mucha gente externa, amigos de los admins e intrusos varios y amigos de estos. El programa Steganos tiene un agradable y útil administrador de passwords.

8- No entrar a los URLs que te recomiendan desconocidos, es muy facil hacer un "Fake Web" de "downloads" o puede ser algun server con Sircam u otro Worm. Puede ser tambien un sitio hecho para que bajes algun trojano sin saber o una falsa Gate o portal para chequear tu mail de Hotmail o Yahoo, falso obviamente.... o simplemente un link con una falla que te borre tu data. (Ver falla XP en punto 1b) En IRC manejese con precaución como asi en los distintos puntos de encuentro donde haya personas desconocidas y crean ser "hackers" con lo que ello significa.

9- En el caso de que uses: Scripts CGI y servicios como SSH, Openssl, Telnet, Ftp, IIS, Apache por ejemplo, actualizalos siempre a la ultima version y configuralos debidamente. Anótate en sus sitios para que te avisen de sus fallas y ultima versión... Por otro lado no le digas a todo el mundo el sofware que usas (y saca sus banners de version) como ser los de Servers, antivirus, firewalls...

10- No bajes patches, e-zines, programas, archivos u otra clase de programa de cualquier sitio tipico de *hack* (autenticos lamers molestos y dañinos) a no ser que sea algun mirror oficial o sitio de origen. El 99% de estos sitios, son hechos sacando cosas (ripeando) de otros sitios y muchos archivos pueden estar con troyanos, corruptos o viejos. (Estos desestabilizan a Windows)

Bloqueo de adjuntos en Outlook Express 6.0

Tanto Microsoft Outlook como Outlook Express, pueden ser configurados para bloquear lo que Microsoft llama datos adjuntos "no seguros" (ver "Nota 2" al final del artículo). Hasta el lanzamiento del nuevo Service Pack 1 de Outlook Express 6 (con el Internet Explorer 6), esta característica se encontraba deshabilitada por defecto (las versiones de Outlook Express anteriores a la 6, directamente no la poseían).

Pero en la nueva versión distribuida vía Windows Update por Microsoft (SP1), los usuarios se encuentran con esta opción habilitada por defecto, sin que hayan tenido que cambiar nada en la configuración del programa, lo que provoca que directamente no sean soportados la mayoría de los archivos adjuntos. En este caso, un mensaje del tipo "Outlook Express quitó el acceso al siguiente archivo adjunto no confiable en su correo", es mostrado al usuario.

Pero aunque pueda parecer una molestia, es MUY RECOMENDABLE que la mayoría de las personas dejen esta habilidad configurada de ese modo, ya que actualmente el uso maligno de los archivos adjuntos es mucho más común que su uso bien intencionado.
Sólo para dar uno de tantos ejemplos, en marzo de 2002 la Universidad James Madison de Estados Unidos, de 2607 mensajes con adjuntos tramitados por sus servidores, 2376 contenían virus. Otras referencias dan cifras muy similares.

Y además debemos recordar que de marzo a octubre de 2002, la cantidad de virus que se aprovecha de los adjuntos en el correo electrónico para propagarse, ciertamente ha aumentado enormemente.

Lo aconsejable en estos casos, es NO ACEPTAR los adjuntos bloqueados por el Outlook Express. Y solo si la persona que le envía el adjunto lo hace a expreso pedido suyo, pedirle que lo vuelva a enviar, pero en un formato diferente, que no pueda ejecutarse por si solo hasta que su antivirus lo examine (por ejemplo, en un archivo .ZIP).

Por otra parte, debemos tener en cuenta que cada vez más proveedores están bloqueando este tipo de adjuntos, de modo que también por esa razón es saludable acostumbrarnos a evitarlos. Si a pesar de lo expuesto, usted desea recibir adjuntos "al viejo estilo", es decir sin que el Outlook Express lo impida, le damos a continuación la forma de hacerlo. Sin embargo, insistimos en que esta es una característica muy importante del OE6, y que si usted la deshabilita, quitará una protección muy útil contra adjuntos de alto riesgo, sobre todo aquellos usados por nuevos virus aún antes que los antivirus hayan actualizado sus bases de datos para detectarlos. Usted puede seleccionar habilitar todos o solo ciertos tipos de adjuntos peligrosos.

Deshabilitar solo ciertos tipos de adjuntos

1. Pinche en Inicio, Configuración, Panel de control
2. Haga doble clic en Opciones de carpetas (o Herramientas, Opciones de carpetas)
3. Pinche en la lengüeta "Tipos de archivos"
4. Localice la extensión del tipo de archivo que usted desea recibir sin que sea bloqueada por el programa, y señálela (si la extensión no está en la lista, usted deberá deshabilitar toda la protección contra adjuntos peligrosos como se indica más adelante).
5. Pinche en "Opciones avanzadas".
6. Desmarque la opción "Confirmar apertura después de la descarga".
7. Pinche en Aceptar

Nota 1: Sea prudente cuando realice esto. Cualquier archivo con esa extensión descargado de Internet podría ejecutarse con consecuencias nefastas para su computadora.

Deshabilitar enteramente la protección contra adjuntos peligrosos.

Si usted deshabilita esta opción, aumenta grandemente los riesgos de ser infectado por virus recién creados, que aún no sean reconocidos por su antivirus. El peligro puede ser muy grande, no lo olvide. Si aún así desea deshabilitar esta característica del OE 6, proceda de la siguiente manera:

1. Inicie el Outlook Express
2. Seleccione "Opciones" en el menú de herramientas
3. Seleccione la lengüeta "Seguridad"
4. Bajo "Protección contra virus", desmarque la opción "No permitir que se guarden o abran archivos adjuntos que puedan contener un virus".
5. Pinche en Aceptar

Nota 2: La documentación de Microsoft dice que la lista mencionada incluye todo tipo de archivo que pueda poseer scripts o código asociado a ellos. Sin embargo, los archivos usados por Microsoft Office (.DOC, .XLS, etc.), no están en esta lista, cuando de hecho pueden contener macros que los virus pueden utilizar para su acción.

Cómo conectar dos PCs con Windows XP

Compartir ocasionalmente archivos es, normalmente, la única necesidad de la mayoría de los usuarios. Por esta razón, montar una red casera utilizando tarjetas y cables de red se convierte en una solución relativamente cara. Sin embargo, otro modo de conectar dos PCs sería utilizando el puerto paralelo del que va provisto cualquier ordenador. Las instrucciones de este Paso a Paso son aplicables solamente a Windows XP. Lo único que necesitarás es un cable paralelo-paralelo que no debe confundirse con el cable paralelo de la impresora.

Paso 1. Crear una nueva conexión
Primero de todo, nos aseguramos que el cable está conectado a los puertos paralelos de los dos PCs e iniciamos los dos ordenadores. Comenzamos con el ordenador principal (host), pinchamos en el botón de Inicio y abrimos el Panel de control. Hacemos clic en el icono Conexiones de red. En la ventana emergente pincharemos la opción Crear conexión nueva.

Paso 2. Computadora principal
El asistente para la nueva conexión aparecerá. Pinchamos en Siguiente y, en la pantalla que obtenemos, seleccionamos Configurar una conexión avanzada antes de pulsar en el botón Siguiente. Ahora, elegimos Conectar directamente a otro equipo y, otra vez, hacemos clic en Siguiente. La siguiente pantalla nos mostrará la pregunta Host o invitado, donde decidiremos por Host, ya que este es la PC a la que queremos tener acceso. Por último, pulsamos en Siguiente.

Paso 3. Nuevo usuario
Una vez seleccionado el ordenador principal elegimos el recurso de conexión, de este modo pinchamos en el menú desplegable y seleccionamos Paralelo directo (LPT1). Ahora, pulsamos en Siguiente y nos pedirá que concedamos los permisos de usuario. Hacemos clic en Agregar y en la ventana Usuario nuevo tecleamos el nombre de usuario y la contraseña que utilizaremos para el PC invitado. Confirmamos la contraseña y pinchamos en Aceptar. Ahora, hacemos clic en Siguiente y en Finalizar. Además, tendremos que compartir las carpetas a las que el ordenador invitado tendrá acceso. Así, con el botón derecho del ratón pinchamos en cualquier disco o carpeta de Mi PC, seleccionamos Compartir y seguridad. Marcamos la opción Compartir esta tarjeta y le damos un nombre. Repetimos el mismo proceso para todas las carpetas que queramos que estén disponibles para el PC invitado.

Paso 4. PC invitada
En el PC invitado, realizamos de la misma manera los dos primeros pasos pero en vez de seleccionar la opción Host en el asistente para la nueva conexión, elegimos Invitado y pulsamos en Siguiente. Introducimos el nombre del ordenador con el que estamos intentando conectar. Si no le pusimos nombre cuando instalamos Windows XP, lo encontraremos pinchando con el botón derecho del ratón en Mi PC, seleccionando Propiedades y resaltando la pestaña Nombre de equipo donde aparecerá como Nombre completo de equipo. Para continuar pulsamos en el botón Siguiente.

Paso 5. Conexión de las dos Computadoras
En la siguiente pantalla seleccionamos Paralelo Directo LPT1 (que es el puerto de la impresora) y hacemos clic en Siguiente. Ahora, pinchamos en Finalizar y aparecerá la caja de diálogo Conectar. Tecleamos el nombre y la contraseña del nuevo usuario que añadimos en el Paso 3. Además, es posible marcar la opción Guardar este nombre y contraseña para los siguientes usuarios antes de pulsar el botón Conectar. Las dos PC's quedarán conectadas y aparecerá el correspondiente icono en la carpeta del sistema. Habrá, también, una nueva entrada en la sección Conexiones de red.

Como configurar el Firewall de Windows XP

Windows XP dispone de su propio Firewall para evitar ser vulnerable a cualquier ataque que provenga de la Red, y evitar que alguien pueda acceder a tus datos. En este artículo vamos a ver como se configura de una forma sencilla, para cualquier usuario de Windows XP. Hacemos clic en el botón Inicio, a continuación sobre Mis sitios de Red, y luego en Ver conexiones de Red. Pulsa una vez con el ratón izquierdo sobre el icono de tu conexión y luego en la parte derecha de la ventana pincha sobre, Cambiar la configuración de esta conexión.En la ventana que aparece pincha sobre la pestaña Avanzadas y activa la casilla Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet.

En la siguiente ventana todas las casillas deberán estar vacías. Si tienes alguna activada, debes desactivarla. Solo en el caso en que utilices alguno de estos servicios debes activar la casilla que corresponda a cada servicio, por ejemplo si tienes tu ordenador como servidor ftp, deberás activar dicha casilla.

Formatear una partición NTFS

En Windows XP el formateado del disco duro es algo mas complicado que el formateado de Windows 98, Me,... etc.

En este artículo vamos a tratar de explicarlo lo mas claro posible para que cualquier usuario de Windows XP siguiendo estas instrucciones pueda formatear su disco duro o partición sin ningún tipo de problema.

Para ello existen dos formas de hacerlo, según esté instalado Windows XP con el sistema de archivos FAT32 o NTFS. Así pues lo primero que debemos saber es con cual de los dos sistemas está instalado Windows XP.

Windows XP está instalado en NTFS. Para formatear la partición NTFS e instalar nuevamente Windows XP seguiremos estos pasos:

1. Con la PC apagada introducimos el disco nº 1 de instalación de Windows XP (en total son 6 discos) y arrancamos el ordenador.
2. A continuación vamos introduciendo los discos 2..3..4..5..6 según los vaya pidiendo.
3. Una vez haya cargado los 6 discos, nos ofrecerá las siguientes opciones. Instalar Windows XP, Recuperar la instalación de Windows XP o Salir del programa.
4. Escogeremos la opción de Instalar Windows XP, pulsando la tecla Intro. Insertamos el CD-ROM de Windows XP en el lector de CD´s y pulsamos nuevamente la tecla Intro.
5. Pulsamos la tecla F8 para aceptar el contrato de licencia y continuar con el proceso.
6. En la siguiente ventana tenemos nuevamente la opción de reparar la instalación de Windows XP o instalación Nueva. Escogemos la opción Instalación nueva y presionamos la tecla ESC. para continuar.
7. En la siguiente pantalla vemos todos los discos y particiones, con tres opciones. Instalar Windows XP. Crear nueva partición, o Eliminar la partición seleccionada.
8. Ahora vamos a eliminar la partición, para ello la seleccionamos y pulsamos la tecla D y luego la tecla L para eliminarla.
9. En el cuadro de particiones veremos que ha desaparecido el nombre de unidad que tenía y en su lugar aparece el texto Espacio no particionado. Seleccionamos el texto de Espacio no particionado y pulsamos la tecla C para crear una nueva partición. Mostrará el espacio que queda libre en el disco, en este caso lo dejamos como está ya que lo que pretendemos es formatear y cargar nuevamente Windows XP (pero podríamos modificar el tamaño de la partición o hacer una nueva partición con menos tamaño de disco). Pulsamos la tecla Intro.

10. Ahora en el cuadro de particiones aparecerá con el nombre de unidad (Por ejemplo F:\) a continuación pulsamos la tecla Intro para continuar con la instalación.
11. En la siguiente ventana aparecerán las opciones para Formatear la partición, escogemos la opción de formatear en NTFS y comenzará de inmediato a formatear la partición.
12. Una vez que termine de formatear la partición continuará automáticamente la instalación de Windows XP, y tan solo tenemos que seguir las instrucciones que van apareciendo en pantalla, hasta terminar la instalación de Windows XP.

Formatear una partición FAT32

De todos los usuarios de Windows XP es sabido los problemas que origina el sistema operativo a la hora de formatear el disco duro, pues bien, con este truco vamos a ver como se formatea el disco duro en FAT32 de forma sencilla.

Lo primero que debemos saber e si el disco duro está en NTFS o FAT32, una vez sepamos que está en FAT32 la manera de formatear el disco duro es idéntica a como se hace con Win95m 98, Me es decir con el disco de inicio de Windows, vale cualquier disco de cualquier Windows.

1. Con la PC apagada introducimos el disco de inicio de Windows 95, 98 o Me.
2. Arrancamos el sistema y comenzará a cargar los archivos de inicio.
3. Una vez los haya cargado se quedará en A:\>
4. Tecleamos Format C: y pulsamos la tecla Intro, a continuación nos avisará de que se van a perder los datos que no hayan sido guardados, lo aceptamos y comenzará a formatear el disco duro o la partición.
5. Una vez que termine, ya tendremos preparado el disco duro para cargar nuevamente Windows XP con el sistema de archivos FAT32.

Nota: Si el disco rigido se encuentra con el sistema de archivos NTFS no nos dejará formatear de esta forma.

Crear discos de instalación

Donde y como se pueden crear los discos de instalación de Windows XP. Si bien a última hora en el CD-ROM de instalación de Windows 2000 se incluyeron las imágenes para poder crear los discos de arranque en aquellos equipos que no soportasen el arranque desde CD-ROM, por alguna razón no se han incluido en el disco de instalación de Windows XP.
En su defecto, podemos descargar las imágenes de los seis discos de instalación, tanto para la edición Home como para la Profesional:

- **Discos de arranque de Windows XP para la edición Home**
- **Discos de arranque de Windows XP para la edición Professional**

Crear discos de contraseñas

Si estás ejecutando Windows XP Profesional como usuario local en un entorno de grupo de trabajo, puedes crear un disco de restablecimiento de contraseñas para iniciar sesión en el equipo cuando olvides la contraseña. Para crear el disco, sigue estos pasos:

1. Haz clic en Inicio, en Panel de control y, a continuación, en Cuentas de usuario.
2. Haz clic en tu nombre de cuenta.
3. Debajo de Tareas relacionadas, haces clic en Prevenir el olvido de contraseñas.
4. Sigue las instrucciones del Asistente para contraseña olvidada con el fin de crear un disco de restablecimiento de contraseña. 5-Guarda el disco en un lugar seguro, ya que cualquiera que lo utilice puede tener acceso a su cuenta de usuario local.

Cómo Proteger tu Windows XP con ZoneAlarm

Explicamos cómo utilizar Zone Alarm, una de las mejores maneras de estar protegidos frente a los peligros que acechan en la Red. Siga los siguientes pasos:

1. Luego de instalarlo (punto en que se nos preguntará qué tipo de conexión poseemos), Zone Alarm nos brindará un pequeño tutorial en el que nos informa las características del programa en varios pasos. Allí avisa que primero hará muchas preguntas, pero que luego éstas irán disminuyendo.

2. Éste es el cuadro de diálogo que veremos cuando una nueva aplicación intente acceder a Internet. Podemos ver el ejecutable que la inició, la IP de destino y el puerto que se está intentando utilizar. El checkbox evita que vuelva a consultar sobre este programa.

3. Éste es un caso especial de los programas que establecen conexiones directas, ya que necesitan privilegios de servidor para funcionar correctamente. Con el botón [More Info] seremos dirigidos al sitio web para obtener información adicional (en todos los casos).

4. Este cuadro nos indica que Zone Alarm ha bloqueado el tráfico hacia nuestro equipo, además de darnos la IP de origen y el tipo de servicio o puerto al cual está intentando acceder. Si marcamos el checkbox, la alarma se guardará pero no veremos un pop-up que nos lo informe.

5. Esta ventana permite configurar el candado que cerrará todas las conexiones a Internet. También podemos configurarlo para que se active automáticamente y permita que algunos programas ignoren su bloqueo y mantengan sus conexiones.

6. Los niveles de seguridad afectan el tráfico que será bloqueado por Zone Alarm. A la izquierda se encuentra el tráfico de nuestra red local (si existe) y a la derecha, el tráfico de Internet. Para redes hogareñas, conviene dejar el local en mínimo y el de Internet en máximo.

7. Todos los permisos de los programas que intentaron acceder a Internet pueden ser modificados desde aquí. Podemos negar el acceso, permitirlo o hacer que se nos consulte la próxima vez que lo intente. Es posible permitir acceso sobre el candado con el checkbox.

8. Lo que se ve en la imagen es el historial de alertas desde que se inició Zone Alarm. Podemos hacer que se loguee todo a un archivo de texto y, si lo deseamos, que se muestren los pop-ups. El botón [More Info] brinda información desde el sitio web de Zone Alarm.

Mejorar ancho de banda del XP Professional

Windows XP se reserva el 20% del ancho de banda disponible, con el fin de ejecutar aplicaciones especiales. La “retención” se produce mediante el denominado el programador de paquetes QoS (Quality of Service – Calidad del Servicio), encargado de la optimización de redes locales.

Sin embargo, para los usuarios privados, que sólo tienen un PC en casa, QoS no es una función necesaria; sino todo lo contrario. Windows XP reserva el 20% del ancho de banda aunque el usuario cancele la función QoS. También se puede optar por desintalar el Programador de paquetes QoS si no tenemos ninguna Red Local.

1) Entrar como administrador.
2) Inicio, ejecutar, escribid: gpedit.msc
3) Aparecen las directivas de grupo, id a Configuración de Equipo.
4) Plantillas Administrativas
5) Red (Network)
6) Programador de Paquetes Qos

7) Doble click en Limitar el ancho de banda reservado
8) Habilitarlo y poner el 0% en Límite de Ancho de Banda.
9) Aplicar y Aceptar
10) Id a propiedades red y comprobad que está marcado el Programador de Paquetes Qos. Opciones de Inicio, Servicios, System.ini, boot.ini, etc
11) Inicio, Ejecutar "msconfig" (sin las comillas)

Instalar Windows XP en equipos con menos de 64 Mb de RAM

Como norma general, Windows XP necesita un mínimo de 64 Mb de RAM para completar con éxito la instalación. Si bien el rendimiento se verá reducido sensiblemente, podemos instalar Windows XP en equipos con 32Mb de RAM. Para ello deberemos copiar los archivos “txtsetup.sif” y “dosnet.inf” en un directorio temporal. Editaremos el primeros de los archivos, cambiando el valor del parámetro “RequiredMemory” por “33030144”. Realizaremos la misma tarea con el archivo “dosnet.inf”, cambiando el parámetro “MinimumMemory” por “33030144”. Por último, desde el intérprete de comandos iniciaremos el programa de instalación con la instrucción **winnt32 /m:C:\Nombre_directorio_temporal<&I>** para que obvie los archivos incluidos en el cd-rom de instalación y utilice los archivos de instalación modificados anteriormente.

Configuración de sistema en Windows XP

Veamos cómo sacarle un peso de encima a nuestra computadora, optimizando los recursos que ya tenemos a mano. Siga los siguientes pasos::

1. Para acceder a las herramientas de configuración del sistema, vamos a **[Inicio/Programas/Accesorios/Herramientas del sistema/Información del sistema].** Una vez abierta la ventana de [Información del sistema] de Microsoft, vamos a [Herramientas/Programas de configuración del sistema].
2. Si nuestro sistema operativo es Windows Millennium, tardaremos mucho en encontrar las utilidades del System Config, porque tendremos que pasar por la ayuda del sistema. Sin embargo, podemos acceder escribiendo "msconfig" en el menú [Ejecutar].
3. En la solapa [General], podemos setear qué tipo de inicio queremos y elegir qué archivos del proceso se ejecutarán cuando Windows arranque. Si tenemos Windows Me o XP, también podemos usar [Iniciar Restaurar Sistema], para que el sistema vuelva al estado anterior.
4. En System.ini encontramos el residuo de los sistemas de 16 bits; están incluidos en los sistemas de 32 bits de Windows 95/98/Me/XP, para conservar la compatibilidad con las aplicaciones viejas. El archivo System.ini tiene información sobre drivers, sobre DLLs y sobre passwords necesaria para iniciar el sistema. Se puede activar o desactivar algo de Sistem.ini desde esta solapa.
5. Al igual que Sistem.ini, Win.ini fue reemplazado por el registro; pero todavía tiene un fin. Hay que evitar realizar cualquier cambio en este archivo, a menos que sepamos muy bien lo que vamos a hacer. Muchas de las configuraciones que guardamos se pueden editar más fácilmente desde el Panel de control.
6. Los archivos VXD son drivers de dispositivos que administran los recursos del sistema. De esta forma, Windows funciona suavemente y sin problemas. No deberíamos involucrarnos (o tocarlos), a menos que sufriéramos repetidamente las típicas "pantallas azules" de cuelgue o que supiéramos de qué problema se trata y cómo resolverlo.
7. La sección [Inicio] es la más utilizada de las solapas del programa de configuración del sistema, y es aquí donde debemos desactivar cualquier programa que intente encenderse al mismo tiempo que Windows. Para removerlo, sólo debemos quitarle la tilde.
8. La solapa [Entorno] nos permite controlar las variables del entorno y los detalles del Path, que generalmente se encuentra en Config.sis y en Autoexe.bat, en el programa de configuración del sistema de Windows 98. La solapa [Internacional], por su parte, permite modificar las opciones de lenguaje, cambiar el código de país, y algunas cosas más.

CÓMO: TOMAR POSESIÓN DE UN ARCHIVO O DE UNA CARPETA

Resumen
En este artículo se describe cómo tomar posesión de un archivo o de una carpeta para los que tiene denegado el acceso. Si necesita tener acceso a un archivo o a una carpeta para los que no tiene acceso (permiso), debe tomar posesión de dicho archivo o carpeta, donde debe reemplazar los permisos de seguridad para permitirse a sí mismo el acceso.

Cómo tomar posesión de una carpeta

NOTA: debe haber iniciado sesión en el equipo con una cuenta que tenga privilegios administrativos.

Para tomar posesión de una carpeta:

1. Haga clic con el botón secundario del mouse (ratón) en la carpeta de la que desee tomar posesión y, a continuación, haga clic en Propiedades.
2. Haga clic en la ficha Seguridad y, después, haga clic en Aceptar en el mensaje de seguridad (si aparece alguno).
3. Haga clic en Avanzadas y, después, haga clic en la ficha Propietario.
4. En la lista Nombre, haga clic en su nombre de usuario, en Administrador si ha iniciado sesión como Administrador o en el grupo Administradores. Si desea tomar posesión del contenido de dicha carpeta, haga clic para activar la casilla de verificación Reemplazar propietario en subcontenedores y objetos.
5. Haga clic en Aceptar. Aparecerá el siguiente mensaje, donde nombre de carpeta es el nombre de la carpeta de la que desea tomar posesión: No tiene permiso de Lectura sobre el contenido del directorio nombre de carpeta . ¿Desea reemplazar los permisos del directorio por permisos que le concedan Control total? Todos los permisos serán reemplazados si contesta Sí. Haga clic en Sí.
6. Haga clic en Aceptar, y vuelva a aplicar los permisos y la configuración de seguridad que desee para la carpeta y su contenido.

Cómo tomar posesión de un archivo

NOTA: debe haber iniciado sesión en el equipo con una cuenta que tenga privilegios administrativos.

Para tomar posesión de un archivo, siga estos pasos:

1. Haga clic con el botón secundario del mouse (ratón) en el archivo del que desee tomar posesión y, a continuación, haga clic en Propiedades.
2. Haga clic en la ficha Seguridad y, después, haga clic en Aceptar en el mensaje de seguridad (si aparece alguno).
3. Haga clic en Avanzadas y, después, haga clic en la ficha Propietario.
4. En la lista Nombre, haga clic en Administrador, o haga clic en el grupo Administradores y, después, haga clic en Aceptar. El Administrador o el grupo Administradores es ahora el propietario del archivo. Para cambiar los permisos de los archivos y las carpetas que hay bajo esta carpeta, continúe en el paso 5.
5. Haga clic en Agregar.
6. En la lista Escriba los nombres de objeto que desea seleccionar (ejemplos), escriba la cuenta de usuario o de grupo a la que desea conceder acceso al archivo. Por ejemplo, Administrador.
7. Haga clic en Aceptar.
8. En la lista Nombres de grupos o usuarios, haga clic en la cuenta que desee (por ejemplo, Administrador) y, después, haga clic para activar las casillas de verificación correspondientes

a los permisos que desee asignar a dicho usuario. Por ejemplo, Control total [Permitir]. Cuando termine de asignar permisos, haga clic en Aceptar.

Conocer información básica de nuestra máquina y TODOS los hotfixes instalados (para XP Profesional)

En una ventana de comandos (cmd.exe) ejecutar: systeminfo
Si se necesita que dé los datos en un fichero de texto, teclear: **systeminfo > c:\informe.txt**
Esto dejará un fichero llamado informe.txt con el resultado del comando anterior.

Este comando sirve tanto para ver la máquina local, como para poder ver máquinas remotas en nuestra red. La sintaxis completa del comando es:

systeminfo[.exe] [/s Computer [/u Domain\User [/p Password]]] [/fo {TABLE|LIST|CSV}] [/nh]

Parameters:

/s Computer
Specifies the name or IP address of a remote computer (do not use backslashes). The default is the local computer.

/u Domain\User
Runs the command with the account permissions of the user specified by User or Domain\User. The default is the permissions of the current logged on user on the computer issuing the command.

/p Password
Specifies the password of the user account that is specified in the /u parameter.

/fo {TABLE|LIST|CSV}
Specifies the format to use for the output. Valid values are TABLE, LIST, and CSV. The default format for output is LIST.

/nh
Suppresses column headers in the output. Valid when the /fo parameter is set to TABLE or CSV.

/?
Displays help at the command prompt.

SOLUCIÓN A LOS ERRORES TÍPICOS DE BOOT

En todos los casos:

1) Arrancar con el CD de XP (es booteable). Si no arrancase, entrar en la Bios y modificar los parámetros para que arranque primero desde CD.
2) En la primera pantalla, seleccionar "R" para entrar en la consola de recuperación.
3) Seleccionar el Windows que queremos reparar. Típicamente será el #1
4) Cuando nos lo solicite, teclear la password del usuario "Administrador". No confundir con la password de un usuario con atributos de administrador. La password del usuario Administrador (que está oculto), es, en XP Profesional, la que se puso durante la instalación del sistema. En XP Home, está sin password. Ambas, posteriormente han podido ser cambiadas.

NTOSKRNL Missing or Corrupt

a) Realizar los puntos 1) a 4) del inicio de este documento. Cambiar a la unidad de CD. Típicamente será la D: si solo tenemos una partición. Cambiar por la letra correspondiente en otro caso.
D:
cd i386
expand ntkrnlmp.ex_ C:\Windows\System32\ntoskrnl.exe

Si Windows XP estuviese instalado en otra localización distinta de c:\Windows, sustiuirla en el comando anterior.

HAL.DLL Missing or Corrupt

a) Realizar los puntos 1) a 4) del inicio de este documento. Ejecutar:
bootcfg /list nos mostrará la lista en el boot.ini
bootcfg /rebuild reparará este.

Corrupted or Missing \WINDOWS\SYSTEM32\CONFIG\SYSTEM

a) Realizar los puntos 1) a 4) del inicio de este documento. Ejecutar:
cd \Windows\system32\config
ren config config.bad
copy \Windows\repair\system

Corrupted or Missing \WINDOWS\SYSTEM32\CONFIG\SOFTWARE

a) Realizar los puntos 1) a 4) del inicio de este documento. Ejecutar:
cd \Windows\system32\config
ren software sftware.bad
copy \Windows\repair\software

NTLDR or NTDETECT.COM Not Found

a) Realizar los puntos 1) a 4) del inicio de este documento. Suponemos que la unidad de cd es la letra D: (sustituirla en el comando posterior si fuese diferente):
COPY D:\i386\NTLDR C\:
COPY D:\i386\NTDETECT.COM C:

Cómo enviar un mail desde la consola de comandos de XP sin necesidad de tener un cliente de correo.

Configurar primero el SMTP.

Para ello, instalar el IIS desde Componentes de Windows (el IIS no está disponible para XP Home Edition, solamente para Pro)

Para configurarlo: ir a Panel de Control, Herramientas Adminsitrativas, Internet Information Services. Con el botón derecho sobre el server SMTP, darle a Propiedades. Pestaña de Acceso, boton de Conexión y autorizar a vuestra IP. Botón posteriormente de Relay (quizá este traducido por Reenvío) y autorizar también a vuestra IP.

Ahora teclear:
telnet nombre_de_vuestra_máquina 25

Helo
mail from: mail_del_que_envía@servidor.com (puede ser mentira)
rcpt to: mail_al_que_quereis_enviar@loquesea.com
data

Texto del mensaje..... lo que querais, puede ocupar varias líneas, y para finalizar teclead INTRO un punto e INTRO de nuevo

Y ya está...

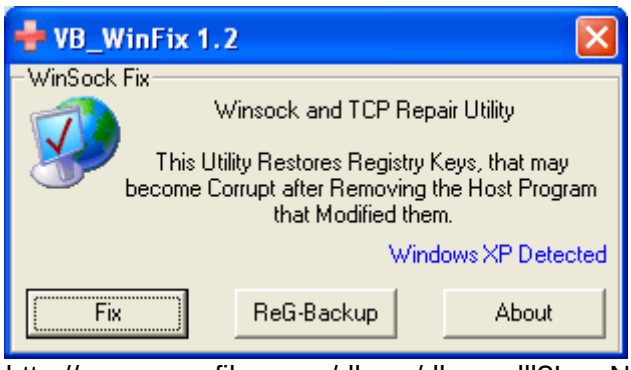
NOTA: La tecla retroceso no funciona -aunque el cursor retrocede, no borra- por tanto si os equivocais.... mala suerte ;-)

Probadlo..... ;-)

Para reinstalar el TC/IP en Windows XP:

Ir A: C:\windows\inf
Encontrar el archivo: nettcpip.inf
Click con el botón derecho, y luego "Instalar".
Listo!

La alternativa es hacerlo usando el WinSock XP Fix:



Descargar de:http://www.snapfiles.com/dlnow/dlnow.dll?Inc=No&ID=107303

ACELERAR EL ACCESO A LOS PROGRAMAS

Aunque tu equipo disponga de suficiente memoria RAM y puedas trabajar con varios programas sin problemas, el sistema de Windows XP siempre utiliza el Kernel para enviar y recibir archivos del archivo de paginación del disco duro, por este motivo la velocidad de respuesta es menor.

Si dispones de memoria RAM suficiente puedes seguir estos pasos para cambiar la configuración de tu Windows XP y obligarlo a que no lo pagine al disco y de esa manera aumentar el rendimiento:

Haz clic sobre el botón Inicio -> Ejecutar, escribe regedit y pulsa el botón Aceptar
Ahora navegamos en nuestro registro de Windows XP hasta ubicarnos en siguiente cadena:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SessionManager/MemoryManagement

Busca en el panel derecho la entrada DisablePagingExecutive y hacemos doble clic sobre ella.
En la ventana que aparece cambia el valor de 0 y pones 1 luego pulsa el botón Aceptar y reiniciamos nuestro Windows XP

Habremos conseguido con ello más velocidad de acceso a los programas, porque ahora nuestro Windows XP utilizará menos el disco duro.

ACELERAR EL MENU INICIO Y LIBERAR MEMORIA RAM

ACELERAR EL MENU DE INICIO

El menú de inicio de Windows XP, aparte de ser extremadamente grande, es también demasiado lento en su despliegue. Si deseas acelerar la velocidad en que se muestra este menú, accede al registro de Windows.

Una vez allí deberás llegar hasta la opción: MenuShowDelay. Para ello sigue la secuencia: **HKEY_CURRENT_USER * Control Panel * Desktop * MenuShowDelay;**
O búscala directamente con la opción "buscar" de regedit. Una vez localizada haz doble clic sobre esta opción y cambia el valor que por defecto esta en (400) por un valor menor. Pon el valor "0" para conseguir la mayor velocidad.

Seguidamente pulsa el botón Aceptar y luego reinicia tu ordenador para que los cambios tengan efecto y puedas ver la diferencia.

LIBERAR MEMORIA RAM

Tras haber ejecutado una o múltiples aplicaciones o juegos que hagan uso intensivo de los recursos del sistema, habremos detectado que Windows queda algo lento.

Esto es debido a que los restos de las aplicaciones usadas, bloquean parte de la RAM que han utilizado, ocasionando lo que se llama fragmentación de memoria.

Mediante un pequeño script podemos liberar esa memoria , forzando al ordenador a descargar el contenido de la memoria al archivo de intercambio de forma que recargue de nuevo toda la información activa en la memoria y deseche la información no útil, de la siguiente forma:

Abrimos el bloc de notas de Windows y dependiendo de la memoria de nuestro ordenador escribiremos los siguientes valores:

Si tienes menos de 128 Mb de memoria RAM, escribes Mystring=(16000000)
Si tienes 128 Mb de memoria RAM o más escribes Mystring=(80000000)

Ahora guarda este archivo en el lugar que quieras, con el nombre liberar.vbe debes poner la extensión .vbe ya que el nombre no importa puedes poner el que quieras.

Ahora hacemos doble clic sobre el archivo que acabamos de crear y Windows refrescará la memoria RAM.

Activar 2 MSN Hotmail en Windows XP

Windows XP trae un ícono de MSN, el cual no está configurado ni menos instalado. No debemos tener ninguna versión de MSN instalada a si que si alguien tiene por ejemplo la versión 6.0 o cualquiera debemos desinstalarla desde panel de control en agregar o quitar programas.

Una vez desinstalado el MSN nos vamos al icono de MSN que trae el Windows XP al activarlo se nos actualiza en una versión de 4.7, una vez instalado se procede a descargar una versión de MSN mayor a esta, puede ser 6.0 ó 6.1 (cualquiera) o si la tienes descargada mejor.

Después se instala la versión que se acaba de descargar (6.0 ó 6.1) y ya estamos listos nuestro pc queda trabajando con 2 MSN sin mayor problema ni de buscar programas que ayudan a eso como el polygramy así de simple. Ahora si quieres dejas como acceso directo cada ícono de cada MSN para que no se te pierdan.

ADMINISTRACION DE VENTANAS

Cambiar entre una ventana y una pantalla completa de MS-DOS

- Presione ALT+ENTRAR.
- Cerrar ventanas consecutivas
- Si está examinando múltiples ventanas y desea cerrar todas las que estén abiertas, presione la tecla MAYÚS y, sin soltarla, haga clic en el botón para cerrar (X) que encontrará en la esquina superior derecha de la barra de título.
- Cascada, Mosaico y Minimizar todo
- Con el botón secundario del mouse, haga clic en la barra de tareas y, a continuación, haga clic en la opción de su preferencia.

Resumen de configuración

- Para imprimir una copia del resumen de configuración del sistema, haga doble clic en el icono Sistema del Panel de control.
- Haga clic en la ficha Administrador de dispositivos.
- Por último, haga clic en PC y, a continuación, en Imprimir.

Apagado automatico

Para hacer que el sistema se apague automáticamente, lo único que hay que hacer es ir al panel de control: Inicio -> Configuración -> Panel de Control, haces doble clic sobre el icono Opciones de energía Una vez que se abra la ventana pinchas en la Pestaña APM, luego marcas la opción que sale que es Habilitar la compatibilidad con la administración de energía, ahora aceptas todo y cierras las ventanas, y listo para el apagado automático.

Apagado rapido del equipo

Vamos a crear un acceso directo en escritorio para apagar el equipo, rápidamente:

- Abrimos el bloc de notas, para ello Inicio->Todos los programas->Accesorios->Bloc de notas
- Escribimos: shutdown -s -t 05 –f
- Salvamos el el fichero como apaga.bat en C:\documents & settings\ el nombre de tu carpeta personal\Escritorio
- El comando shutdown usado con el parametro -s apaga el sistema.
- El parametro -t es seguido del numero los segundos que se esperará para que se apague el sistema.
- El parametro -f hace que se cierren todas las aplicaciones sin preguntar (si quieres que se te pregunte lo puedes omitir).

Averigua quien esta conectado a tu ordenador

Para saber quien esta conectado a tu ordenador, cuando te encuentras en Internet haz lo siguiente:

- Haces clic en el botón Inicio y luego en Todos los Programas
- Seleccionas Accesorios y luego Símbolos del sistema.
- En la ventana de Símbolo de sistema escribe netstat y pulsa la tecla Intro. Ahora en pantalla verás todas las conexiones que estás recibiendo.

Bloquear las barras de herramientas

Ahora en Windows XP las barras de herramientas se pueden bloquear y puedes ajustarlas.

Puedes personalizar muchas funciones de Windows XP como la Barra de tareas, el menú Inicio e incluso los iconos de la barra de tareas de Internet Explorer y de Outlook Express.

Recuerda el clic con el ratón derecho:

- Haz clic con el ratón derecho en una barra de herramientas y, a continuación, haz clic en Bloquear las barras de herramientas para quitar la marca de verificación.

- Haga clic de nuevo con el ratón derecho en la barra de herramientas y, a continuación, haz clic en Personalizar.
- Puedes agregar y quitar botones de la barra de herramientas, cambiar opciones de texto y opciones de iconos.
- Cuando tengas personalizada la barra de herramientas, haz clic en Cerrar. Ahora, haga clic con el ratón derecho en la barra de herramientas y, a continuación, haz clic en Bloquear la barra de herramientas para bloquearla automáticamente.

Bloquear pagina inicio de Internet Explorer

Para bloquear la página inicio de Internet Explorer y que ningún adware te la cambie procederemos de la siguiente manera:

Inicio -> Ejecutar -> Regedit
Ya una vez dentro del editor de registro nos desplazamos hasta:
HKEY_CURRENT_USER - Software - Policies – Microsoft

Una vez dentro de la carpeta Microsoft creamos una nueva clave, clic con el botón derecho:
Nuevo -> Clave -> Internet Explorer

Nos situamos en la nueva carpeta Internet Explorer recién creada y procedemos a crear una nueva clave, clic botón derecho - **Nuevo -> Clave -> Control Panel**

Ahora nos situamos en la carpeta Control Panel y creamos un valor DWORD, **clic botón derecho > Nuevo -> Valor DWORD -> Homepage**

Aqui procederemos a establecer su valor en 1, para ello seleccionamos Homepage , clic botón derecho -> Modificar -> Información valor = 1

Tener el valor a 1 significa el bloqueo ningun programa podrá cambiar nuestra página de inicio para nuestro Internet Explorer. Si le damos el valor 0 podremos volver a modificar la página de inicio predeterminada, en el caso de que deseemos cambiarla.

Borrar elementos pasados

Para borrar Elementos pasados de la barra de notificaciones de XP seguiremos estos pasos:

Hacemos clic sobre el botón Inicio -> Ejecutar escribimos Regedit y pulsamos el botón Aceptar
Una vez en el registro buscamos la siguiente clave:
HKey_Current_User\Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify

Borramos las claves IconsStreams y PastIconsStream y cerramos el registro.
Creamos un punto de restauración del sistema y reiniciamos el equipo.
Una vez que arranque el equipo vamos **Inicio-->Programas->Accesorios->Herramientas del sistema ->Restaurar sistema** y restauramos al punto creado anteriormente.
Por último comprueba de nuevo y verás que los iconos de elementos pasados habrán desaparecido.

Borrar mensajes pantalla de bienvenida

Borrar la lista de mensajes no leídos que queda guardada en el inicio de sesión del Messenger y mostrados también en la pantalla de bienvenida durante el inicio de sesión se puede llevar a cabo mediante la edición del registro

Para ello iniciaremos la herramienta regedit.exe desde el menú Inicio->Ejecutar->regedit
Una vez abierto navegaremos hasta la clave
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Unreadmail

En esta clave, encontraremos todas las cuentas de correo existentes.
Señalando cada una, en el arbol q se despliega en la parte de la derecha, veremos un valor DWORD MessageCount cuyo contenido tendremos que poner a 0 para que no te vuelva a indicarnos la pantalla de bienvenida el número de mensajes sin leer.

Cambiar los colores, de los elementos del simbolo del sistema

1. Abra símbolo del sistema.
2. Haga clic con el botón secundario del mouse (ratón) en la barra de título y realice una de las acciones siguientes:

Para cambiar esta configuración en todas las ventanas de símbolo del sistema, haga clic en Predeterminados.
Para cambiar únicamente esta configuración en la ventana de símbolo del sistema actual, haga clic en Propiedades.

3. En la ficha Colores, seleccione los colores del texto de pantalla, el fondo de la pantalla, el texto emergente o el fondo de las ventanas emergentes; para ello, haga clic en el elemento que desea cambiar y, a continuación, haga clic en el color que desee.

Notas

Para abrir la ventana de comandos, haga clic en Inicio, seleccione Todos los programas, Accesorios y, a continuación, haga clic en Símbolo del sistema o Inicio->Ejecutar->cmd.

- Colores de pantalla seleccionados muestra cómo aparecerán en la pantalla los colores de texto y de fondo que ha seleccionado.
- Colores seleccionados para ventanas emergentes muestra cómo aparecerán en una ventana emergente los colores de texto y de fondo que ha seleccionado.

Como averiguar cual es tu direccion IP

Si quieres saber cual es tu dirección IP, solamente tienes que pulsar el botón Inicio->Ejecutar, escribe cmd y pulsa el botón Aceptar.

Este comando abrirá una ventana en modo MS-DOS.
Ahora escribe en la línea de comandos ipconfig y te mostrara tu dirección IP y tu mascara de red.
Recuerda que si tienes una IP dinámica, esta cifra será diferente cada vez que conectes a Internet.

Como cambiar de directorio en la linea de comandos sin escribir su nombre completo

Los usuarios avanzados de Windows NT o Windows 2000 tienen que utilizar con frecuencia la línea de comandos.

Aunque la línea de comandos soporta el uso de nombres largos, a veces acceder a un directorio varias veces es algo engorroso porque su nombre es muy largo.

Existe una utilidad bastante útil y muy desconocida para acceder a estos directorios que consiste en utilizar el * como comodín para acceder a un directorio.

Por ejemplo si queremos acceder al directorio Archivos de programa, en vez de escribir cd "Archivos de programa" escribiremos cd arch*.

Como desactivar el envio de mensajes de error a Microsoft

Si estás harto de que te aparezca cuando algún programa se cierra inesperadamente el mensaje de envió de error a Microsoft, simplemente tienes que hacer esto: pulsa el botón de Inicio -> Panel de control -> Sistema -> Opciones avanzadas -> informe de errores y ahí podrás habilitar o deshabilitar ese informe que tanta lata da y a veces tan molesto.

COMO DESFRAGMENTAR LOS VOLUMENES DEL DISCO DURO

Para desfragmentar el disco en Windows XP, puede hacerse de tres maneras

Método 1:

1. Abra Mi PC.
2. Haga clic con el botón secundario en el volumen de disco que quiere desfragmentar y, después, en Propiedades.
3. En la ficha Herramientas, haga clic en Desfragmentar ahora.
4. Haga clic en Desfragmentar.

Método 2: Usar Administración de equipos de MMC

1. Inicie la herramienta Administración de equipos de MMC **(Compmgmt.msc)**. Para ello Inicio-> Ejecutar-> Compmgmt.msc
2. Haga clic en Desfragmentador de disco.
3. Haga clic en el volumen que desea desfragmentar y, a continuación, haga clic en Desfragmentar.

Método 3: Usar el Desfragmentador de disco de MMC.

1. Inicie la herramienta Desfragmentador de disco de MMC (Dfrg.msc).Para ello **Inicio-> Ejecutar-> Dfrg.msc**
2. Haga clic en el volumen que desea desfragmentar y, a continuación, haga clic en Desfragmentar.

Como establecer permisos para archivos y carpetas compartidas

Compartir archivos y carpetas se puede administrar de dos formas.

Si elige el uso compartido sencillo de archivos, podrá compartir sus carpetas con cualquier persona de su red o grupo de trabajo, o puede privatizar sus carpetas. En Windows XP Profesional, también puede establecer permisos de carpeta para usuarios o grupos específicos. Para ello, en primer lugar, debe cambiar la configuración predeterminada que es uso compartido sencillo de archivos.

Para cambiar esta configuración, siga estos pasos:

- Abra Panel de control, haga clic en Herramientas y, a continuación, haga clic en Opciones de carpeta.
- Haga clic en la ficha Vista, y desplácese hasta la parte inferior de la lista de Configuración avanzada.
- Desactive la casilla de verificación Utilizar uso compartido simple de archivos (recomendado).
- Para administrar permisos de carpeta, localice la carpeta en el Explorador de Windows, haga clic con el botón secundario del mouse (ratón) en la carpeta y, a continuación, haga clic en Propiedades.
- Haga clic en la ficha Seguridad y asigne permisos, de control total, modificación, lectura o lectura y escritura, a cada uno de los usuarios.
- Puede establecer permisos de archivos y carpetas sólo en las unidades formateadas para utilizar el sistema de archivos NTFS, y usted debe ser el administrador o tener permiso de administrador.

Como registrar una DLL

Algunos de los errores que nos da Windows se deben a que alguna Dll no está debidamente registrada.

Esto suele suceder con lo que se refiere al acceso a datos RDO350.DLL por ejemplo y con los controles ActiveX éstos no son las dll, son los ficheros con la extensión .ocx.

En este caso a veces puede funcionar registrar estos ficheros manualmente utilizando Regsvr32.

El uso es:

Regsvr32 [/u] [/s] <nombre del fichero>
Por ejemplo:
REGSVR32 c:\windows\system\Dao350.dll

Los parámetros opcionales [/u] [/s] tienen el significado siguiente:
[/u] Lo utilizaremos cuando queremos eliminar una DLL registrada o un .ocx en vez de registrarlo.
[/s] De esta manera no se despliega los mensajes durante la operación, es Modo silencioso.

Como restringir las aplicaciones que los usuarios puedan utilizar

Cuando utilizamos un ordenador compartido con otros usuarios, es posible que queramos restringir las aplicaciones que puedan usar el resto de usuarios del PC por motivos variados, la forma correcta de hacerlo es la siguiente:

Hacemos clic sobre el botón Inicio y luego en Ejecutar, a continuación tecleamos Regedit y pulsamos el botón Aceptar.

Ahora buscamos la cadena siguiente, para abrirla:
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Policies/Explorer

Ahora crearemos o modificaremos el valor DWORD RestricRun con el valor 1 para activar la restricción, y con el valor 0 para desactivarla. A continuación tendremos que definir que aplicaciones serán restringidas.

Para ello nos iremos a la clave:
HKEY_CURRENT_USER/SOFTWARE/Microsoft/Windows/CurrentVersion/Policies/Explorer/RestricRun

En este punto introduciremos valores alfanuméricos cuyo nombre serán números consecutivos y como contenido tendrán los nombres de los ejecutables de cada aplicación. Para terminar cerramos el Editor del registro y reiniciamos el ordenador.

Como se realiza un Scandisk en el XP

Para realizar un Scandisk a cualquier disco duro desde Windows, hay varias formas de hacerlo, pero una de ellas es hacer clic en el botón Inicio, luego sobre Mi PC y finalmente haces clic con el ratón derecho sobre las propiedades del disco duro al cual le quieres hacer el Scandisk.

Escoge la pestaña Herramientas y pulsa sobre el botón Comprobar ahora, en la ventana que te aparece seleccionas el tipo de reparación que deseas en caso de errores y pulsas el botón Iniciar, a partir de este momento si no hay ningún problema grave con el disco duro, realizará la comprobación.

Otra forma de hacer el Scandisk es reiniciar el ordenador con el disco de arranque y cuando se encuentre en MS-DOS tecleas SCANDISK y comenzará la comprobación del disco duro.

Comprobar y aumentar la velocidad del disco duro.

Para saber si estamos aprovechando al máximo el hardware de nuestro equipo, debemos hacerlo desde la consola de Administración siguiendo estos pasos:

Hacemos clic con el ratón derecho sobre el icono Mi PC y luego sobre Administrar.
Dentro de la rama Administrador de dispositivos buscaremos el apartado Controladores IDE/ATAPI.

Pulsando sobre cada uno de los canales IDE, y luego en la pestaña de configuración avanzada podremos comprobar y configurar el modo de transferencia de datos que se está utilizando.

Configurar dispositivos disco y lectores CD- DVD-RW

Windows XP escanea todos los canales IDE de la máquina en busca de nuevos dispositivos, por defecto cada vez que iniciamos el sistema. Este comportamiento resulta útil si acabamos de instalar un nuevo dispositivo IDE o si alteramos la conexión de los dispositivos IDE del sistema.

Como estas actividades no suelen realizarse con frecuencia, el escaneado de los canales IDE durante el inicio del sistema simplemente aumentará el tiempo que necesitará el sistema para iniciarse.

Para evitar que Windows XP y Windows 2000 escaneen todos los puertos IDE:

Dentro del Administrador de dispositivos, al que llegaremos pulsando con el ratón derecho sobre Mi PC y seleccionando Administrar encontraremos listados dentro de la rama Controladores IDE ATA/ATAPI una lista de los controladores IDE del sistema. Seleccionaremos el Canal IDE Primario haciendo doble clic sobre él y en la pestaña Configuración avanzada comprobaremos si alguno de los puertos no contiene ningún dispositivo conectado, en cuyo caso deshabilitaremos el puerto seleccionando en Tipo de dispositivo la opción ninguno. Repetiremos el mismo proceso para el Canal IDE secundario y tras reiniciar el sistema comprobaremos que éste se realiza en un tiempo sensiblemente inferior.

Nota: Deberemos tener en cuenta que si desactivamos todos los canales IDE, ninguno de nuestros dispositivos IDE funcionarán. Windows XP necesita escanear y detectar todos los dispositivos IDE disponibles en el sistema para hacer uso de ellos. Así pues, únicamente podremos deshabilitar puertos IDE que no tengan ningún dispositivo conectado.

Sin embargo, una de las mejores características de Windows XP es que podemos activar las extensiones DMA (Direct Memory Access) sin ninguno de los posibles problemas que esto conllevaba en plataformas Windows 9x. Esto es debido a que el sistema comprobará dinámicamente la compatibilidad con los dispositivos instalados en cada uno de los canales IDE si nosotros así se lo hemos especificado, en vez de forzar su utilización incluso si contamos con una unidad de disco incompatible.

Para activar DMA, iniciaremos el Administrador de dispositivos. Allí buscaremos de entre la lista de elementos de sistema nuestro controlador IDE y seleccionaremos el Canal IDE primario, en la pestaña Configuración avanzada, seleccionaremos para cada dispositivo la autodetección y su modo de transferencia a DMA si está disponible incluso si estaba seleccionada la opción Sólo PIO, este ajuste funcionará también para las unidades CD-ROM, DVD-ROM y CD-RW.

Repetiremos el proceso para el Canal IDE secundario y reiniciaremos el sistema.

El modo DMA reducirá el porcentaje de uso del procesador del 90 al 10%, y aumentará el ratio de transferencia de discos duros de 16,6 Mb hasta los 100Mb, lo que nos permitirá ejecutar los programas de forma mas rápida.

Configurar el tipo de altavoces en XP

Para personalizar el rendimiento de nuestra tarjeta de sonido.

En el Panel de control, dentro del apartado Sonidos y dispositivos de audio encontraremos en la pestaña Volumen el apartado configuración de altavoces donde pulsando sobre

Avanzada podremos especificar el tipo de altavoces que tiene nuestro sistema.

Así mismo, bajo la pestaña Rendimiento especificaremos el nivel de aceleración y ratio de conversión que utilizará el sistema.

CONFIGURAR RATON MOUSE

Ajuste su ratón para zurdos

Si usted es zurdo y le gustaría que su ratón trabajara de la manera que usted lo hace, puede cambiar la configuración para que su ratón también sea zurdo.

Para cambiar la configuración:

Haga clic en Inicio -> Panel de control -> Mouse.
Haga clic en en la pestaña Punteros del ratón.
En la pestaña Botones, abajo de Configuración de botones, seleccione Intercambiar botónes primario y secundario.
Haga clic en Aceptar.

Cambie la apariencia del puntero del ratón

Windows XP ofrece mucha flexibilidad si desea utilizar punteros del ratón diferentes a la flecha y reloj de arena. Puede cambiar todos sus punteros a la vez, o puede cambiarlos de manera individual. Para cambiar la apariencia del puntero:

Haga clic en Inicio -> Panel de control -> Mouse.
Haga clic en en la pestaña Punteros del ratón.
En la opción Punteros, haga lo siguiente:
Cambie todos sus punteros a la vez, seleccionando en la lista desplegable un Esquema.

Para cambiar punteros de manera individual, haga clic en el puntero que quiere cambiar en la lista Personalizar. Después de cada selección, haga clic en Examinar, haga clic en la imagen de puntero que quiere asignar (una vista previa de la imagen se despliega en la esquina inferior izquierda), y después haga clic en Abrir.
Haga clic en Aplicar y Aceptar para completar el procedimiento.

Para ajustar la velocidad del puntero

Con Windows XP, usted tiene control sobre su ratón.
Haga clic en Inicio -> Panel de control -> Mouse.
Haga clic en en la pestaña Punteros del ratón.
En la opción Opciones del puntero, bajo Movimiento, deslice la barra a la izquierda para hacer que el puntero se mueva más lento, o hacia la derecha para hacer que el puntero se mueva más rápido.

Si selecciona una velocidad rápida, asegúrese que se encuentre seleccionado Mejorar la precisión del puntero (esto proporciona mejor control del puntero cuando se mueve a distancias cortas), y después haga clic en Aceptar.

Configurar rendimiento en XP

A Windows XP lo podemos hacer liviano y ligero, claro esta que con ello perderá todo lo bonito y lo que lo hace agradable a la vista.

Vete a Inicio->Panel de control->Sistema->Pestaña Opciones avanzadas->Rendimiento (Botón Configuración)-> Efectos visuales: Señala Ajustar para obtener el mejor rendimiento.

Ahora nos vamos a Inicio->Panel de control->Herramientas administrativas->Servicios-> Buscamos Temas y lo deshabilitamos, doble clic, y en Tipo de inicio elegimos: Deshabilitado

Por ultimo Inicio->Ejecutar->msconfig->Pestaña Inicio y desmarcamos todos los programas que nos arrancan con el equipo y no sean imprescindibles, ya que lo único que suelen hacer es consumir recursos innecesarios.

Comprobaras q es mas feo, pero también mucho mas suelto y rápido.

Convertir ficheros FAT32 a NTFS

El sistema de archivos Fat32 que se utiliza con lasversiones de Windows 95, 98, Me, no es el más apropiado para el Windows XP, ya que limita las posibilidades de este sistema operativo. Por ello es preferible usar NTFS.

Este sistema de archivos se puede elegir en el momento de la instalación del propio Windows Xp, pero si ya lo has instalado o lo has actualizado desde Windows 98 o Me y no te has acordado de cambiar de Fat32 a NTFS ahora lo podrás hacer sin necesidad de reinstalar el sistema operativo, ya que Microsoft proporciona una utilidad pensada para realizar esta conversión. Ten en cuenta que convertir una unidad formateada en FAT32 a NTFS es un proceso irreversible. Por ello es recomendable previamente hacer una copia de seguridad de tus archivos más importantes por si la conversión no funcionase correctamente.

Cuando estés preparado debes pulsar el botón Inicio -> Ejecutar, a continuación escribes cmd y pulsas el botón Aceptar.

Entonces se abrirá una ventana MS-DOS, en la que tienes que teclear CD.. y pulsar Intro las veces que sea necesario hasta quedarte en C:\> luego escribes esto: convert c: /fs:ntfs (siendo c: la letra de la unidad que quieras convertir). Un mensaje te indicará que no puede realizar la conversión porque el disco está en uso.

Pulsa la tecla N y te preguntará si deseas que realice la conversión cuando vuelvas a iniciar el sistema. Ahora pulsa S y al reiniciar el PC la conversión del sistema de archivos se llevará a cabo.

Tienes que tener en cuenta que el pasar al NTFS tiene sus ventajas y desventajas también, como pudiera ser que tendrías varias particiones en FAT desde las cuales no veras esta en NTFS, a no ser que uses un software especial al efecto.

Crear un disco de restablecimiento de contraseñas

Si estás ejecutando Windows XP Profesional como usuario local en un entorno de grupo de trabajo, puedes crear un disco de restablecimiento de contraseñas para iniciar sesión en el equipo cuando olvides la contraseña. Para crear el disco, sigue estos pasos:

- Haz clic en Inicio, en Panel de control y, a continuación, en Cuentas de usuario.
- Haz clic en tu nombre de cuenta.
- Debajo de Tareas relacionadas, haces clic en Prevenir el olvido de contraseñas.
- Sigue las instrucciones del Asistente para contraseña olvidada con el fin de crear un disco de restablecimiento de contraseña.
- Guarda el disco en un lugar seguro, ya que cualquiera que lo utilice puede tener acceso a su cuenta de usuario local.

Cree un acceso directo a Mostrar escritorio

Si usted tiene Windows Me, 2000, 98 o 95 con la Actualización de escritorio de Internet Explorer instalada, la barra de herramientas de Quick Launch en su barra de tareas de Windows probablemente incluye un icono de Mostrar escritorio (con un pequeño secante, papel y lápiz) que cambia entre minimizar y maximizar todas las ventanas abiertas.

¿Pero qué sucede si usted o alguna aplicación borran este icono? Para restaurarlo, escoja **Inicio>Buscar->Archivos o carpetas-> escriba "Show Desktop.scf"** (incluidas las comillas).

Especifique Unidades de discos locales en el campo de Buscar en... Pulse Buscar ahora, y si tiene suerte, el utensilio de Buscar localizará una copia de este archivo. Cuando la tenga, arrastre el archivo desde la ventana de Buscar a la barra de Quick Launch para poner allí un icono de Mostrar escritorio.

Si su búsqueda no arroja resultados positivos, puede volver a crear este archivo por su cuenta. Abra el Bloc de notas. Entonces seleccione Archivo->Guardar como, y navegue a la carpeta donde están guardados los elementos de Quick Launch. Para encontrar esta carpeta, pulse el botón derecho del ratón sobre un espacio vacío de la barra de herramientas de Quick Launch (o la raya que usted arrastra para cambiar el tamaño de la barra de herramientas) y escoja Abrir. El nombre de la carpeta aparecerá en la barra de Dirección.

En la caja de Nombre de archivo escriba **"Show Desktop.scf".** No se olvide de incluir las comillas para impedir que el Bloc de notas agregue su extensión .txt predeterminada.

El atajo deberá reaparecer ahora en la barra de herramientas de Quick Launch. Si tiene dificultades para encontrar la carpeta de Quick Launch, siempre puede guardar el archivo **Show Desktop.scf** en el escritorio, y arrastrarlo luego a la barra de Quick Launch.

Desactivar los globos de notificación

A veces pueden ser molestos los globos que salen en la parte inferior de la pantalla y que informan

sobre las actualizaciones para instalar, los íconos inactivos ocultos o los programas activos. Para desactivarlos, coloque el cursor sobre el reloj de la barra de tareas y dé clic con el botón derecho.

Luego elija la opción Personalizar notificaciones.

Allí verá una ventana con la lista de programas que se inician con Windows y que activan esas notificaciones. Dé clic en el que quiera ocultar y escoja Siempre oculto.

Descargar de la memoria RAM las DLL no utilizadas

Todas las dll´s que se quedan cargadas en la memoria cuando se cierra el programa que las usaba, son dll´s que no sirven para nada, salvo para ocupar memoria inútilmente y reducir tu velocidad de trabajo, para ello lo mejor es forzar la descarga de memoria.

Con este truco vamos a conseguir que Windows las borre de la memoria automáticamente, para ello sigue estos pasos:

- Haz clic en el botón Inicio-> Ejecutar -> escribe regedit y pulsa el botón Aceptar
- Ahora en el registro de Windows debes desplazarte por las siguientes claves: **HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer**
- En el panel de la derecha, haces clic con el ratón derecho y escoges Nuevo y Valor alfanumérico.
- Le das el nombre de AlwaysUnloadDll y pulsas la tecla Intro para que se genere el nuevo nombre.
- Ahora haces doble clic sobre él valor nuevo creado y en la ventana que aparece teclea 1 y pulsas el botón Aceptar.
- Cierra todas las ventanas y reinicia el ordenador.

DESHABILITAR EL ACCESO AL REGISTRO DE WINDOWS XP

Para deshabilitar el acceso al registro de Windows: Regedit debemos seguir estos pasos:

- Localizar la siguiente clave: **HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Policies/System.**
- En la ventana de la derecha creamos un nuevo valor DWORD y le damos el nombre DisableRegistryTools.
- Hacemos doble clic sobre él y asignamos el valor 1 para deshabilitar las funciones de edición del registro.

Para habilitar el acceso al registro de Windows: Regedit debemos seguir estos pasos:

- Abrimos el bloc de notas y escribimos las siguientes líneas:
  Windows Registry Editor Version 5.00
  [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\system]
  "DisableRegistryTools"=dword:00000000
- Guardamos el bloc de Notas con el nombre unlock.reg y a partir de ahora cuando queramos habilitar el registro de Windows, después de haberlo deshabilitado solo habrá que hacer doble clic sobre el archivo que acabamos de crear unlock.reg.

Deshabilitar la restauracion del sistema en Windows XP

Cómo sucedía con Windows Millenium, en Windows XP también debemos deshabilitar la opción Restaurar Sistema o AutoRestore, para la limpieza de algunos virus. Esta característica implementada por primera vez en Windows Me y ahora también presente en Windows XP, realiza un respaldo automático de los archivos esenciales del sistema para poder restituirlos ante cualquier modificación crítica. Sin embargo, algunos virus, por copiarse en ciertas carpetas o ubicaciones especiales, también son respaldados, causando problemas a los antivirus al intentar eliminarlos.

Para deshabilitar la herramienta Restaurar sistema en Windows XP, siga estos pasos:

- Seleccione, Inicio, Mi PC
- Haga clic en Ver información del sistema
- Seleccione la etiqueta Restauración de sistema
- Marque la casilla Deshabilitar Restauración del Sistema en todos los discos y pulse en Aplicar.
- El sistema le preguntará si está seguro de querer deshabilitarlo. Confírmelo pulsando en SI.
- La opción que muestra el estado de los discos en la ventana Restauración del Sistema aparecerá deshabilitada (todo gris). Pulse en el botón Aceptar.
- Reinicie su PC, y proceda a escanearlo con uno o dos antivirus actualizados.

Para rehabilitar la opción Restauración del sistema repita todos los pasos anteriores, desmarcando en el punto 4 la casilla Deshabilitar Restauración del Sistema en todos los discos.

Donde puedo encontrar la maquina virtual de Java

La máquina virtual de Java sirve para ejecutar aplicaciones en Java (es decir, archivos con extensión *.class o *.jar) y también los applets de Java que podemos encontrarnos en algunas páginas web (normalmente, chats y utilidades similares). Debido a las "peleillas" y litigios entre Sun y Microsoft, Microsoft retiró durante una temporada la JVM de su web, aunque ya la incluye en el último Service Pack (SP1) de Windows XP por lo que, para instalarla, deberás instalar el SP1 completo. No obstante, es posible descargarla aparte (de la web de Sun).

Por lo tanto, hay dos JVMs diferentes entre las que se puede elegir:

- La de Microsoft, incluida en el Service Pack 1 (SP1), que se puede descargar de Windows Update (http://windowsupdate.microsoft.com).
- La de Sun está disponible en http://java.sun.com/getjava/download.html y ocupa unos 10 MB.

Si se instala la de Sun aparece un nuevo icono en el panel de control de Windows llamado Java Plug-in con dos opciones interesantes. En la pestaña "Básico" puedes marcar "No iniciar consola" para evitar que te aparezca un icono en la bandeja del sistema (al lado del reloj de Windows) cada vez que se ejecuta un applet. En la pestaña "Explorador" puedes indicar qué navegadores quieres que usen la JVM de Sun.

Debido a que la JVM de Microsoft no es 100% compatible con el estándar de Java (ni tampoco suele estar demasiado actualizada), es posible que te encuentres applets que no te funcionen porque estén diceñados justo para la JVM que no estés usando. Siempre puedes acudir al Panel de Control y cambiar de máquina virtual a voluntad (es necesario cerrar el navegador para hacer efectivos los cambios).

Eliminar archivos que no se dejan borrar

Alguna vez nos encontramos que al intentar borrar un archivo, XP nos contesta que no se puede eliminar porque el archivo está siendo usado por otro programa, este problema suele ocurrir cuando intentamos borrar archivos en formato .avi.

Normalmente el problema suele producirlo algún .avi está dañado y el codec correspondiente se bloquea y no lo libera.

Recuerda que .AVI no es un tipo de fichero, sino que es un contenedor de formato de video, y que en la cabecera interna, lleva realmente grabado el tipo de video que es y por tanto el sistema sabe a que codec debe llamar.

Para solucionar este problema abriremos una ventana de comandos: **Inicio -> Ejecutar-> escribimos cmd** y pulsamos el botón Aceptar.

Cerramos todos los programas que tengamos abiertos menos la pantalla de MS-DOS que acabamos de abrir.

Volvemos ha el botón: **Inicio->Ejecutar -> escribimos Taskmgr.exe** y pulsamos el botón Aceptar

Ahora cerraremos todos los programas que tengamos abiertos, finalizamos el proceso explorer.exe, y dejamos, también, el Administrador de tareas abierto.

Volvemos a la ventana de comandos e iremos a la carpeta donde tengamos el archivo que queremos eliminar y escribiremos: del (dejamos un espacio) nombre_archivo

Volvemos de nuevo al administrador de tareas, Archivo -> Nueva tarea y escribimos explorer.exe para reestablecer el escritorio.

Ya podemos cerrar el administrador de tareas y la ventana de comandos.

Eliminar el login y el password de Windows NT

Para ello iniciamos el editor del registro y buscaremos en el registro de Windows la siguiente clave:
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT_CurrentVersion\WinLogin

Ahora tendremos que crear las siguientes variables:

DefaultDomainName: Nombre de dominio por defecto.
DefaultPassword: Password por defecto.
Default UserName: Nombre de usuario login por defecto.
AutoAdminLogon: Le damos el valor 1 para que no aparezca el login/pass.

Eliminar entradas de la barra de direcciones del Navegador

Para eliminar las entradas que aparecen en la barra de direcciones sin tener que borrar el Historial, debes editar el Registro de Windows, busca esta subclave:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

En el panel derecho verás todas las URL.
Elimina las que te interesen que no aparezcan en la barra de direcciones.

Eliminar entradas de la lista Ejecutar

Si quieres borrar los elementos de la lista desplegable en la casilla de Inicio->Ejecutar debes seguir los siguientes pasos:

- Abrimos el Regedit y con el propio Inicio -> Ejecutar escribimos Regedit.exe
- Una vez ejecutado buscamos la clave:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- Haz clic en esta carpeta y ya puedes eliminar las entradas que no quieras que aparezcan. Las entradas de nuestras ejecuciones, son las que tienen el abecedario.
- No elimines los elementos restantes de la lista MRUList, Predeterminado.
- La próxima vez que abras el Windows el cambio habrá surtido efecto.

Eliminar opciones del boton derecho del raton

Cuando hacemos clic con el botón derecho en un programa, archivo o directorio aparecen una serie de opciones pero muchas veces estas opciones molestan más de lo que ayudan.

- Para eliminarlas hacemos lo siguiente:
- Iniciamos el registro de Windows: Inicio-> Ejecutar >Regedit
- En las ramas:
  HKEY_CLASSES_ROOT\Directory\shellex\ContextMenuHandlers
  HKEY_CLASSES_ROOT*\shellex\ContextMenuHandlers
- Eliminamos las entradas que no necesitemos, así no aparecerán dichas opciones al pulsar con el botón derecho.

Eliminar referencia a un programa mal desinstalado

Cuando borramos un programa sin desinstalarlo, sigue apareciendo en la lista de programas instalados en Agregar o quitar programas, a continuación te explico como eliminar estas referencias a esos programas q ya no existen en nuestro disco duro.

- Abrimos el editor de registro de Windows: Inicio -> Ejecutar -> Regedit
- Una vez dentro del editor de registro seleccionamos:
  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
- Ahora buscamos la entrada del programa que queremos eliminar, lo seleccionamos y lo eliminamos.
- Una vez hecho lo anterior reiniciamos el equipo.

Es una manera muy sencilla de limpiar aquellas referencias a programas que no se pueden desinstalar porque ya no existen.

Eliminar servicios en el registro

Para eliminar un servicio en el registro vamos a:

Inicicio ->Ejecutar-> Regedit-> Buscamos la cadena:

[HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/servicio a quitar]

Se puede quitar cualquier servicio de Windows XP.

Nota: Siempre exportar una copia de seguridad antes de borrar una clave, para poder recuperarlo después en caso de necesidad o renombrando esa clave, yo le suelo añadir una X así en cualquier momento y volviendo a editarlo lo dejo como estaba.

¿Por qué hacerlo?: en ciertos casos los servicios desactivados se reactivan al actualizar el sistema. Borrando las entradas ya no existen.Con respecto al uso de la desactivación de servicios en Windows XP ver un tutoríal sobre ellos, pero la razón evidente es la seguridad de nuestros datos, la rapidez del sistema al quitar procesos no usados y puertas abiertas para Microsoft en nuestro sistema.

Forzar a que Windows reconozca las extensiones largas

Por defecto Windows NT y Windows 2000 no reconocen el cuarto y posteriores caracteres de las extensiones de los archivos, algo que puede ser muy peligroso si se quiere borrar ciertos archivos de un directorio a la vez y además existen otros cuya extensión es más larga pero comienza por los tres caracteres de los archivos que queremos borrar.

Para solucionar esto debemos acceder al registro, luego localizaremos la clave
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem.
Una vez ahí debemos modificar el valor de Win95TruncatedExtensions poniéndolo a cero.

Guardar descargas de Windows Update

Seguramente, más de uno habréis tenido que reinstalar Windows despues de formatear, y luego claro, pasar por Windows Update y esperar en el mejor de los casos con línea ADSL casi dos horas, no digamos con módem de 56k.

Pues bien, hay una manera de conservar los archivos de Windows Update, primero, en Opciones de carpeta activamos ver carpetas ocultas y desactivamos la opción de ocultar programas del sistema operativo, luego buscamos la carpeta Wutemp si tienes más de un disco, Windows suele ponerla en el disco de mayor capacidad y donde no esté el S.O., ahora creamos otra con el nombre que queramos.

Luego empezamos a descargar las actualizaciones, aquí hay que estar atento, en el momento en que Windows te diga que está instalando las actualizaciones, deberemos copiar y pegar todas las carpetas que han sido descargadas y pegarlas en la carpeta creada a tal efecto.

De esta forma, tendremos una copia de todas las actualizaciones, para nuestro próximo formateo.

Hay unos detalles importantes a tener en cuenta, y es que algunas de las actualizaciones, como directx9, nos pedirá conectar a Internet, pero podremos descargarlas a nuestro disco también y el otro es que no hace falta que reiniciemos el sistema cada vez que instalemos una actualización, marcamos la casilla de no reiniciar ahora y seguimos instalando actualizaciones.

COMANDOS DESDE LA CONSOLA EN WINDOWS XP

Además de las numerosas opciones de configuración que incluye Windows XP en el Panel de Control, existen otras opciones adicionales que sólo son accesibles a través de ciertos comandos.

El sistema operativo Microsoft Windows XP incluye muchas funciones a las que tan sólo podemos acceder a través de la consola de comandos. A menudo estas herramientas nos pueden ayudar a mejorar el rendimiento de nuestro sistema operativo, diagnosticar y corregir problemas o simplemente obtener más información sobre la configuración de nuestro equipo.

Para acceder a la consola de comandos, tan sólo tendremos que ir al menú Inicio, seleccionar la opción ejecutar y escribir cmd.exe ó simplemente cmd. También podremos acceder a este menú mediante la combinación del teclado tecla Windows+R.

Para obtener ayuda adicional sobre un comando, las opciones que incluye y algunos ejemplos de uso, tan sólo tendremos que añadirle la opción /h ó /?.

Archivos y sistemas de ficheros

cacls: Permite modificar los permisos en ficheros y carpetas, permitiendo o prohibiendo a cada usuario leer, escribir o modificar el contenido de dichos archivos o carpetas.
chkdsk: Comprueba el estado de una partición y repara los daños en caso de que encuentre alguno. Si lo ponemos sin ningún parámetro simplemente escaneará la partición, si queremos que además corrija los errores, deberemos añadir la opción /F, es decir, chkdsk /F. cipher: Permite cifrar archivos, directorios o particiones siempre que se encuentren en el sistema de archivos NTFS.
comp: Compara archivos o carpetas y muestra las diferencias existentes entre ellos.
compact: Permite comprimir archivos o carpetas para ahorrar espacio en el disco duro. Para comprimir los archivos deberemos utilizar el modificador /c y para descomprimirlo en modificador /u. Por ejemplo, para comprimir la carpeta c:\pruebas debemos utilizar el comando compact /c c:\pruebas y para descomprimirla compact /u c:\pruebas.
convert: Convierte particiones FAT ó FAT32 a NTFS. Antes de utilizar este comando es recomendable realizar una copia de seguridad puesto que es posible que durante la conversión se pierdan datos.
defrag: Desfragmenta los archivos de una unidad, similar a la utilidad Defragmentador de discos de Windows pero en modo consola.
diskpart: Permite crear, eliminar y administrar particiones. Este programa en modo consola debemos utilizarlo con cuidado puesto que es fácil que eliminemos sin darnos cuenta todo el contenido del disco duro o de la partición activa.
find y findstr: Estos comandos buscan cadenas de textos en el interior de uno o varios archivos. Sin embargo, el comando findstr ofrece más opciones de búsqueda que el comando find.
iexpress: Este comando lanzará un asistente para crear archivos comprimidos .CAB autodescomprimibles.
openfiles: Muestra a un administrador los archivos abiertos en un sistema a un administrador y permite desconectarlos si se han abierto a través de red.

Configuración del sistema

bootcfg: Permite ver y modificar las entradas del archivo boot.ini. Estas entradas nos permiten seleccionar con que sistema operativo deseamos iniciar el equipo.
control userpasswords2: Permite modificar las claves y los permisos de los diferentes usuarios, así como requerir la pulsación de control+alt+suprimir para poder iniciar sesión, haciendo el inicio de sesión más seguro.
driverquery: Hace un listado de todos los drivers instalados en el sistema y muestra información sobre cada uno de ellos.
dxdiag: Lanza la herramienta de diagnóstico de Direct X, con la cual podremos comprobar la versión Direct X que tenemos instalada y permite comprobar mediante tests que todo lo referente a estos controladores funcione correctamente.
gpresult: Muestra información sobre las políticas de grupo aplicadas a un usuario.
gpupdate: Vuelve a aplicar las políticas de grupo.
msconfig: Desde esta aplicación en modo gráfico podremos seleccionar que programas y servicios se cargan durante el inicio de Windows así como los sistemas operativos que el usuario puede seleccionar para iniciar el ordenador.
pagefileconfig: Permite configurar el archivo de paginación de Windows.
prncnfg: Muestra información sobre las impresoras instaladas prnjobs: Muestra información sobre los trabajos de impresión en cola.
reg: Permite ver y modificar valores del registro de Windows. Las opciones posibles son:

- **reg query =>** realiza una consulta en el registro
- **reg add =>** añade una entrada al registro
- **reg delete =>** elimina una clave del registro
- **reg copy =>** copia una clave del registro a otra parte del registro o a otro equipo
- **reg save =>** guarda una parte del registro en un archivo
- **reg restore =>** restaura una parte del registro de un archivo
- **reg load =>** carga una clave o árbol al registro desde un archivo
- **reg unload =>** descarga una clave o árbol del registro
- **reg compare =>** compara varios valores del registro
- **reg export =>** exporta el registro o parte del registro a un archivo
- **reg import =>** importa el registro o parte del registro de un archivo

regedit: Editor del registro en modo gráfico.

sc: Este commando nos permite administrar los servicios, ya sea iniciar uno, detenerlo, mandarle señales, etc.
sfc: Este comando permite buscar archivos del sistema dañados y recuperarlos en caso de que estén defectuosos (es necesario el CD de instalación del sistema operativo para utilizarlo). Para realizar una comprobación inmediata, deberemos ejecutar la orden sfc /scannow.
systeminfo: Muestra información sobre nuestro equipo y nuestro sistema operativo: número de procesadores, tipo de sistema, actualizaciones instaladas, etc.
taskkill: Permite eliminar un proceso conociendo su nombre o el número del proceso (PID).
tasklist: Realiza un listado de todos los procesos que hay. Útil si deseamos eliminar un proceso y no conocemos exactamente su nombre o su PID.

Redes

arp: Muestra y permite modificar las tablas del protocolo ARP, encargado de convertir las direcciones IP de cada ordenador en direcciones MAC (dirección física única de cada tarjeta de red).

ftp: Permite conectarse a otra máquina a través del protocolo FTP para transferir archivos.
getmac: Muestra las direcciones MAC de los adaptadores de red que tengamos instalados en el sistema.
ipconfig: Muestra y permite renovar la configuración de todos los interfaces de red.
nbtstat: Muestra las estadísticas y las conexiones actuales del protocolo NetBIOS sobre TCP/IP, los recursos compartidos y los recursos que son accesibles.
net: Permite administrar usuarios, carpetas compartidas, servicios, etc. Para un listado completo de todas las opciones, escribir net sin ningún argumento. Para obtener ayuda sobre alguna opción en concreto, escribier net help opción.
netsh: Este programa en modo consola permite ver, modificar y diagnosticar la configuración de la red
netstat: Mediante este comando obtendremos un listado de todas las conexiones de red que nuestra máquina ha realizado.
nslookup: Esta aplicación se conecta a nuestros servidores DNS para resolver la IP de cualquier nombre de host. Por ejemplo, si ejecutamos nslookup y escribimos www.xdireccion.com, nos responderá con algo como:

Respuesta no autoritativa:
Nombre: www.xdireccion.com
Address: 217.76.130.250
Esto quiere decir que la dirección web www.xdireccion.com corresponde con la IP 217.76.130.250.

pathping: Muestra la ruta que sigue cada paquete para llegar a una IP determinada, el tiempo de respuesta de cada uno de los nodos por los que pasa y las estadísticas de cada uno de ellos.
ping: Poniendo detrás del comando ping el nombre o la dirección IP de la máquina, por ejemplo ping 192.168.0.1 enviaremos un paquete a la dirección que pongamos para comprobar que está encendida y en red. Además, informa del tiempo que tarda en contestar la máquina destino, lo que nos puede dar una idea de lo congestionada que esté la red.
rasdial: Permite establecer o finalizar una conexión telefónica.
route: Permite ver o modificar las tablas de enrutamiento de red.
tracert: Muestra el camino seguido para llegar a una IP y el tiempo de respuesta de cada nodo.

Varios

at: Permite programar tareas para que nuestro ordenador las ejecute en una fecha o en un momento determinado.

logoff:: Este comando nos permite cerrar una sesión iniciada, ya sea en nuestro ordenador o en otro ordenador remoto.

msg:: Envía un mensaje a unos o varios usuarios determinados mediante su nombre de inicio de sesión o el identificador de su sesión

msiexec:: Permite instalar, desinstalar o reparar un programa instalado mediante un paquete MSI (archivos con extensión .msi).

runas: Permite ejecutar un programa con privilegios de otra cuenta. Útil por ejemplo si estamos como usuario limitado y queremos hacer algo que necesite privilegios de administrador.

shctasks: Permite administrar las tareas programadas.

shutdown: Permite apagar, reiniciar un ordenador o cancelar un apagado. Es especialmente útil si hemos sido infectado con el virus Blaster o una de sus variantes para cancelar la cuenta atrás. Para ello, tan sólo tendremos que utilizar la sintaxis shutdown -a.

Microsoft Management Console (MMC)

Estos comandos nos darán acceso a distintas partes de la Microsoft Management Console, un conjunto de pequeñas aplicaciones que nos permitirán controlar varios apartados de la configuración de nuestro sistema operativo.

Para acceder a estas opciones, no es necesario entrar en la consola del sistema (cmd.exe), sino que basta con introducirlos directamente desde inicio - ejecutar.

ciadv.msc: Permite configurar el servicio de indexado, que acelera las búsquedas en el disco duro.
compmgmt.msc: Da acceso a la Administración de equipos, desde donde podemos configurar nuestro ordenador y acceder a otras partes de la MMC.
devmgmt.msc:: Accede al Administrador de dispositivos.
dfrg.msc: Desfragmentador del disco duro.
diskmgmt.msc: Administrador de discos duros.
fsmgmt.msc: Permite administrar y monitorizar los recursos compartidos.
gpedit.msc: Permite modificar las políticas de grupo.
lusrmgr.msc: Permite ver y modificar los usuarios y grupos locales.
ntmsmgr.msc: Administra y monitoriza los dispositivos de almacenamientos extraíbles.
ntmsoprq.msc: Monitoriza las solicitudes del operador de medios extraíbles.
perfmon.msc: Monitor de rendimiento del sistema.
secpol.msc: Configuración de la política de seguridad local.
services.msc: Administrador de servicios locales.
wmimgmt.msc: Configura y controla el servicio Instrumental de administración (WMI) de Windows.

Como podemos comprobar, muchas de las opciones aquí listadas sólo son accesibles a través de esta consola, por lo que tareas como personalizar nuestro sistema de acuerdo a nuestros gustos, adaptarlo a nuestras necesidades con una mayor precisión o simplemente por conocer cómo funciona nuestro sistema operativo o cómo está configurado podemos realizarlas con ayuda de estos menús ocultos

---

Hacer que el modem marque más rapido

Para hacer esto, abre al Panel de control de Windows XP, clica el icono de **Modems -> Propiedades -> Conexión -> Avanzadas -> Configuraciones Adicionales.**

En este campo deberás escribir el siguiente comando S11=50.

Imprimir una parte de una pagina web

Mientras se navega por Internet es posible encontrar alguna cosa interesante que queramos imprimir. ¿Pero que ocurre si la página es larga y no queremos imprimirla entera?

- Seleccionar con el ratón la parte de la página que se desea imprimir.
- A continuación, se selecciona Menu->Archivo ->Imprimir.
- Se abrirá la ventana de imprimir.
- En ella hay que activar la casilla Selección que aparece dentro del apartado Intervalo de Impresión.

- Pulsaremos, entonces, Aceptar y de esta forma se consigue impresa en papel la parte seleccionada en el punto anterior.

Login tradicional en Windows XP

Un truco para Windows XP que apreciarán principalmente los que se consideren usuarios avanzados de este sistema operativo, relativo a la seguridad, es especialmente recomendable.

Al instalar Windows XP Home o Professional si no forma parte de un dominio, disfrutamos de la posibilidad de efectuar cambios rápidos de usuario y otras características que hacen más fácil el uso simultáneo de nuestro ordenador por parte de varias personas.

La pantalla de bienvenida de Windows XP nos muestra una lista con los usuarios disponibles en el sistema de forma que, pulsando sobre uno cualquiera de ellos, podemos entrar con su cuenta. A estos usuarios se les puede asignar una contraseña, con lo que la seguridad de acceso queda controlada.

Por defecto, en esta pantalla sólo se muestran ciertos usuarios que habremos creado desde la utilidad Cuentas de usuario del Panel de control o que se definieron durante la instalación del sistema. Sin embargo, los usuarios avanzados del sistema, y sobre todo los que hayan migrado a Windows XP desde Windows 2000 Professional, se encontrarán con que no pueden acceder con otras cuentas de usuario, principalmente con la cuenta Administrador, ya que no está disponible en la pantalla de bienvenida.

Existe un truco muy sencillo y directo para conseguir un cuadro de autenticación idéntico al de Windows 2000 Pro para los usuarios avanzados: desde la pantalla de bienvenida, con todas las sesiones de usuario cerradas esto es importante basta con pulsar al mismo tiempo la combinación de teclas **CTRL+ALT+SUPR** dos veces seguidas para que podamos introducir manualmente el nombre de cualquier usuario y su contraseña, a través de un diálogo como el de la figura, que parece.

Más informacion sobre el procesador

Al hacer clic con el botón derecho del ratón sobre el icono Mi PC y seleccionar Propiedades, Windows muestra una ventana Propiedades de Sistema en la que, entre otras cosas, aparece una escueta reseña sobre el procesador instalado en el equipo.

Si desea obtener una información más detallada al respecto, no hay más que ejecutar el Editor del Registro y buscar esta clave:
HKEY_LOCAL_MACHINE\Hardware\Description\System\CentralProcessor\0
Edite el valor VendorIdentifier, que debe contener la cadena GenuineIntel (si se trata de un procesador Intel). Lo que hay que hacer es introducir un espacio entre las palabras Genuine e Intel, cerrar el registro, acceder a las propiedades de Mi PC y comprobar como la descripción que se obtiene ahora es algo más detallada.

Modificaciones en el Boot.ini

Existen una serie de parámetros que podemos introducir en el archivo de configuración del inicio de sistema boot.ini que pueden ayudarnos a obtener el máximo rendimiento del mismo o a diagnosticar posibles problemas en la máquina.

Entre los más importantes destacan:

/FASTDETECT Con este parámetro, durante el proceso de arranque la detección de los dispositivos instalados en los puertos paralelo y serie se realizará haciendo uso de los mecanismos plug&play, y no a través del archivo ntdetect.com como se realizaba en anteriores versiones, traduciéndose en un tiempo de arranque del sistema menor.

/BOOTLOG Con este parámetro, Windows XP creará un archivo de registro %SystemRoot%NTBTLOG.TXT que incluirá entradas detallando los controladores han sido cargados con éxito y de forma fallida durante el proceso de inicio del sistema.

/MAXMEM=x Limitará el uso de memoria a Windows XP únicamente a la cantidad especificada, interpretada en Mbytes.

/ONECPU Limitará el uso de más de una CPU en sistemas multiprocesador.

/NUMPROC= Únicamente serán utilizados por el sistema el número de procesadores especificado.

/SOS Obligará a Windows XP a mostrar en pantalla información referente a los controlados a medida que son cargados en memoria y el sistema iniciado.

/WIN95 Este parámetro resulta pertinente únicamente en sistemas con arranque triple entre Windows XP, Windows 9x y DOS. Con ello obligamos a ntldr a iniciar el sector de arranque de Windows 9x que se encontrará en el archivo bootsect.w40.

/WIN95DOS Resulta pertinente únicamente en sistemas con arranque triple entre Windows XP, Windows 9x y DOS. Con él se obliga a ntldr a iniciar el sector de arranque de DOS, que se encontrará en el archivo bootsect.dos.

Navegar más rapido en Internet

Para aumentar la velocidad de acceso a servidores HTTP, y visualizar las páginas Webs más rápido, sigue estos pasos:

- Haz clic en el botón Inicio y luego sobre Ejecutar, escribe Regedit y pulsa el botón Aceptar.
- Una vez estás en el editor del registro busca la siguiente cadena:
  HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- En la ventana de la derecha, crear o modificar los valores DWORD siguientes:
  MaxConnectionsPerServer: doble clic sobre ese valor y escribir 4 en decimal,para ADSL escribir 20.
  MaxConnectionsPer1_0Server: doble clic sobre ese valor y escribir 8 en decimal, para ADSL escribir 20.
- Esos valores corresponden al número de demandas simultáneas de acceso a un servidor de tipo 1 o 1.1.
- Cerrar Regedit y reiniciar Windows.
- /NOSERIALMICE=[COMx | COMx,y,z...] Deshabilita la detección de ratones en los puertos serie especificados. Únicamente utilizaremos este parámetro si tenemos cualquier otro

dispositivo que no sea un ratón en el puerto serie durante la secuencia de arranque. Si utilizamos el parámetro sin especificar un puerto COM, la detección de ratones serie se deshabilitará para todos los puertos COM.

Nuestros programas favoritos en menu Inicio y mostrar la barra de herramientas de Inicio rapido

Siempre se tiene algún programa favorito que se utiliza frecuentemente

Aumente su prioridad en el menú Inicio colocándolo al principio de la lista. Esto garantiza que el programa permanecerá en el menú Inicio y que no podrá ser desplazado por otros programas, incluso si los utiliza de manera más frecuente.

Haga clic con el botón secundario del ratón en su programa favorito en el menú Inicio y seleccione Agregar al menú Inicio.

El programa se quedará permanentemente en la parte superior de la lista, justo debajo del explorador y de los programas de correo electrónico.

Para mostrar la barra de herramientas de Inicio rápido con la que se está familiarizado:

Haga clic con el botón secundario del ratón, en la barra de tareas, haga clic en Barras de herramientas y, a continuación, haga clic en Inicio rápido.

Así aparece la barra de Inicio rápido. Para agregar elementos a la barra de herramientas de Inicio rápido, haga clic en el icono del programa que quiere agregar y arrástrelo hasta la zona de Inicio rápido de la barra de tareas.

Pasos previos para actualizacion o restauracion del sistema

Es conveniente antes de restaurar o actualizar el sistema operativo, eliminar todos los ficheros y programas que no necesitemos y toda la basura que el sistema anterior, los juegos y programas generaran durante toda su vida.

- Primero borraremos los ficheros basura que ocupan espacio en disco y no los necesitamos. La mayoría están en el directorio Temp. Y tienen extensión .bak .tmp .$$$ .old, etc.
- Lo segundo que haremos será desinstalar,si es posible las aplicaciones y borrar los ficheros que creamos que ya no vamos a utilizar.
- Tercero ejecutar ScanDisk y Desfragmentador de disco para preparar el disco duro, estos programas los encontraremos en Inicio->Programas->Accesorios->Herramientas de Sistema.

Registro de Windows XP

Windows consulta continuamente su información durante su funcionamiento, por lo que un registro

mal configurado nos reportará errores y fallos inesperados. Este registro sustituye a la mayoría de los archivos .ini (pero no a todos) que se usaban en Windows 3.x y MS-DOS, así como a AUTOEXEC.BAT y CONFIG.SYS.

En el registro, los datos se organizan en una base de datos jerárquica, donde se ramifican en forma arbórea, de modo que cada una de las ramas recoge claves de la configuración. Para tener acceso al editor de registro deberás seleccionar Inicio y luego Ejecutar, sobre la línea de ejecución, escribe regedit, y luego pulsa sobre Aceptar.

Con esto accederás a la ventana del Regedit, si te desplazas por las claves:
HKEY_CURRENT_CONFIG/Display/Settings/Resolution,
Aquí encontrarás la resolución de tu monitor, como por ejemplo 800 x 600). Algunas de estas claves son:

HKEY_USERS: recoge la información de todos los usuarios que usan la máquina. Aquí se encuentra información acerca de las aplicaciones instaladas, conexiones de red, etc. de cada usuario.

HKEY_LOCAL_MACHINE:identifica la información del estado físico del hardware de nuestro ordenador, como el tipo de memoria usada, bus del sistema, tarjetas instaladas, etc.

HKEY_CLASSES_ROOT: es una subclave de **HKEY_LOCAL_MACHINE/Software** y contiene las claves que aseguran que los archivos serán abiertos de manera efectiva por sus respectivos programas.

HKEY_CURRENT_CONFIG: engloba la información acerca de los perfiles del hardware de nuestro sistema y acerca del arranque del mismo, y está vinculada a **HKEY_LOCAL_MACHINE**.

Backup del Registro de Windows

En ocasiones, después de modificar el registro, nuestro sistema empieza a comportarse de un modo extraño y queremos volver a la situación anterior. Para ello es recomendable hacer un backup antes de realizar cualquier cambio en el registro y tenemos varias opciones, una de ellas es pinchando en el botón de inicio, haremos clic en ejecutar, escribimos regedit.exe y daremos a aceptar. Una vez abierto el programa, pincharemos en el menú Registro y le daremos a exportar archivo del registro dándole un nombre de archivo.

Para restaurarlo bastara con hacer doble clic sobre este archivo que hemos exportado, o con importarlo desde el regedit. Otra opción es pinchando en el botón de inicio y dándole a la opción de ejecutar, y escribir scanregw.exe, programa que nos hará una comprobación del registro y posteriormente nos dará la opción de realizar una copia de seguridad la cual podremos restaurar desde el símbolo del sistema fuera de Windows escribiendo scanreg.exe /restore.

Robo y crackeo de los hashes de password de los usuarios

Herramientas necesarias:
a. pwdump2

b. Cain & Abel

Requerimientos:

Entrar desde una cuenta de administrador (si no somos administradores ver tutorial del Cia Commander para aprender como cambiar momentáneamente el pass de un administrador y restaurarlo después, obviamente si cambiamos el password de alguien ese password no lo podremos crackear pero como existe un administrador por defecto creado durante la instalación siempre podremos cambiar ese para entrar y hacernos con los demás)

Bajar pwdump2 en una carpeta cualquiera: ej C:\pwdump2

Abrir el símbolo del sistema y cambiar al directorio del pwdump2 ej: Incio->Ejecutar->escribir cmd y Aceptar, después para cambiar de directorio escribir cd C:\pwdump2 y Aceptar.

Robarse lo hashes de las contraseña desde el registro y volcarlos a un archivo hashes.txt con el comando: pwdump2 P.I.D > hashes.txt donde hay que sustituir P.I.D por el P.I.D del proceso lsass.exe que podemos ver en el administrador de tareas (si no es visible darle al menu ver ->seleccionar columnas y marcarlo) suponiendo que el P.I.D. sea 600 quedaría así:
pwdump2 600 > hashes.txt

Salvar el hashes.txt a un floppy y después cómodamente en nuestra computadora personal importamos los hashes con el Cain & Abel dándole a la pestaña crack->LM & NTLM Hashes ->clic derecho en el área util->add to list->seleccionar nuestro archivo hashes.txt (el Cain se puede descargar freeware desde http://www.oxid.it) armarse de paciencia y crackearlos.

Saber que codec tenemos instalados en nuestro sistema

Para saber que codec tenemos instalados en nuestro sistema, procederemos así:

Abrimos el interprete de comandos, Inicio -> Ejecutar -> cmd, tecleamos dvdupgrd /detect y pulsamos Enter. En el caso de que no aparezca ningún tipo de información significaría que no tenemos ninguno instalado.

Sincronizar el reloj con el horario de Internet

Está tu equipo en hora. Si tu equipo no forma parte de un dominio, puede sincronizar el reloj del equipo con un servidor horario de Internet.

Para ello:

- Haz doble clic en la hora de la barra de tareas.
- Haz clic en la ficha Hora de Internet.
- Selecciona el servidor horario que deseas utilizar y asegúrate de activar la casilla de verificación.
- Sincronizar automáticamente con un servidor horario de Internet.
- Asegúrate de que has configurado la fecha correcta antes de intentar sincronizar el reloj ya que el servidor horario de Internet no actualizará la hora si la fecha no es correcta.

- Si tienes un servidor de seguridad personal o de red, puede que tengas que realizar algún cambio en la configuración para desbloquear la sincronización.

Usar el FTP integrado que trae el Windows XP

¿A que no sabías que el Windows XP trae un FTP incorporado?

Como no viene habilitado por defecto vamos a tener que instalarlo desde el CD Instalación. Para ello seguiremos los siguientes pasos: Inicio -> Panel de control y ahí elegiremos Agregar/Quitar programas, ahora señalareremos donde pone Agregar o quitar componentes de Windows. En la nueva ventana emergente elegiremos donde pone... Servicios de Internet Information server IIS y haremos doble clic sobre el y seleccionaremos 3 cosas: Archivos comunes, Complemento de servicios y Servicio de protocolo (ftp).

Luego aceptaremos e instalaremos esos servicios para lo cual nos pedirá que ingresemos el CD de instalación.

Luego iremos a Inicio -> Panel de control -> Rendimiento y mantenimiento y elige Herramientas administrativas. En esa carpeta te saldrá el acceso directo al programa que buscamos, el Servicios de Internet Information Server (FTP).

Lo configuraremos así:

Donde pone sitio ftp predeterminado dale a botón derecho -> propiedades e ingresamos nuestra IP, aceptamos.

Donde señala sitio ftp predeterminado pulsas con el botón derecho y eliges todas las tareas-> asistentes para permisos, y eliges esto:

- 2º opcion->siguiente->ftp public->siguiente->
- 3º opcion->siguiente->siguiente->fin

Utilizar el NetMeeting en Windows XP

El programa se haya en C:\Archivos de programa\NetMeeting\conf.exe.

- Para instalar NetMeeting, proceda como sigue:
- Abra la carpeta C:\Archivos de programa\NetMeeting
- Haga un doble click del botón izquierdo en el archivo conf.exe (puede ser visible sólo como conf según su configuración).
- Durante el proceso de instalación, deje seleccionadas una o ambas de las casillas:
- Crear un acceso directo a NetMeeting en mi Escritorio
- Crear un acceso directo a NetMeeting en mi barra de Inicio rápido
- Ya tiene disponible NetMeeting en su equipo.

Ver conexiones de red

Tanto Windows como Linux nos ofrece una herramienta que nos va a mostrar que conexiones de red tenemos en cada momento.

Esa herramienta es el programa netstat, y para ejecutarla, en ambos casos, necesitamos abrir una Consola.

En Windows abrimos Símbolo del sistema y escribimos: netstat –an

Para entender mejor que conexiones tenemos abiertas, lo mejor es que antes de ejecutar esta orden cerremos TODOS los programas a excepción de Símbolo del sistema e ir desde el principio comprobando que conexiones tenemos y cuales se van abriendo.

Una vez ejecutada la orden, nos aparecerá una pantalla de tipo en MSDOS. Si queremos que se actualice automáticamente la información, podemos escribir netstat -an 5 (poner el número en segundos del intervalo que queramos que actualice la información)

La información que nos muestra esta pantalla básicamente es una tabla con 4 Columnas para MSDOS o 6 Columnas para Linux y diversas filas que contienen la información:

Proto: Nos indica el protocolo utilizado para la comunicación por cada una de las conexiones activas (TCP/UDP)

Dirección Local (Local Address): Nos indica la dirección origen de la conexión y el puerto.

Dirección Remota: (Foreign Address): Nos indica la dirección de destino y el puerto.

Estado (State): Nos indica el estado de dicha conexión en cada momento. Los principales estados son:

Listening (Listen): El puerto está escuchando en espera de una conexión

Established: La conexión ha sido establecida

Close_Wait: La conexión sigue abierta, pero el otro extremo nos comunica que no va a enviar nada más.

Time_Wait: La conexión ha sido cerrada, pero no se elimina de la tabla de conexión por si hay algo pendiente de recibir.

Last_ACK: La conexión se está cerrando.

Closed: La conexión ha sido cerrada definitivamente.

La columna de Dirección Local nos muestra la IP de la conexión de nuestro ordenador:

Además de la IP asociada a nuestra conexión a Internet, los ordenadores utilizan una dirección IP interna, denominada loopback, que es utilizada para pruebas y para la comunicación entre diversos procesos en la misma máquina. Usualmente tiene la dirección IP 127.0.0.1 y que también se le suele asignar el nombre localhost.

Ahora solo nos queda ir comprobando todas las conexiones que tenemos, que están haciendo y por supuesto el ¿porque?.

Para ello podemos servirnos de los listados de puertos.

Esto es muy útil para detectar la actividad de troyanos en nuestro ordenador.

VER LA CUENTA DE ADMINISTRADOR Y ESCONDER CUENTAS DE USUARIOS

Ver la cuenta de Administrador

Primero navegaremos hasta:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList

Si no existe crearemos un nuevo valor: Segundo botón del ratón -> nuevo valor, que sea DWORD, le damos nombre -> Administrador -> OK. Hacemos doble click en el y le damos el valor DECIMAL-> 1.

Si existe, sólo tendremos que modificar el valor por un 1.

Esconder cuentas de usuario de la pantalla de bienvenida

Cuando añadimos una cuenta para ciertos usuarios en Windows XP, sus nombres aparecerán en la pantalla de bienvenida.

En ocasiones un usuario necesita ser añadido a una máquina Windows XP porque necesita acceso vía red, a los recursos de esa máquina, pero jamás iniciará sesión físicamente en el ordenador.

Para eliminar completamente la cuenta de acceso de la pantalla de bienvenida, iniciaremos la herramienta de edición del registro del sistema con el comandoregedit.exe desde el menú Inicio->Ejecutar y localizaremos la clave:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\SpecialAccounts\UserList

Para cada usuario cuya cuenta queramos ocultar, crearemos un nuevo valor de tipo DWORD cuyo nombre será el nombre de usuario y su contenido 0 para ocultarlo.

Será necesario reiniciar Windows para que los cambios surtan efecto.

CENTRO DE SEGURIDAD CON EL SP2

Administrar la configuración de seguridad

Service Pack 2 (SP2) de Windows XP contiene tecnología diseñada a contribuir a la seguridad de la información personal y del equipo. Además, con SP2 es más fácil supervisar la configuración con el nuevo Centro de seguridad de Windows, al que se puede tener acceso desde el Panel de control.

El Centro de seguridad le permite comprobar el estado de las opciones de seguridad esenciales. También puede utilizarlo para buscar información sobre los virus o amenazas de seguridad más recientes u obtener servicios de atención al cliente de Microsoft en relación con un problema de seguridad.

Para abrir el Centro de seguridad

Haga clic en Inicio y, a continuación, en Panel de control.

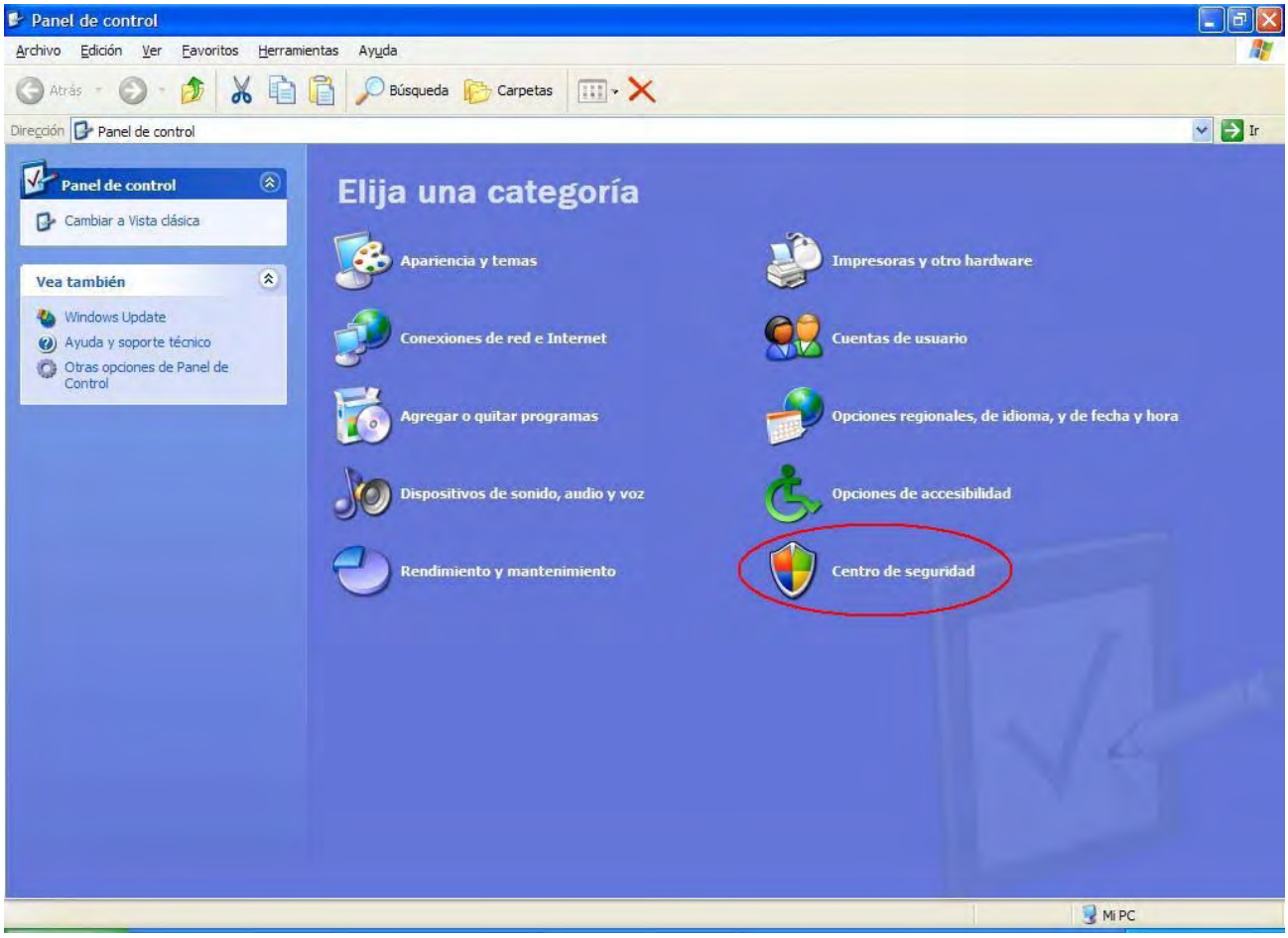


Fig 1 Panel de control con el nuevo icono del Centro de seguridad

Haga doble clic en Centro de seguridad. Verá una ventana como la que se muestra a continuación:

Fig 2 Centro de seguridad

El Centro de seguridad también comprueba que se dispone de:

- Un servidor de seguridad.
- Un programa antivirus actualizado
- La configuración correcta de Actualizaciones automáticas para descargar e instalar actualizaciones de forma automática.

Si el Centro de seguridad detecta que el equipo podría beneficiarse de una mayor seguridad en alguna de las tres áreas mencionadas, muestra una alerta en el área de notificación (a la derecha de la barra de tareas, encima del reloj). Verá una alerta como la que se muestra debajo cada vez que inicie sesión, hasta que el problema se corrija.

Sugerencia Para averiguar cómo hacer frente a un problema, haga clic en una alerta y se abrirá el Centro de seguridad.

En el Centro de seguridad, haga clic en Recomendaciones.

Nota: Si el equipo forma parte de un dominio (un grupo de equipos en una red), la configuración de seguridad suele administrarla un administrador de red. En este caso, el Centro de seguridad no muestra el estado de seguridad ni envía alertas.

El Centro de seguridad de Windows comprueba la presencia de numerosos programas antivirus y de servidor de seguridad conocidos, pero es posible que esté usando un programa que Windows no encuentra.

Deshabilitar la descarga de virus troyanos y dialers en IE

Este truco es muy recomendable para filtrar y limitar la descarga de los usuarios para prevenir la aparición de virus, troyanos y dialers en el sistema.

Para realizar este truco debe seguir los siguientes pasos:

- Hacemos clic en el botón **Inicio->Configuración y finalmente Panel de control**, doble clic en **Opciones de carpetas o Herramientas-> Opciones de carpetas** ahora seleccionamos la pestaña **Tipos de archivos.**
- Buscamos la extensión del tipo de archivo que deseamos recibir sin que sea bloqueada por el programa y la señalamos si la extensión no está en la lista, tendremos que deshabilitar toda la protección contra adjuntos peligrosos.
- Hacemos clic en Opciones avanzadas.
- Desmarcamos la opción Confirmar apertura después de la descarga.
- Finalmente hacemos clic en el botón Aceptar para confirmar los cambios.

Eliminar mensajes no deseados

Más de una vez nos habrán enviado a nuestra cuenta de correo electrónico mensajes que no hemos solicitado, en ocasiones de gran tamaño. Podemos eliminar estos mensajes a través de nuestro programa de correo pero así tendríamos que descargarlos en nuestro ordenador en cualquier caso. Sin embargo, también podremos acceder al servidor de correo de otra forma y borrar los mensajes que no queramos.

Primero, abre una sesión de telnet.exe a través de Inicio->ejecutar. Haz clic en Conectar->Sistema remoto... introduce el nombre de tu correo entrante (POP) bajo el apartado Nombre de Host.

Escribe 110 en el campo puerto y haz clic en el botón conectar.

Una vez iniciada la sesión escribe user **NOMBRE_DE_USUARIO** y cuando lo acepte, pass **CONTRASEÑA** con tu nombre de usuario y clave.

A continuación, verás los mensajes.

A partir de aquí puedes usar los siguientes comandos:

- **List** para listar los mensajes.
- **DELE n** donde **n** es el número de mensaje a borrar.
- **LOOP n m,** donde **n** es el número de mensaje y **m** el número de líneas del cuerpo del mensaje que se visualizarán en cada mensaje.
- **QUIT** para salir.

Enviar un correo electronico anónimamente

Si tienes algo muy importante que mandar por correo electrónico, por ejemplo, el número de tu tarjeta de crédito, y quieres mandarlo con especiales medidas de seguridad, necesitas un servicio de mensajes seguros.

Desde que el mensaje de correo electrónico sale hasta que llega a su destino, todos los trazos son encriptados, convirtiendo tu mensaje en una compleja fórmula matemática imposible de descifrar.

Funciona como una cuenta de correo normal: simplemente abres una cuenta y te comprometes a no hacer nada ilegal con ella. Hushmail, por ejemplo, ofrece un servicio gratuito de mensajes seguros.

Si quieres asegurarte que el correo electrónico que has enviado ha sido borrado, Disappearinginc, tiene una sencilla aplicación que funciona con el programa de correo electrónico Outlook Express.

Una vez instalada, al redactar un mensaje aparece en pantalla una caja de texto en la que debes especificar la fecha en que quieres que el mensaje desaparezca. Una vez destruido, nadie podrá recuperarlo, y esto incluye a quien lo escribió.

Escribir un mensaje de correo mediante un acceso directo

Si tienes el programa de correo Outlook puedes crear un mensaje nuevo desde un acceso directo, para ello haz clic con el botón derecho del ratón en una zona libre del Escritorio. En el menú que se despliega selecciona la entrada Nuevo y luego Acceso directo. Verás la pantalla del asistente para Crear acceso directo.

Escribe en la Línea de comandos la siguiente línea: mailto: pulsa siguiente escribe el nombre con el que quieras que aparezca en el escritorio y pulsa finalizar.

Cuando pulses sobre el icono aparecerá directamente la ventana del mensaje nuevo, sin necesidad de tener que abrir Outlook.

Evitar la desconexion del MODEM

Si tu moden se te suele desconectar, con demasiada facilidad suele ser debido al ruido de la línea, para evitarlo tienes que hacer lo siguiente.

Pulsa Inicio-> Panel de control->doble clic en modem.
Seleccionamos el moden y pulsamos en Propiedades pulsamos la pestaña Conexión pulsa la opción Avanzada en el campo Configuración extra introduce: S10=50

Ya esta listo no hace falta reiniciar el equipo.

Evitar mandar un virus a nuestros contactos

Si tienes la mala fortuna de que un virus te entre, puedes evitar diseminar el virus.

En Outlook o Outlook Express, ponemos en la Libreta de direcciones o en la carpeta Contactos un contacto con nombre y dirección !0000@0000.00 aaaa@aaaaa.aa.

Este contacto va a aparecer como primero en la lista de direcciones.

Si un virus quiere autoenviarse para todas las direcciones de la libreta, va a aparecer un mensaje de error que dice: Uno o más destinatarios no tienen dirección de correo electrónico; y se bloqueará todo.

Extraer sonidos de un correo

Todos los que disponemos de correo electrónico hemos recibido más de una vez algún correo con llamativos fondos y música.

Nos referimos a datos insertados en el mensaje, no que aparezcan como fichero adjunto. De esta manera si algún si algún fondo o imagen nos interesa podemos guardarla usando el botón derecho del ratón y usando la opción Guardar imagen como.

Pero si quieres guardar ese archivo sonoro o similar y hacerlo independientemente del mensaje, solo necesitarás los programas Winzip 8.0 y Outlook.

Al enviar un correo en formato HTML los gestores de correo como Outlook Express utilizan la codificación MIME.

Para empezar guarda el correo como un archivo en formato .eml -correo.eml-, luego renómbralo Rename- cambiando la extensión .eml por .mim el sistema lo reconocerá como un archivo de tipo Winzip.

Haz doble clic sobre el archivo y aparecerá todo el correo desglosado en archivos.

Ahora puedes abrir y descomprimir cualquiera de ellos y guardarlo.

Es muy probable que este truco funcione con otros programas de correo y tal vez con otros descompresores. Igual de válido resultará renombrar el archivo con las extensiones .b64, .bhx, .hqx, .uue, .xxe.

Personalizacion del Internet Explorer

Podemos darle unos pequeños toques personales al Internet Explorer mediante la modificación de las claves correspondiente en el registro de Windows. Antes de modificar cualquier parte del registro de Windows, se aconseja hacer una copia de seguridad del mismo o, al menos, de la rama que vamos a modificar.

Para abrir el editor del registro, pulsar en Inicio -> Ejecutar, escribimos regedit y pulsamos Enter.

En este caso las opciones hay que buscarlas a partir de la clave
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer

Las opciones configurables son varias y vamos a describir una a una.

1º El titulo del documento de Internet Explorer reside en la clave
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title

El texto que escribamos en este valor aparecerá como titulo de Internet Explorer en todas las ventanas abiertas.

2º Se puede cambiar la animación de Windows volando típica de la barra del menú del Explorer por cualquier animación que se quiera.

La condición es que tenga un formato específico:

- Tiene que ser una imagen de 22x682 pixels en formato .bmp.
- La imagen tiene que estar compuesta por 31 fotogramas de 22x22 pixels, enlazadas una debajo de otra hasta formas la imagen total de 22x682 pixels.
- Una vez creada la imagen ejecuta Inicio -> Ejecutar, escribimos regedit y pulsamos Enter.
- Abrir la clave:
  HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Toolbar\SmBrandBitmap.
- Por defecto esta clave no aparece, con lo que habrá que crearla pulsando con el botón derecho sobre la pantalla derecha -> Nuevo -> Valor alfanumérico, poner como nombre **SmBrandBitmap** y en valor la ruta del archivo de imagen.
- En esta clave debe indicarse como valor la ruta del archivo .bmp que se haya creado.

3º Se puede cambiar la animación de imagen de fondo del menú del Explorer por cualquier imagen siempre que sea .bmp.

La condición es que tenga un formato específico:

- Tiene que ser una imagen en formato .bmp.
- Preferentemente en 256 colores aunque se ha probado con otra imagen de mas colores y funciona.
- Una vez creada la imagen ejecuta Inicio -> Ejecutar, escribimos regedit y pulsamos Enter.
- Abrir la clave:
  HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Toolbar\BackBitmapIE5.
- Por defecto esta clave no aparece, con lo que habrá que crearla pulsando con el botón derecho sobre la pantalla derecha -> Nuevo -> Valor alfanumérico, poner como nombre **BackBitmapIE5** y en valor la ruta del archivo de imagen.
- En esta clave debe indicarse como valor la ruta del archivo .bmp que se haya creado.

Personalizar barra de herramientas de I. Explorer 6

Escoja las características que desea tener en la barra de herramientas de Internet Explorer 6. Si desea simplificar la barra de herramientas, podrá eliminar iconos, cambiarlos a iconos pequeños, o eliminar las etiquetas de texto que se muestran junto a los iconos.

Para personalizar la barra de herramientas: Haga clic con el botón derecho en la barra de herramientas Estándar, y pulse Personalizar.

En la lista de Opciones de texto, haga clic en Sin etiquetas de texto para eliminarlas.

En la lista de Opciones de icono, haga clic en Iconos pequeños para cambiar la configuración por defecto.

En la lista de Botones de la barra de herramientas, haga clic en el icono que quiera eliminar y pulse Quitar.

Para guardar los cambios, haga clic con el botón derecho de nuevo en la barra de herramientas y asegúrese de seleccionar Bloquear las barras de herramientas.

Ver codigo fuente de una web

En algunos casos nos gustaría poder visualizar el código fuente de una pagina Web para poderla estudiar y aprender nuevas formas de adornas nuestras propias webs.

Sin embargo, algunos programadores protegen mediante código, el botón derecho del ratón que es la forma más rápida de conseguir dicho código. En estos casos, poder conseguir dicho código de la siguiente forma:

En la barra de dirección del navegador escribiremos, delante de la dirección Web las palabras view-source:

Se abrirá una ventana del bloc de notas donde aparecerá el código HTML de la Web aunque este protegido.

CONFIGURACION DE WINDOWS XP PROFESSIONAL

Verificar que todas las particiones de disco están formateadas con NTFS.

Las particiones NTFS ofrecen controles de acceso y protección que no existen en los sistemas de archivos FAT, FAT32 o FAT32x. Compruebe que todas las particiones de disco de su ordenador están formateadas con NTFS. Si es preciso, utilice el programa Convert para transformar sus particiones FAT en NTFS sin destruir los datos.

Proteger las carpetas compartidas

Por defecto, los ordenadores con Windows XP Professional que no se conectan a un dominio utilizan un modo de acceso a la red denominado Compartición simple de archivos, donde todos los intentos de conexión al ordenador desde la red se convierten en accesos forzados con la cuenta Invitado. Esto supone que el acceso en la red mediante Server Message Blocks (SMB, utilizados para acceso a archivos e impresoras), así como las llamadas a procedimientos remotos (RPC, Remote Procedure Call, utilizados en la mayoría de las herramientas de gestión remota y acceso remoto al registro), solo estarán disponibles para la cuenta Invitado.

En el modelo de Acceso Simple a Archivos, los archivos y carpetas compartidos pueden crearse de manera que el acceso desde la red se haga en modo solo lectura, o alternativamente, con permisos para leer, crear, cambiar y borrar archivos. Simple File Sharing está pensado para usarse en redes domésticas y detrás de un firewall, como el que se incorpora dentro de Windows XP. Si Vd. Está conectado a Internet y no está protegido por un firewall, debe tener presente que cualquier recurso compartido que cree podría ser accedido por cualquier usuario desde Internet.

El modelo clásico de seguridad se utiliza cuando el sistema Windows XP se incorpora a un dominio o cuando se deshabilita Simple File Sharing. En el modelo clásico de seguridad, los usuarios que intentan hacer logon en la máquina local desde la red han de autentificarse como cuentas de usuario propias, no se hacen corresponder con la cuenta de Invitado. De esta manera, los recursos compartidos pueden crearse de modo que solo puedan se accedidos por los grupos y usuarios con los privilegios adecuados.

Utilizar Internet Connection Sharing (ICS) para las conexiones compartidas a Internet

Windows XP ofrece la posibilidad de compartir una única conexión a Internet entre varios ordenadores en una red doméstica o pequeña red empresarial con la función ICS (Internet Connection Sharing). Un ordenador, denominado Host ICS conecta directamente a Internet y comparte esa conexión con el resto de los ordenadores de la red. Las máquinas clientes se apoyan en el host ICS para salir a Internet. El uso de ICS refuerza la seguridad de la red porque solo el host ICS es visible desde Internet.Para activar ICS haga clic con el botón derecho del ratón en una conexión a Internet dentro de la carpeta Conexiones de Red. Haga clic en Propiedades, luego en la solapa Avanzadas y después seleccione el cuadro de opción adecuado. También puede configurar ICS utilizando el Asistente para Redes Domésticas. Para más información acerca de ICS puede consultar el Centro de Soporte y Ayuda en Windows XP.

Habilitar el Firewall de Conexión a Internet (ICF)

El Firewall de conexión a Internet está diseñado para su uso en casa o en pequeñas redes empresariales y proporciona protección para máquinas Windows XP que se conectan directamente a Internet o para ordenadores y dispositivos conectados al host ICS que está ejecutando este Firewall. El Firewall de Conexión a Internet utiliza un filtrado de paquetes activo, lo que significa que los puertos del firewall se abren dinámicamente solo por el tiempo necesario para permitir el acceso a los servicios que se desea.

Para activar ICF haga click con el botón derecho en una conexión a Internet en Conexiones de Red. Después seleccione Propiedades y la solapa Avanzadas, y finalmente, seleccione la opción correspondiente. También puede configurar ICF usando el Asistente para Configuración de Redes Domésticas. Para más información sobre ICF puede consultar el Centro de Soporte y Ayuda en Windows XP.

Utilizar las políticas de restricción de software

Las políticas de restricción de software ponen a disposición de los administradores un mecanismo basado en directivas que identifica el software que se ejecuta en su dominio y permite controlar la ejecución de dicho software. Mediante políticas de restricción de software un administrador puede prevenir la ejecución no deseada de ciertos programas; esto incluye virus, troyanos y otro software del que se sabe que puede causar problemas cuando se instala. Las políticas de restricción de software pueden utilizarse en una máquina aislada configurando las directivas locales de seguridad. Las políticas de restricción de software también están integradas en Políticas de Grupo y Directorio Activo.

Para más detalles acerca de la creación de políticas de restricción de software recomendamos leer el documento **What's New in Security for Windows XP Professional and Windows XP Home Edition white paper.**

Utilizar passwords para las cuentas de usuario

Para proteger a los usuarios que no protegen sus cuentas con passwords, las cuentas de usuario de Windows XP Professional sin password solamente pueden iniciar sesión en la consola física del

ordenador. Por defecto, las cuentas con passwords en blanco no podrán utilizarse en adelante para acceder remotamente desde la red, o para ninguna otra actividad de validación excepto desde la pantalla de inicio de sesión de la consola física. Por ejemplo, no se puede utilizar el servicio de inicio de sesión secundario (“RunAs”) para ejecutar un programa como un usuario local con password en blanco.

Mediante la asignación de passwords a las cuentas locales se evita la restricción que prohibe hacer logon en la red. Esto permite a las cuentas de usuario acceder a los recursos para los cuales tiene permisos, incluso a través de la red. Por consiguiente, es preferible dejar una cuenta con la password en blanco que asignarle una password fácil de descubrir. Cuando se asignen passwords, asegúrese de que tiene una longitud de nueve caracteres como mínimo, y que incluye al menos un signo de puntuación o un carácter ASCII no imprimible dentro de los primeros siete caracteres.

Precauciones

Si su ordenador no está en una ubicación físicamente segura, se recomienda que asigne passwords a todas las cuentas de usuario locales. De no hacerlo así, cualquiera con acceso físico al ordenador podría fácilmente iniciar sesión utilizando una cuenta que no tiene password. Esto es especialmente importante en el caso de portátiles, que deberán siempre blindarse con passwords difíciles de descubrir para todas sus cuentas locales.

Configurar cookies en IE

Si queremos disfrutar de todos los servicios de la mayoría de las Webs y foros actuales, necesitaremos configurar nuestro navegador para aceptar las cookies del mismo servidor y si queremos acceder a nuestras cuentas de correo de Hotmail o de Yahoo entre otras tendremos que aceptar también las cookies de terceros.

Si nuestro sistema operativo es Windows XP o si disponemos de la versión 6.0 del Internet Explorer, podremos indicarle a nuestro navegador que bloquee las cookies y así mismo podremos volverlas a activar en cualquier momento.

Podemos conocer la versión de nuestro Internet Explorer pulsando en el menú Ayuda y después en Acerca de Internet Explorer.

Si has bloqueado las cookies sin darte cuenta y ahora no te acuerdas como reestablecer la configuración original, o si más bien deseas bloquearlas porque requieres de una mayor seguridad en tu navegación puedes hacerlo siguiendo los siguientes pasos:

Lo primero que deberás hacer es abrir tu Internet Explorer y pulsar en el menú Herramientas, seguidamente pulsarás en Opciones, tal como se muestra en la siguiente imagen. En la nueva ventana pulsa la pestaña Privacidad y pulsa el botón Opciones Avanzadas.

Una opción adecuada seria en cookies de origen Aceptar o Pedir datos y en cookies de terceros Bloquear. De nuevo en la pestaña Privacidad pulsa el botón Editar.

Si tenias opciones y bloqueos en las cookies te aparecerán un listado de las Webs visitadas en esta ventana. Si quieres desbloquear las cookies pulsa el botón Quitar todo. Si solo quieres desbloquear alguna, puedes cambiarlo con los botones Bloquear, Permitir o Quitar.

CONSOLA DE RECUPERACIÓN DE WINDOWS 2000 & XP

LA CONSOLA DE RECUPERACIÓN

Vamos a ver es este articulo que es la Consola de Recuperación y como usarla correctamente, ya que se puede convertir en nuestra mejor aliada, sobre todo cuando no es posible acceder a nuestro equipo en “modo seguro”.

La Consola de Recuperación puede llevarnos a engaño por su aspecto austero de línea de comandos, pero puede ser utilizada para recuperarnos de serios problemas de inicio, accediendo a ella como usuario con derechos administrativos.

La ejecución de la Consola de Recuperación se puede llevar a cabo de dos maneras:

- Iniciándola directamente desde el CD de Windows XP

- Instalándola en nuestro sistema y accediendo a ella desde el menú de inicio

1. WINDOWS 2000

Más información

Con la consola de recuperación de Windows 2000 puede obtener acceso limitado a volúmenes NTFS, FAT y FAT32 sin iniciar la interfaz gráfica de Windows. En la consola de recuperación puede:

- Utilizar, copiar, cambiar el nombre o reemplazar archivos y carpetas del sistema operativo.
- Habilitar o deshabilitar el inicio de servicios o dispositivos la próxima vez que inicie el equipo.
- Reparar el sector de inicio del sistema de archivos o el Registro de inicio principal (MBR, *Master Boot Record*).
- Crear y dar formato a particiones de las unidades de disco.

Tenga en cuenta que sólo un administrador puede obtener acceso a la consola de recuperación para que ningún usuario no autorizado pueda utilizar un volumen NTFS.

Iniciar la consola de recuperación

Para iniciar la consola de recuperación, emplee cualquiera de los métodos siguientes:

- Inicie el equipo mediante los discos de instalación de Windows 2000 o con el CD-ROM de Windows 2000. En la pantalla **Programa de instalación**, presione F10 o R para reparar y, después, presione C para iniciar la consola de recuperación.
- Agregue la consola de recuperación a la carpeta Inicio de Windows 2000 mediante la aplicación Winnt32.exe con el modificador "/cmdcons". Esto requiere aproximadamente 7 MB de espacio de disco en la partición de sistema para alojar el directorio y los archivos de cmdcons. Tenga en cuenta que si utiliza el reflejo de software, debe consultar también el siguiente artículo en Microsoft Knowledge Base:
  229077 Mirroring prevents pre-installing the Recovery Console
- Siga las instrucciones del artículo siguiente de Microsoft Knowledge Base:
  222478 Template to Run Recovery Console Using a Remote Install Server

Uso de la consola de comandos

Después de iniciar la consola de recuperación, recibirá el mensaje siguiente:
Intérprete de comandos de la consola de inicio de Windows NT(TM).

ADVERTENCIA:

Este símbolo del sistema tiene funciones limitadas y sólo está diseñado como aplicación de recuperación del sistema para usuarios avanzados. Si utiliza incorrectamente esta aplicación puede tener serios problemas de sistema que requerirán volver a instalar Windows NT para corregirlos.

Escriba 'exit' para salir del símbolo del sistema y reinicie el equipo.

1: C:\WINNT

¿En qué instalación de Windows NT desea iniciar sesión (entrar o anular)?
Después de escribir el número de la instalación de Windows 2000 adecuada, escriba la contraseña de la cuenta Administrador. Tenga en cuenta que si utiliza tres veces una contraseña incorrecta, saldrá de la consola de recuperación. Asimismo, si la base de datos SAM no se encuentra o está dañada, no podrá utilizar la consola de recuperación porque no se puede autenticar correctamente. Después de escribir la contraseña e iniciar la consola de recuperación, si escribe "exit" se reiniciará el equipo.

Restricciones y limitaciones de la consola de comandos

En la consola de recuperación sólo puede utilizar las carpetas siguientes:

- La carpeta raíz.
- La carpeta %SystemRoot% y las subcarpetas de la instalación de Windows 2000 en la que inició sesión.
- La carpeta Cmdcons.
- Unidades de medios extraíbles, por ejemplo unidades de CD-ROM.

NOTA: si trata de obtener acceso a otras carpetas, recibirá un mensaje de error "Acceso denegado". Además, mientras esté en la consola de recuperación no podrá copiar ningún archivo del disco duro local a un disquete. Podrá copiar un archivo de un disquete o un disco compacto a un disco duro, y de un disco duro a otro.

Comandos disponibles

HELP

HELP muestra todos los comandos admitidos siguientes:

ATTRIB DELETE FIXBOOT MD TYPE
CD DIR FIXMBR MKDIR SYSTEMROOT
CHDIR DISABLE FORMAT MORE
CHKDSK DISKPART HELP RD
CLS ENABLE LISTSVC REN
COPY EXIT LOGON RENAME
DEL EXPAND MAP RMDIR

ATTRIB

El comando ATTRIB con cualquiera de los parámetros siguientes puede cambiar los atributos de un archivo o carpeta:

-R
+R
-S
+S

-H
+H

+ Establece un atributo.
- Restablece un atributo.
R Atributo de archivo de sólo lectura.
S Atributo de archivo de sistema.
H Atributo de archivo oculto.

NOTA: es necesario activar o desactivar al menos un atributo. Para ver los atributos, utilice el comando DIR.

CD y CHDIR

Los comandos CD y CHDIR cambian la carpeta. CD.. especifica que desea cambiar a la carpeta principal. Escriba CD unidad: para mostrar la carpeta actual en la unidad especificada. Escriba CD sin parámetros para mostrar la unidad y carpeta actuales. El comando CHDIR trata los espacios como delimitadores. Debido a esto, debe escribir entre comillas los nombres de subcarpeta que contengan espacios. Por ejemplo:

CD "\winnt\profiles\nombreUsuario\programas\menú inicio"

El comando CHDIR sólo funciona en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales.

CHKDSK

CHKDSK *unidad* /P /R

Comprueba y, si es necesario, repara o recupera una unidad. También marca los sectores erróneos y recupera la información legible.

unidad especifica la unidad que desea comprobar. El modificador /P indica a CHKDSK que efectúe una comprobación exhaustiva de la unidad incluso si no tiene problemas marcados y que corrija los errores que encuentre. El modificador /R localiza los sectores erróneos y recupera la información legible. Tenga en cuenta que especificar el modificador /R implica el modificador /P. CHKDSK puede especificarse sin argumentos, en cuyo caso se implica la unidad actual sin modificadores. Opcionalmente, se aceptan los modificadores enumerados. El comando CHKDSK requiere el archivo Autochk.exe. CHKDSK localiza automáticamente este archivo en la carpeta de inicio. Normalmente, se tratará de la carpeta Cmdcons si se instaló previamente la consola de comandos. Si no se encuentra en la carpeta de inicio, CHKDSK intenta localizar los medios de instalación del CD-ROM de Windows 2000. Si no se encuentran los medios de instalación, CHKDSK le pide que proporcione la ubicación del archivo Autochk.exe.

CLS Borra la pantalla.

COPY

COPY *origen destino* Copia un archivo.

origen: especifica el archivo que se va a copiar. No admite comodines o copias de carpetas. Un archivo comprimido del CD-ROM de Windows 2000 se descomprime automáticamente a medida que se copia.
destino: especifica la carpeta o el nombre del nuevo archivo. Si no se especifica, cambia de forma predeterminada a la carpeta actual. Si el archivo ya existe, se le pregunta si desea sobrescribirlo.

DEL y DELETE

DEL *unidad*:*rutanombreArchivo*
DELETE *unidad*:*rutanombreArchivo*
Elimina un archivo

unidad:*rutanombreArchivo* especifica el archivo que se va a borrar.

El comando DELETE sólo funciona en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales. El comando DELETE no acepta caracteres comodín (*).

DIR

DIR *unidad*:*rutanombreArchivo*

Muestra una lista de archivos y subcarpetas de una unidad.

unidad:*rutanombreArchivo*: especifica la unidad, la carpeta y los archivos que se van a mostrar. El comando DIR muestra todos los archivos, incluidos los ocultos y de sistema. Los archivos pueden tener los atributos siguientes:

D: directorio R: archivo de sólo lectura
H: archivo oculto A: archivos preparados para almacenar
S: archivo de sistema C: comprimido
E: cifrado P: punto de reanálisis

El comando DIR sólo funciona en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales.

DISABLE

DISABLE *nombreServicio*

El comando DISABLE deshabilita un servicio del sistema o un controlador de Windows 2000.

nombreServicio: el nombre del servicio o controlador que desea deshabilitar. Puede utilizar el comando LISTSVC para mostrar todos los servicios o controladores disponibles para deshabilitar. DISABLE imprime el tipo de inicio antiguo del servicio antes de establecerlo como SERVICE_DISABLED. Debido a esto, se debe anotar el tipo de inicio antiguo por si es necesario volver a habilitar el servicio.

Los valores de tipo de inicio que muestra el comando DISABLE son:
SERVICE_DISABLED
SERVICE_BOOT_START
SERVICE_SYSTEM_START
SERVICE_AUTO_START
SERVICE_DEMAND_START

DISKPART

DISKPART */add /delete nombreDispositivo nombreUnidad nombrePartición tamaño*

Puede utilizar el comando DISKPART para administrar las particiones de los volúmenes del disco duro.

/add: crea una partición nueva.
/delete: elimina una partición existente.

nombreDispositivo: nombre de dispositivo para crear una partición nueva. El nombre puede obtenerse a partir del resultado del comando MAP. Por ejemplo: \Dispositivo\DiscoDuro0

nombreUnidad: es un nombre basado en la letra de la unidad que se utiliza para eliminar una partición existente. Ejemplo D:

nombrePartición: es un nombre basado en la partición que se emplea para eliminar una partición existente y se puede utilizar en lugar del argumento nombreUnidad. Ejemplo: \Dispositivo\DiscoDuro0\Partición1

tamaño : tamaño de la nueva partición en megabytes.

NOTA: si no se utilizan argumentos, aparecerá una interfaz de usuario que permite administrar las particiones.

ADVERTENCIA: este comando puede dañar la tabla de particiones si el disco se ha actualizado a una configuración de discos dinámicos. No modifique la estructura de discos dinámicos a menos que emplee la herramienta Administración de discos.

ENABLE

ENABLE *nombreServicio tipoInicio*

Puede utilizar el comando ENABLE para habilitar un servicio de sistema o un controlador de Windows 2000.

nombreServicio: el nombre del servicio o controlador que desea habilitar. Puede utilizar el comando LISTSVC para mostrar todos los servicios o controladores disponibles para habilitar. El comando ENABLE imprime el tipo de inicio antiguo del servicio antes de restablecerlo al nuevo valor. Debe anotar el valor antiguo por si es necesario restaurar el tipo de inicio del servicio.

tipoInicio: los valores válidos de tipo de inicio son:

SERVICE_BOOT_START
SERVICE_SYSTEM_START
SERVICE_AUTO_START
SERVICE_DEMAND_START

NOTA: si no se especifica un tipo de inicio nuevo, ENABLE imprime automáticamente el tipo de inicio antiguo.

EXIT

Puede utilizar el comando EXIT para salir de la consola de comandos y reiniciar el equipo.

EXTRACT

EXTRACT *origen destino*

Extrae un archivo del archivo .cab de controladores en el medio de instalación y, a continuación, lo copia al destino.

origen: especifica el nombre del archivo que se va a extraer.

destino: especifica la carpeta o el nombre del nuevo archivo. Si no se especifica, cambia de forma predeterminada a la carpeta actual.

NOTA: este comando sólo funciona cuando el equipo se ha iniciado desde el medio de instalación CD-ROM.

FIXBOOT

FIXBOOT *nombre de unidad*:

escribe código nuevo del sector de inicio de Windows 2000 en la partición de inicio. Esto soluciona problemas causados por daños en el sector de inicio de Windows 2000. El proceso Reparación de emergencia también arregla el sector de inicio.

nombre de unidad: letra de la unidad en la que se escribirá el sector de inicio. Esto suplanta al valor predeterminado, que es escribir en la partición de inicio del sistema. El comando FIXBOOT sólo se admite en la plataforma x86.

FIXMBR

FIXMBR *nombre de dispositivo*

Repara el Registro de inicio principal (MBR) de la partición de sistema. Se utiliza en los casos en que un virus ha dañado el MBR y no puede iniciarse Windows 2000.

ADVERTENCIA: este comando podría dañar las tablas de particiones si hay un virus o si existe un problema de hardware. Este comando puede hacer que las particiones queden inaccesibles. Microsoft sugiere que se ejecute software antivirus antes de utilizar este comando.

nombre de dispositivo : nombre de dispositivo opcional que especifica el dispositivo que necesita un nuevo MBR. El nombre puede obtenerse a partir del resultado del comando MAP. Si se deja en blanco, se repara el MBR del dispositivo de inicio. Por ejemplo:

FIXMBR \dispositivo\discoDuro2

Si FIXMBR detecta una firma de tabla de particiones no válida o diferente de la estándar, le pide permiso antes de volver a escribir el MBR. El comando FIXMBR sólo se admite en la plataforma x86.

FORMAT

FORMAT *unidad: /Q /FS:sistema de archivos*

Da formato a la unidad especificada con el sistema de archivos especificado.

unidad: letra de unidad de la partición a la que se va a dar formato.
/Q: da formato rápidamente a la unidad.
/FS:sistema de archivos: especifica el tipo de sistema de archivos que se va a utilizar: FAT, FAT32 o NTFS. Si no se especifica ninguno, se emplea el formato de sistema de archivos existente si hay uno disponible.

LISTSVC

El comando LISTSVC muestra todos los servicios y controladores disponibles y sus tipos de inicio para la instalación actual de Windows 2000. Esto puede resultar útil al emplear los comandos DISABLE y ENABLE.

NOTA: los valores se extraen del sector %systemroot%\System32\config\SYSTEM. Si el sector SYSTEM está dañado o no se encuentra, pueden producirse resultados impredecibles.

LOGON

LOGON

El comando LOGON muestra todas las instalaciones detectadas de Windows 2000 y Windows NT, y le pide la contraseña de administrador local para la copia de Windows en la que haya elegido iniciar sesión. Si efectúa más de tres intentos de inicio de sesión sin éxito, se cerrará la consola y se reiniciará el equipo.

MAP

MAP *arc*

El comando MAP muestra las letras de unidades, los tipos de sistemas de archivos, los tamaños de las particiones y las asignaciones de dispositivos físicos.

arc: el parámetro arc indica a MAP que utilice rutas de acceso ARC en lugar de rutas de acceso de dispositivo de Windows.

MD y MKDIR

Los comandos MD y MKDIR crean carpetas. No admiten caracteres comodín. El comando MKDIR sólo funciona en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales.

MORE

MORE *nombreArchivo*

El comando MORE muestra un archivo de texto en la pantalla.

RD y RMDIR

Los comandos RD y RMDIR eliminan una carpeta.

Los comandos RMDIR y RD sólo funcionan en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales.

REN y RENAME

Los comandos REN y RENAME pueden cambiar el nombre de un archivo. Tenga en cuenta que no se puede especificar una nueva unidad o ruta de acceso para el archivo de destino. Los comandos REN y RENAME sólo funcionan en las carpetas de sistema de la instalación actual de Windows 2000, en medios extraíbles, en la carpeta raíz de una partición de disco duro o en los orígenes de instalación locales.

SET

El comando SET permite mostrar o modificar las opciones de entorno.
AllowWildCards = FALSE
AllowAllPaths = FALSE
AllowRemovableMedia = FALSE
NoCopyPrompt = FALSE

SYSTEMROOT

El comando SYSTEMROOT establece la carpeta de trabajo actual como la carpeta %SystemRoot% de la instalación de Windows 2000 en la que ha iniciado sesión.

TYPE

TYPE *nombreArchivo*

El comando TYPE muestra un archivo de texto.

2. WINDOWS XP

Resumen

Para recuperar el sistema operativo cuando el equipo no se inicia correctamente o no se inicia, es posible que quiera instalar y usar la consola de recuperación de Windows. Sin embargo, Microsoft sólo recomienda este método de recuperación del sistema a los usuarios avanzados. En relación con la consola de recuperación aprenda también acerca del símbolo del sistema, las acciones de comandos, las reglas y el modo de quitarla, así como la forma de instalarla durante una instalación desatendida.

INTRODUCCIÓN

Microsoft recomienda que use la consola de recuperación sólo cuando no haya funcionado el Modo a prueba de errores y otras opciones de inicio. La consola de recuperación sólo se recomienda para usuarios avanzados que sepan utilizar los comandos básicos para identificar y buscar problemas en controladores y archivos. Además, se requiere ser administrador para utilizar la consola de recuperación.

Más información

Cómo instalar la consola de recuperación

Puede instalar la consola de recuperación en el equipo para tenerla disponible si no puede reiniciar Windows. Puede seleccionar la opción Consola de recuperación en la lista de sistemas operativos disponibles durante el inicio. Instale la consola de recuperación en los servidores importantes y en las estaciones de trabajo del personal de IT. Este artículo describe cómo instalar la consola de recuperación en un equipo con Microsoft Windows XP. Para instalar la consola de recuperación, debe iniciar sesión como administrador.

Si bien es posible ejecutar la consola de recuperación arrancando directamente desde el CD de Windows XP, suele ser más conveniente configurarla como opción en el menú de inicio. Para ejecutar la consola de recuperación directamente desde el CD, consulte la sección "Cómo utilizar la consola de recuperación".

Para instalar la consola de recuperación, siga estos pasos:

1. Inserte el CD de Windows XP en la unidad de CD-ROM.
2. Haga clic en **Inicio** y, a continuación, en **Ejecutar**.
3. En el cuadro **Abrir**, escriba *d*:\i386\winnt32.exe /cmdcons donde *d* es la letra de la unidad de CD-ROM.
4. Aparece un cuadro de diálogo de instalación de Windows. El cuadro de diálogo Programa de instalación de Windows describe la opción Consola de recuperación. Para confirmar la instalación, haga clic en **Sí**.
5. Reinicie el equipo. La próxima vez que inicie su equipo, aparecerá "Consola de recuperación de Microsoft Windows" en el menú de inicio.

Nota: como alternativa, puede utilizar una conexión establecida conforme a la especificación UNC (convención de nomenclatura universal) para instalar la consola de recuperación desde un recurso compartido de red.

Cómo utilizar la consola de recuperación
Puede habilitar y deshabilitar servicios, dar formato a unidades, leer y escribir datos en una unidad local (incluyendo las unidades a las que se les ha dado formato para utilizar el sistema de archivos NTFS) y realizar otras muchas tareas administrativas. La consola de recuperación es particularmente útil si tiene que reparar el equipo copiando un archivo en su unidad de disco duro desde un disco o un CD-ROM, o si tiene que reconfigurar un servicio que impide que el equipo se inicie correctamente.

Si no puede iniciar el equipo, puede ejecutar la consola de recuperación desde los discos de inicio o el CD-ROM de Microsoft Windows XP. En este artículo se describe cómo realizar esta tarea.

Una vez instalado Windows XP en el equipo, para iniciar el equipo y usar la consola de recuperación necesita los discos de inicio o el CD-ROM de Windows XP.

Para obtener información adicional acerca de cómo crear discos de inicio para Windows XP (no se incluyen con Windows XP), haga clic en el número de artículo siguiente para verlo en Microsoft Knowledge Base:
310994 Obtener discos de inicio del programa de instalación de Windows XP.

Nota: para iniciar el equipo desde el CD-ROM de Windows XP, deberá configurar el sistema básico de entrada y salida (BIOS) del equipo para que se inicie desde la unidad de CD-ROM.

Para ejecutar la consola de recuperación desde los discos de inicio o el CD-ROM de Windows XP, siga estos pasos:

1. Inserte el disco de inicio de Windows XP en la unidad de disquete o inserte el CD-ROM de Windows XP en la unidad de CD-ROM y, a continuación, reinicie el equipo.
   Si se le pide, haga clic para seleccionar las opciones necesarias que se le soliciten para iniciar el equipo desde la unidad de CD-ROM.
2. Cuando aparezca la pantalla "Programa de instalación", presione R para iniciar la consola de recuperación.
3. Si tiene un equipo con inicio dual o múltiple, seleccione la instalación a la que debe tener acceso desde la consola de recuperación.
4. Cuando se le indique, escriba la contraseña de administrador. Si la contraseña de administrador estuviera en blanco, presione ENTRAR.

   En el símbolo del sistema, escriba los comandos apropiados para diagnosticar y reparar la instalación de Windows XP.

5. Para obtener una lista de los comandos disponibles en la consola de recuperación, escriba recovery console commands o help en el símbolo del sistema y presione ENTRAR.

   Para obtener información acerca de un comando concreto, escriba help *nombreComando* en el símbolo del sistema y, después, presione ENTRAR.
6. Para salir de la consola de recuperación y reiniciar el equipo, escriba exit en el símbolo del sistema y presione ENTRAR.

Cómo utilizar el símbolo del sistema de la consola de recuperación
Cuando usa la consola de recuperación, trabaja en un símbolo del sistema especial, no en el ordinario de Windows. La consola de recuperación tiene su propio intérprete de comandos. Para

utilizar este intérprete de comandos, la consola de recuperación le pide que escriba la contraseña de administrador local.

Una vez iniciada la consola de recuperación, puede presionar F6 para instalar un controlador SCSI o RAID de otro fabricante, en caso de que sea necesario para el acceso al disco duro. Este indicador funciona del mismo modo que durante la instalación del sistema operativo.

La consola de recuperación tarda unos segundos en iniciarse. Cuando aparece el menú de la consola de recuperación, se muestra una lista numerada de las instalaciones de Windows existentes en el equipo. (Normalmente, sólo existe c:\Windows.) Aun cuando sólo se muestre una entrada, deberá presionar el número correspondiente antes de presionar ENTRAR. Si presiona ENTRAR sin seleccionar el número, el equipo se reiniciará y todo el proceso comenzará de nuevo.

En cuanto vea el indicador de %raízSistema% (normalmente, C:\\Windows), podrá empezar a utilizar los comandos disponibles de la consola de recuperación.

Consulta Rápida de las Acciones de comando

La lista siguiente describe los comandos disponibles para la consola de recuperación:

- **Attrib**: cambia los atributos en un archivo o subdirectorio.
- **Batch**: ejecuta los comandos especificados en el archivo de texto, ArchivoEntrada. ArchivoSal contiene la salida de los comandos. Si omite el parámetro ArchivoSal, el resultado se mostrará en la pantalla.
- **Bootcfg**: modifica el archivo Boot.ini file para la recuperación y configuración del inicio.
- **CD (Chdir)**: sólo funciona en los directorios de sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición del disco duro y en los orígenes de instalación locales.
- **Chkdsk**: el modificador **/p** ejecuta Chkdsk incluso aunque la unidad no se haya etiquetado como "incorrecta". El modificador **/r** busca posibles sectores defectuosos y recupera en ellos la información legible. Este modificado implica a **/p**. Chkdsk requiere Autochk. Chkdsk busca automáticamente Autochk.exe en la carpeta de inicio. Si Chkdsk no puede encontrar el archivo en la carpeta de inicio, lo busca en el CD-ROM de instalación de Windows 2000. Si Chkdsk no puede encontrar el CD-ROM de instalación, Chkdsk pregunta al usuario por la ubicación de Autochk.exe.
- **Cls**: borra la pantalla.
- **Copy**: copia un archivo en una ubicación de destino. De manera predeterminada, el destino no puede ser un soporte extraíble y, además, no puede usar caracteres de tipo comodín. Al copiar un archivo comprimido desde el CD-ROM de instalación, se descomprime el archivo automáticamente.
- **Del (Delete)**: elimina un archivo. Sólo funciona en los directorios de sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición del disco duro y en los orígenes de instalación locales. De manera predeterminada, no puede usar caracteres comodín.
- **Dir**: muestra todos los archivos, incluidos los ocultos y los de sistema.
- **Disable**: deshabilita un controlador o un servicio del sistema de Windows. La variable *servicio_o_controlador* es el nombre del servicio o del controlador que quiere deshabilitar. Cuando utiliza este comando para deshabilitar un servicio, el comando muestra el tipo de inicio original del servicio antes de cambiar el tipo a SERVICE_DISABLED. Anote el tipo de inicio original para que pueda usar el comando **enable** para reiniciar el servicio.
- **Diskpart**: administra las particiones en los volúmenes del disco duro. La opción **/add** crea una partición nueva. La opción **/delete** elimina una partición existente. La variable de dispositivo es el nombre de dispositivo para la nueva partición (como \dispositivo\discoduro0). La variable de

unidad es la letra de unidad que para una partición que está eliminado (por ejemplo, D). Partición es el nombre basado en la partición para una partición que está eliminando (por ejemplo: \dispositivo\discoduro0\partición1) y se puede usar en lugar de la variable de unidad. El tamaño de la variable es el tamaño, en magabytes, de una nueva partición.

- **Enable**: habilita un controlador o un servicio del sistema de Windows. La variable *servicio_o_controlador* es el nombre del servicio o del controlador que quiere habilitar y *tipo_inicio* es el tipo de inicio de un servicio habilitado. El tipo de inicio usa uno de los siguientes formatos:
  SERVICE_BOOT_START
  SERVICE_SYSTEM_START
  SERVICE_AUTO_START
  SERVICE_DEMAND_START
- **Exit**: sale de la consola de recuperación y reinicia el equipo.
- **Expand**: expande un archivo comprimido. La variable de origen es el archivo que quiere expandir. De manera predeterminada, no puede usar caracteres comodín. La variable de destino es el directorio para el nuevo archivo. De manera predeterminada, el destino no puede ser un soporte extraíble y no puede ser de sólo lectura. Puede usar el comando **attrib** para quitar del directorio de destino el atributo de sólo lectura. Se requiere la opción **/f:filespec** si el origen contiene más de un archivo. Esta opción permite caracteres comodín. El modificador **/y** deshabilita el comando de confirmación de sobrescritura. El modificador **/d** especifica que los archivos no se expandirán y muestra un directorio de los archivos en el origen.
- **Fixboot**: escribe un nuevo sector de inicio en la partición del sistema.
- **Fixmbr**: repara el código de inicio principal de la partición de inicio. La variable de dispositivo es un nombre opcional que especifica el dispositivo que requiere un registro de inicio maestro. Omita esta variable cuando el destino sea el dispositivo de inicio.
- **Format**: da formato a un disco. El modificador **/q** ejecuta un formato rápido. El modificador **/fs** especifica el sistema de archivos.
- **Help**: si no usa la variable de comandos para especificar un comando, **help** enumera todos los comandos que son compatibles con la consola de recuperación.
- **Listsvc**: muestra todos los controladores y servicios disponibles en el equipo.
- **Logon** muestra las instalaciones de Windows detectadas y solicita la contraseña de administrador local para esas instalaciones. Use este comando para pasar a otra instalación o subdirectorio.
- **Map**: muestra las asignaciones de dispositivo activas actualmente. Incluya la opción **arc** para especificar el uso de rutas de Computación avanzada de RISC (ARC) (el formato para Boot.ini), en lugar de las rutas de dispositivo de Windows.
- **MD (Mkdir)**: sólo funciona en los directorios de sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición del disco duro y en los orígenes de instalación locales.
- **More/Type**: muestra en pantalla el archivo de texto especificado.
- **Net Use**: conecta con un recurso compartido remoto para la consola de recuperación de Windows XP. El texto siguiente describe la sintaxis de este comando:
  NET USE [nombreDispositivo | *] [\\nombreEquipo\nombreRecursoCompartido[\volumen] [contraseña | *]]
  [/USER:[nombreDominio\]nombreUsuario]
  [/USER:[nombre dominio con puntos\]nombreUsuario]
  [/USER:[nombreUsuario@[nombre dominio con puntos]
  [/SMARTCARD]
  [/SAVECRED]
  [[/DELETE] | [/PERSISTENT:{YES | NO}]]

NET USE {nombreDispositivo | *} [contraseña | *] /HOME

NET USE [/PERSISTENT:{YES | NO}]

- **Rd (Rmdir)**: sólo funciona en los directorios de sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición del disco duro y en los orígenes de instalación locales.
- **Ren (Rename)**: sólo funciona en los directorios de sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición del disco duro y en los orígenes de instalación locales. No puede especificar una nueva unidad o ruta como destino.
- **Set**: muestra y configura las variables de entorno de la consola de recuperación.
- **Systemroot**: configura el directorio actual en %raízSistema%.

Consulta Rápida de Reglas de la consola de recuperación

Mientras se trabaja con la consola de recuperación se aplican varias reglas de entorno. Escriba set para ver el entorno actual. De manera predeterminada, las reglas son éstas:

- **AllowAllPaths = FALSE**: evita el acceso a los directorios y subdirectorios desde fuera de la instalación de sistema seleccionada al entrar en la consola de recuperación.
- **AllowRemovableMedia = FALSE**: evita el acceso a los medios extraíbles como destino para la copia de archivos.
- **AllowWildCards = FALSE** evita la compatibilidad con comodines para comandos como **copy** y **del**.
- **NoCopyPrompt = FALSE**: significa que la consola de recuperación solicitará confirmación antes de sobrescribir un archivo existente.

Consulta Rápida de Cómo eliminar la consola de recuperación

Para eliminar la consola de recuperación:

1. Reinicie el equipo, haga clic en **Inicio**, seleccione **Mi PC** y, a continuación, haga doble clic en el disco duro en el que tenga instalada la consola de recuperación.
2. En el menú **Herramientas**, haga clic en **Opciones de carpeta** y, a continuación, haga clic en la ficha **Ver**.
3. Haga clic en **Mostrar todos los archivos y carpetas ocultos**, desactive la casilla de verificación **Ocultar archivos protegidos del sistema operativo** y, a continuación, haga clic en **Aceptar**.
4. En la carpeta raíz, elimine la carpeta **Cmdcons** y el archivo **Cmldr**.
5. En la carpeta raíz, haga clic con el botón secundario del *mouse* en el archivo **Boot.ini** y, a continuación, haga clic en **Propiedades**.
   Desactive la casilla de verificación **Sólo lectura** y, a continuación, haga clic en **Aceptar**.
6. **Advertencia**: la modificación incorrecta del archivo Boot.ini puede impedir que se reinicie el equipo. Asegúrese de que elimina únicamente la entrada correspondiente a la consola de recuperación. Asimismo, una vez finalizado este procedimiento, devuelva al archivo Boot.ini el atributo de sólo lectura. Abra el archivo Boot.ini en el Bloc de Notas de Microsoft Windows y quite la entrada de la consola de recuperación. El resultado será similar a éste:
   C:\cmdcons\bootsect.dat="Microsoft Windows Recovery Console" /cmdcons
7. Guarde el archivo y ciérrelo.

Cómo instalar la consola de recuperación durante una instalación desatendida

Para instalar la consola de recuperación durante la instalación desatendida de Windows, debe usar la sección [GuiRunOnce] del archivo unattend.txt.
Command1="*ruta*\winnt32 /cmdcons /unattend"

INICIO DE LA CONSOLA DESDE EL CD DE WINDOWS XP

- Cambiamos la secuencia de arranque de nuestro equipo desde las opciones “Advance BIOS Features” de nuestra BIOS y colocamos el CD como primer dispositivo de lectura en el arranque o reinicio “First Boot Device”
- Colocamos el CD de Windows XP en su bandeja y reiniciamos nuestro equipo
- Pulsamos cualquier tecla para iniciar desde CD (veras un aviso en el extremo inferior de la pantalla “Presiona cualquier tecla para iniciar desde el CD”)
- Esperamos a la carga de archivos
- Aparecerá la pantalla de instalación de Windows XP y seleccionamos la opción del medio “Para recuperar una instalación de Windows XP usando la consola de recuperación, presiona la tecla R”
- Si tenemos multiarranque, seleccionaremos el sistema a recuperar mediante el numeral correspondiente al que este asociado en la pantalla
- Te solicitará posteriormente la contraseña de administrador que pusiste cuando instalaste el sistema por primera vez (OJO, la consola NO activa el “num lock”, si tu contraseña tiene números y usas el teclado numérico de la derecha del teclado, actívalo)
- Mas adelante se describen los comandos, pero si quieres verlos desde la pantalla de la Consola de Recuperación, escribe “help”, una vez obtenidos, puedes ver una descripción de los mismos escribiendo “help comando”
- Para salir de la Consola de Recuperación y reiniciar el equipo, escribiremos “exit”.

INSTALACIÓN DE LA CONSOLA DE RECUPERACIÓN EN EL MENU DE INICIO

- Colocamos el CD de Windows XP en su unidad y desde “Inicio – Ejecutar”, escribimos:

- X:\i386\winnt32.exe /cmdcons

- Donde “X” corresponde a la letra de la unidad donde se encuentra el CD.

- Aparecerá un mensaje del programa de instalación que describe la opción de la Consola de Recuperación, el espacio que requiere en el disco duro y la pregunta:

Desea instalar la Consola de Recuperación?

- Pulsamos “SI” y la próxima vez que arranquemos nuestro equipo, tendremos en el menú de arranque la opción de la Consola de Recuperación.

- Una de las mayores ventajas de la Consola de Recuperación respecto por ejemplo al “modo seguro”, es que esta, nos permite acceder incluso en el caso que existan archivos corruptos y desde la misma es posible realizar las siguientes opciones:

- Copiar, cambiar, reemplazar, cambiar el nombre de archivos y carpeta de XP
- Activar o desactivar Servicios o dispositivos
- Crear y dar formato a unidades
- Reparar el sector de arranque
- Reparar el sistema desde un CD

RESTRICCIONES

Solo será posible acceder a los archivos que se encuentren en las siguientes ubicaciones:

- El directorio raíz de cualquier volumen
- La carpeta %SystemRoot% y las carpetas que cuelgan de ella donde XP se haya instalado (C:\Windows por regla general)
- La carpeta Cmdcons de la Consola de Recuperación y sus subcarpetas (solo si hemos instalado la Consola de Recuperación como opción en el menú de inicio)
- Los archivos y carpetas que se encuentran en discos extraíbles (CD, ZIP, disquetes)

REPARAR ARCHIVOS DE ARRANQUE DAÑADOS

Archivo boot.ini esta dañado o no aparece, desde la Consola de Recuperación, escribimos:

- bootcfg/scan para ver las instalaciones de XP disponibles en todos los discos
- bootcfg/rebuild para reemplazar automáticamente el archivo boot.ini existente
- bootcfg/add para añadir una instalación de XP a boot.ini sin cambiar las entradas existentes.

Archivos críticos del sistema están dañados o no están:

Podemos restaurar los archivos Ntldr, Ntoskrnl.exe, Ntdetect.com y controladores en función de su ubicación, si el archivo esta en el CD de XP, podemos usar el comando “copy” especificando origen y destino.

Windows abre automáticamente los archivos comprimidos, en el caso que estos se encuentren en un archivo “*.cab”, deberemos utilizar el comando “expand”.

Otro sistema ha reemplazado el código del sector de arranque:

Escribiremos:

Fixboot

Para rescribir el código del sector de arranque, deberemos reiniciar el sistema.

ACTIVAR-DESACTIVAR SERVICIO Y CONTROLADORES

Debemos saber que no todos los servicios de XP pertenecen al sistema, algunos de ellos son instalados por terceros, por ejemplo, Nvidia, así como los controladores. Algunas veces estos servicios y controladores de terceros, no están escritos o programados de manera eficiente y causan problemas en XP generando reinicios o paradas del sistema incluso entrando al mismo en “modo seguro”.

Con la Consola de Recuperación, podremos por ejemplo desactivar un servicio si sospechamos que es el causante del problema y no podemos acceder al sistema en “modo seguro”.

Listsvc Con este comando, podemos ver una lista de los servicios y controladores del sistema y su estado actual

Disable Con este comando, seguido del nombre del controlador o servicio, podremos detenerlo. Este comando define el tipo de inicio del servicio como “service_disabled”, así que antes de

hacerlo, deberemos consultar el valor del tipo de inicio actual del servicio a deshabilitar: service_boot_start, service_system_start, service_auto_start o service_demand_start y tomar nota del mismo para el caso de volverlo a activar.

Enable Con este comando, seguido del nombre del servicio o controlador mas el valor del tipo de inicio que anotamos al deshabilitarlo, podremos volver a activar el servicio o controlador deshabilitado, una vez comprobado que no es el causante de nuestro problema.

EXPLICACIÓN A FONDO DE LOS COMANDOS DE LA CONSOLA DE RECUPERACIÓN

Attrib

Cambia los atributos de archivo de un único archivo o directorio. Este comando establece o quita los atributos de sólo lectura, sistema, oculto y comprimido asignados a los archivos o a los directorios.

El comando attrib con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando attrib con distintos parámetros está disponible desde el símbolo del sistema.

attrib [+r|-r] [+s|-s] [+h|-h] [+c|-c] [[unidad:][rutaDeAcceso] nombreDeArchivo]

Parámetros

+r Establece el atributo de archivo de sólo lectura.
-r Quita el atributo de archivo de sólo lectura.
+s Establece el atributo de archivo del sistema.
-s Quita el atributo de archivo del sistema.
+h Establece el atributo de archivo oculto.
-h Quita el atributo de archivo oculto.
+c Establece el atributo de archivo comprimido.
-c Quita el atributo de archivo comprimido.
[[unidad:][rutaDeAcceso] nombreDeArchivo]

Especifica la ubicación y el nombre del archivo o el directorio que desea procesar. Puede cambiar los atributos para sólo un archivo o un directorio cada vez.

Nota
• Puede cambiar varios atributos para un archivo o un directorio determinados con un único comando.

Batch

Ejecuta los comandos especificados en un archivo de texto. El comando batch sólo está disponible cuando se utiliza la Consola de Recuperacion, que se puede iniciar desde el CD de instalación. batch archivoDeEntrada [archivoDeSalida]

Parámetros

archivoDeEntrada

Especifica el archivo de texto que contiene la lista de comandos que se van a ejecutar. archivoDeEntrada puede constar de una letra de unidad seguida de un signo de dos puntos, un nombre de directorio, un nombre de archivo o una combinación de ellos.

archivoDeSalida
Si se especifica alguno, almacena el resultado de los comandos en el archivo citado. Si no se especifica este parámetro, el resultado se presentará en la pantalla.

Ejemplo
El ejemplo siguiente ejecuta el archivo de proceso por lotes C:\Trabajos\Buscar.txt y almacena el resultado en el archivo C:\Trabajos\Resultados.txt:
batch c:\trabajos\buscar.txt c:\trabajos\resultados.txt

Nota
- Un archivo por lotes no puede contener un comando batch anidado.

Bootcfg
Utilice el comando bootcfg para la configuración y recuperación de inicio (boot.ini en la mayoría de los equipos).

El comando bootcfg con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando bootcfg con distintos parámetros está disponible desde el símbolo del sistema.

Uso:

bootcfg /default
Establece la entrada de inicio predeterminada.

bootcfg /add
Agrega una instalación de Windows a la lista de inicio.

bootcfg /rebuild
Se repite en todas las instalaciones de Windows y permite al usuario elegir qué elementos agregará.

Nota
- Antes de utilizar ***bootcfg /rebuild*** debe haber hecho previamente una copia de seguridad del archivo boot.ini mediante ***bootcfg /copy.***

bootcfg /scan
Analiza todos los discos para encontrar instalaciones de Windows y muestra los resultados.

Nota
- Estos resultados se almacenan estáticamente durante la sesión actual. Si la configuración del disco cambia durante esta sesión, deberá reiniciar el equipo y volver a examinar los discos para poder obtener un recorrido actualizado.

bootcfg /list
Enumera las entradas ya incluidas en la lista de inicio.

bootcfg /disableredirect
Deshabilita la redirección en el cargador de inicio.

bootcfg /redirect [velocidadBaudiosPuerto] | [utilizarConfiguraciónBios]
Habilita la redirección en el cargador de inicio con la configuración especificada.

Ejemplo:
bootcfg /redirect com1 115200

bootcfg /redirect useBiosSettings

Chdir (Cd)
Muestra el nombre del directorio actual o cambia la carpeta actual.
El comando chdir o cd con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando chdir con distintos parámetros está disponible desde el símbolo del sistema.

chdir [unidad:][rutaDeAcceso] [..]
o bien
cd [unidad:][rutaDeAcceso] [..]

Parámetros: ninguno
Si utiliza el comando chdir sin parámetros, muestra el nombre de la carpeta y la unidad actuales. Si lo utiliza solamente con una letra de unidad (por ejemplo, cd C:), chdir muestra el directorio actual de la unidad especificada.

[unidad:][rutaDeAcceso]
Especifica la unidad (si es distinta de la unidad actual) y el directorio a los que desea cambiar.

[..]
Especifica que desea cambiar a la carpeta principal. Utilice un espacio en blanco entre chdir y el signo de dos puntos.

Notas
- Chdir trata los espacios como delimitadores. Utilice comillas alrededor de un nombre de directorio que contenga espacios en blanco. Por ejemplo:
  cd "caché de controladores"
- Chdir funciona únicamente dentro de los directorios del sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición de disco duro o en los orígenes de la instalación local.

Chkdsk
Crea y muestra un informe de estado del disco duro. El comando chkdsk también enumera y corrige los errores del disco.

El comando chkdsk con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando chkdsk con distintos parámetros está disponible desde el símbolo del sistema.
chkdsk [unidad:] [/p] [/r]

Parámetros: ninguno

Si se utiliza sin parámetros, chkdsk muestra el estado del disco de la unidad actual.

unidad: Especifica la unidad que se desea comprobar mediante chkdsk.

/p
Realiza una comprobación exhaustiva aunque la unidad no esté marcada para que se ejecute chkdsk. Este parámetro no realiza cambios en la unidad.

/r
Encuentra los sectores defectuosos y recupera la información que sea legible. Implica /p.

Nota
• El comando chkdsk requiere el archivo Autochk.exe. Si no lo puede encontrar en el directorio de inicio (\%systemroot%\System32, de forma predeterminada), lo buscará en el CD de instalación de Windows. Si dispone de un equipo de inicio múltiple, asegúrese de especificar este comando desde la unidad que contiene Windows.

Cls
Borra la pantalla. La pantalla mostrará únicamente el símbolo del sistema y el punto de inserción.

cls
Parámetros: ninguno

Copy
Copia un archivo a otra ubicación. El comando copy con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando copy con distintos parámetros está disponible desde el símbolo del sistema.
copy origen [destino]

Parámetros

origen
Especifica el nombre y la ubicación del archivo que se va a copiar. Origen puede constar de una letra de unidad y un signo de dos puntos, un nombre de directorio, un nombre de archivo o una combinación de ellos.

destino
Especifica la ubicación y el nombre del archivo o el conjunto de archivos donde se colocará la copia. Destino puede constar de una letra de unidad y un signo de dos puntos, un nombre de carpeta, un nombre de archivo o una combinación de ellos.

Notas
- El origen puede ser medios extraíbles, cualquier directorio contenido en los directorios del sistema de la instalación actual de Windows, el directorio raíz de cualquier unidad, los orígenes de instalación local o el directorio Cmdcons.
- El destino puede ser cualquiera de las mismas ubicaciones que el origen, salvo los medios extraíbles. Si no se especifica un destino, la copia se realizará de forma predeterminada en el directorio actual.
- Los archivos comprimidos del CD de instalación de Windows se descomprimen a medida que se copian.
- Copy no acepta caracteres comodín.

Delete (Del)
Elimina un archivo. El comando delete o del con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando delete o del con distintos parámetros está disponible desde el símbolo del sistema.

delete [unidad:][rutaDeAcceso] nombreDeArchivo
o bien
del [unidad:][rutaDeAcceso] nombreDeArchivo

Parámetros

[unidad:][rutaDeAcceso] nombreDeArchivo
Especifica la ubicación y el nombre del archivo que desea eliminar.

Nota
• Delete funciona únicamente dentro de los directorios del sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición de disco duro o en los orígenes de la instalación local.

Dir
Muestra una lista de los archivos y subdirectorios de un directorio. El comando dir con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando dir con distintos parámetros está disponible desde el símbolo del sistema.
dir [unidad:][rutaDeAcceso][nombreDeArchivo]

Parámetros

[unidad:][rutaDeAcceso]
Especifica la unidad y el directorio cuya lista desea ver.

[nombreDeArchivo]
Especifica el archivo o el grupo de archivos cuya lista desea ver. Pueden utilizarse varios nombres de archivo. Los nombres de archivo pueden separarse mediante espacios en blanco, comas o signos de punto y coma. Puede utilizar caracteres comodín (? y *) con el parámetro nombreDeArchivo para mostrar un grupo de archivos.

Dir también muestra la etiqueta de volumen y el número de serie del disco, así como el número total de archivos enumerados, su tamaño acumulado y el espacio libre (en bytes) que queda en el disco. Para cada archivo y subdirectorio, dir muestra la extensión del nombre de archivo, el tamaño en bytes del archivo, la fecha y la hora en que se modificó por última vez el archivo y los siguientes atributos, si procede:

Abreviatura	Atributo
d	Directorio
h	Archivo oculto
s	Archivo del sistema
e	Cifrado
r	Sólo lectura
a	Archivos listos para archivar
c	Comprimidos
p	Punto de análisis repetido

Nota
• Dir funciona únicamente dentro de los directorios del sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición de disco duro y en los orígenes de la instalación local.

Disable
Deshabilita un servicio o un controlador de dispositivo del sistema de Windows XP, Windows 2000 o Windows NT 4.0. El comando disable sólo está disponible cuando se utiliza la Consola de recuperación.
disable [nombreDeServicio] | [nombreDeControladorDeDispositivo]

Parámetros

nombreDeServicio
El nombre del servicio del sistema que desea deshabilitar.

nombreDeControladorDeDispositivo

El nombre del controlador de dispositivo que desea deshabilitar.
Ejemplo
El siguiente ejemplo deshabilita el servicio Registro de sucesos:
disable eventlog

Notas
• El comando disable establece el tipo de inicio como SERVICE_DISABLED para el servicio o el controlador que especifique.

• Cuando utilice el comando disable para deshabilitar un servicio del sistema o un controlador de dispositivo, el nombre del tipo de inicio anterior correspondiente al servicio del sistema o al controlador de dispositivo aparecerá en la pantalla. Debe anotar este nombre por si tiene que restaurar el tipo de inicio a su configuración anterior mediante el comando enable.

• Hay cinco tipos de inicio: Los tres primeros, SERVICE_AUTO_START, SERVICE_DISABLED y SERVICE_DEMAND_START, corresponden a los tipos de inicio estándar (Automático, Deshabilitado y Manual) que suele configurar mediante Servicios en la herramienta administrativa Administración de equipos. Los dos últimos, SERVICE_BOOT_START y SERVICE_SYSTEM_START, se utilizan normalmente para configurar el modo en que se cargan los controladores de dispositivo; por ejemplo, cuando se inicia el equipo o cuando se inicia Windows.

Diskpart
Crea y elimina particiones de discos duros. El comando diskpart sólo está disponible cuando se utiliza la Consola de recuperación.

diskpart [/add | /delete] [nombreDeDispositivo | nombreDeUnidad | nombreDePartición] [tamaño]

Parámetros: ninguno

Si se utiliza sin parámetros, el comando diskpart inicia la versión en modo de caracteres de Windows de diskpart.

/add
Crea una partición nueva.

/delete
Elimina una partición existente.

nombreDeDispositivo
El dispositivo en el que desea crear o eliminar una partición. El nombre se puede obtener del resultado del comando map. He aquí un ejemplo de un nombre de dispositivo:
\Device\HardDisk0
nombreDeUnidad

La partición que desea eliminar, por letra de unidad. Sólo se utiliza con /delete. A continuación se muestra un ejemplo de nombre de unidad:
D:

nombreDePartición
La partición que desea eliminar, por nombre de partición. Se puede utilizar en lugar de nombreUnidad. Sólo se utiliza con /delete. He aquí un ejemplo de nombre de partición:
\Device\HardDisk0\Partition1

tamaño
El tamaño, en megabytes (MB), de la partición que desea crear. Sólo se utiliza con /add.

Ejemplos
Los siguientes ejemplos eliminan una partición:
diskpart /delete \Device\HardDisk0\Partition3
diskpart /delete F:

El siguiente ejemplo agrega una partición de 20 MB al disco duro:
diskpart /add \Device\HardDisk0 20

Enable
Habilita o inicia un servicio o un controlador de dispositivo del sistema de Windows XP, Windows 2000 o Windows NT 4.0. El comando enable sólo está disponible cuando se utiliza la Consola de recuperación.

enable {nombreDeServicio | nombreDeControladorDeDispositivo} [tipoDeInicio]

Parámetros

nombreDeServicio
El nombre del servicio del sistema que desea habilitar.

nombreDeControladorDeDispositivo
El nombre del controlador de dispositivo que desea habilitar.

tipoDeInicio
El tipo de inicio que desea designar para el servicio o el controlador de dispositivo. Entre los tipos de inicio válidos se incluyen:

- SERVICE_BOOT_START
- SERVICE_SYSTEM_START
- SERVICE_AUTO_START
- SERVICE_DEMAND_START

Ejemplo
El siguiente ejemplo establece el tipo de inicio para el servicio Registro de sucesos como Automático o SERVICE_AUTO_START:
enable eventlog service_auto_start

Notas
- Si no designa un tipo de inicio, el comando enable muestra el tipo de inicio actual para el servicio o el controlador de dispositivo que especificó en nombreDeServicio.

• Cuando utilice el comando enable para cambiar un tipo de inicio, el nombre del tipo de inicio anterior aparecerá en la pantalla. Debe anotar este nombre por si tiene que restaurar el tipo de inicio a su configuración anterior.

Exit
Cierra la Consola de recuperación y reinicia el equipo. El comando exit está disponible cuando utiliza la Consola de recuperación.

exit
Parámetros: ninguno

Expand
Extrae un archivo de un archivo comprimido. Utilice este comando para extraer un archivo de controlador de un archivo contenedor (.cab) o un archivo comprimido.

El comando expand con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando expand con distintos parámetros está disponible desde el símbolo del sistema.

expand origen [/F:especificaciónDeArchivo}] [destino] [/d] [/y]

Parámetros:

origen
Especifica el archivo que se va a expandir. Utilice este atributo si el archivo de origen sólo contiene un archivo. Origen puede constar de una letra de unidad y un signo de dos puntos, un nombre de directorio, un nombre de archivo o una combinación de ellos. No puede utilizar caracteres comodín.

/f:especificaciónDeArchivo
Si el origen contiene más de un archivo, especifica el nombre del archivo que desea extraer. Puede utilizar caracteres comodín para los archivos que desea extraer.

destino
Especifica el directorio de destino y el nombre de archivo para el archivo extraído, o cada uno por separado.

/d
Muestra una lista de los archivos incluidos en el archivo contenedor sin expandirlo y sin extraer dichos archivos del mismo.

/y
Suprime la pregunta de si desea sobrescribir archivos cuando expande o extrae archivos.

Ejemplos

El siguiente ejemplo extrae el archivo Msgame.sys del archivo contenedor Drivers de un CD de instalación y lo copia a C:\Windows\System\Drivers:
expand d:\i386\driver.cab /f:msgame.sys c:\Windows\system\drivers

El siguiente ejemplo expande el archivo comprimido Access.cp_:
expand d:\i386\acces.cp_ c:\Windows\system32\access.cpl

El siguiente ejemplo enumera todos los archivos incluidos en el archivo contenedor Drivers del CD de instalación:
expand /d d:\i386\driver.cab

Importante
• *El archivo contenedor Driver, que alberga la mayoría de los controladores suministrados por Windows, incluye miles de archivos. El proceso de expansión de todos los archivos desde este archivo contenedor al disco duro tardará algunos minutos y ocupará mucho espacio en disco. Se recomienda que de este archivo sólo extraiga el archivo que necesite.*

Notas
• Si no se ha especificado el destino, el archivo se copiará al directorio actual.
• No puede especificar como destino un medio extraíble, por ejemplo una unidad de disco o un CD-ROM.

Fixboot

Escribe un nuevo sector de inicio de partición en la partición del sistema. El comando fixboot sólo está disponible cuando se utiliza la Consola de recuperación.
fixboot [unidad]

Parámetro

unidad
La unidad en la que se escribirá un sector de inicio. Reemplaza la unidad predeterminada, que es la partición del sistema en la que ha iniciado la sesión. A continuación se muestra un ejemplo de unidad:
D:

Ejemplo
El siguiente ejemplo escribe un nuevo sector de inicio de partición en la partición del sistema de la unidad D:
fixboot d:

Nota
• Si utiliza el comando fixboot sin ningún parámetro, se escribirá un nuevo sector de inicio de partición en la partición del sistema en la que inició la sesión.

Fixmbr

Repara el registro de inicio maestro del disco de inicio. El comando fixmbr sólo está disponible cuando se utiliza la Consola de recuperacion.

fixmbr [nombreDeDispositivo]

Parámetro

nombreDeDispositivo
El dispositivo (unidad) en el que se desea escribir un nuevo registro de inicio maestro. El nombre se puede obtener del resultado del comando map. He aquí un ejemplo de un nombre de dispositivo:
\Device\HardDisk0.

Ejemplo
El siguiente ejemplo escribe un nuevo registro de inicio maestro en el dispositivo especificado:
fixmbr \Device\HardDisk0

Notas
- Si no especifica un nombreDeDispositivo, se escribirá un nuevo registro de inicio maestro en el dispositivo de inicio, que es la unidad en la que se carga el sistema principal.
- Si se detecta una firma de tabla de particiones no estándar o no válida, el sistema le preguntará si desea seguir. Si no tiene problemas de acceso a las unidades, no debe continuar. Si escribe un registro de inicio maestro en la partición del sistema, podría dañar las tablas de particiones e imposibilitar el acceso a las particiones.

Format

Formatea la unidad especificada con el sistema de archivos especificado. El comando format con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando format con distintos parámetros está disponible desde el símbolo del sistema.

format [unidad:] [/q] [/fs:sistemaDeArchivos]

Parámetros

unidad:

Especifica la unidad que desea formatear. No puede formatear un disquete desde la Consola de recuperación.

/q

Realiza un formateo rápido de la unidad. No se comprueba si existen zonas dañadas en la unidad, por lo que sólo debe utilizar este parámetro en aquellas unidades que haya formateado previamente.

/fs:sistemaDeArchivos

Especifica el sistema de archivos que se va a utilizar: FAT, FAT32 o NTFS. Si no especifica ningún sistema de archivos, se utilizará el formato del sistema de archivos existente.

Help

Proporciona información en pantalla acerca de los comandos de la Consola de recuperación.

help [nombreDeComando]

Parámetro: ninguno

Enumera los comandos disponibles en la Consola de recuperación.

nombreDeComando

Proporciona información acerca del comando, incluidos los parámetros que puede utilizar con el comando.

Nota
- Existen dos maneras de obtener Ayuda en pantalla acerca de un comando. Puede especificar el nombre del comando a continuación del comando help o puede escribir el nombre del comando seguido del modificador /? en el símbolo del sistema. Por ejemplo, puede escribir cualquiera de los comandos siguientes para obtener información acerca del comando extract:

help extract
extract /?

Listsvc

Enumera los servicios y los controladores disponibles en el equipo. El comando listsvc sólo está disponible cuando se utiliza la Consola de recuperación.

listsvc

Parámetros: Ninguno

Logon

Inicia una sesión en una instalación de Windows. El comando logon sólo está disponible cuando se utiliza la Consola de recuperación.

logon

Parámetros: Ninguno

Notas

- El comando logon enumerará todas las instalaciones detectadas de Windows y solicitará la contraseña del administrador local de dicha instalación para iniciar la sesión.
- Después de tres intentos fallidos de inicio de sesión se cerrará la Consola de recuperación y se reiniciará el equipo.

Map

Muestra la asignación de letras de unidad a nombres de dispositivos físicos. Esta información es útil cuando ejecuta los comandos fixboot y fixmbr. El comando map sólo está disponible cuando se utiliza la Consola de recuperación.

Map [arc]

Parámetro

arc

Indica al comando map que muestre nombres de dispositivo Informática avanzada de RISC (ARC) en lugar de los nombres de dispositivo. A continuación se muestra un ejemplo de nombre de dispositivo ARC:

multi(0)disk(0)rdisk(0)partition(1)

El nombre de dispositivo equivalente es:

\Device\HardDisk0\Partition1

Ejemplo

El siguiente ejemplo asigna los nombres de dispositivo físico a las letras de unidad utilizando nombres de dispositivo ARC:

map arc

Notas

- Si no utiliza el parámetro arc, el comando map muestra los nombres de dispositivo de Windows.
- El comando map muestra también el tipo de sistema de archivos y el tamaño de cada disco en megabytes (MB).

Mkdir (Md)

Crea un directorio o un subdirectorio. El comando mkdir con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando mkdir con distintos parámetros está disponible desde el símbolo del sistema.

mkdir [unidad:]rutaDeAcceso

o bien

md [unidad:]rutaDeAcceso

Parámetros

unidad:
Especifica la unidad en la que desea crear el nuevo directorio.

rutaDeAcceso
Especifica el nombre y la ubicación del nuevo directorio. No puede utilizar caracteres comodín.

Nota
• Mkdir funciona únicamente dentro de los directorios del sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición de disco duro o en los orígenes de la instalación local.

More
Presenta el contenido de un archivo de texto. Utilice el comando more o type para examinar un archivo de texto sin modificarlo. El comando more con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando more con distintos parámetros está disponible desde el símbolo del sistema.

more [unidad:][rutaDeAcceso] nombreDeArchivo
o bien
type [unidad:][rutaDeAcceso] nombreDeArchivo

Parámetro

[unidad:][rutaDeAcceso] nombreDeArchivo
Especifica la ubicación y el nombre del archivo que desea examinar.
Si utiliza una unidad NTFS y el nombre de archivo contiene espacios en blanco, deberá escribir el nombre de archivo entre comillas (").

Net use
Conecta un recurso compartido de red a una letra de unidad. El comando net use con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando net use con distintos parámetros está disponible desde el símbolo del sistema.

Sintaxis
net use [\\nombreDeEquipo\nombreDeRecursoCompartido [/user:[nombreDeDominio\] nombreDeUsuario] contraseña] | [letraDeUnidad:] [/d]

Parámetros

\\nombreDeEquipo\nombreDeRecursoCompartido
Especifica el nombre del servidor y del recurso compartido. Si nombreDeEquipo contiene caracteres en blanco, escriba entre comillas el nombre completo del equipo, desde las dos barras diagonales inversas (\\) hasta el final del nombre del equipo. El nombre de equipo puede tener entre 1 y 15 caracteres.

/user:
Especifica el nombre de usuario con el que se realiza la conexión.

nombreDeDominio
Nombre de dominio que debe utilizarse al validar las credenciales del usuario.

NombreDeUsuario
Especifica el nombre de usuario con el que se iniciará la sesión.

Contraseña
Especifica la contraseña necesaria para tener acceso al recurso compartido. Déjela en blanco para que se le pida la contraseña. Los caracteres de la contraseña no se muestran en la pantalla a medida que los escribe.

/d
Indica que esta conexión se va a desconectar.

Rename (Ren)
Cambia el nombre de un archivo. El comando rename con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando rename con distintos parámetros está disponible desde el símbolo del sistema.

rename [unidad:][rutaDeAcceso] nombreDeArchivo1 nombreDeArchivo2
o bien
ren [unidad:][rutaDeAcceso] nombreDeArchivo1 nombreDeArchivo2

Parámetros

[unidad:][rutaDeAcceso] nombreDeArchivo1
Especifica la ubicación y el nombre del archivo cuyo nombre desea cambiar. No puede utilizar caracteres comodín.

nombreDeArchivo2
Especifica el nuevo nombre del archivo. No es posible indicar una unidad o una ruta de acceso nueva cuando se cambia el nombre de archivos.

Rmdir (Rd)
Quita (elimina) un directorio. El comando rmdir con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando rmdir con distintos parámetros está disponible desde el símbolo del sistema.

rmdir [unidad:]rutaDeAcceso
o bien
rd [unidad:]rutaDeAcceso

Parámetros

[unidad:]rutaDeAcceso
Especifica la ubicación y el nombre del directorio que desea eliminar. No puede utilizar caracteres comodín.

Notas
- El directorio debe estar vacío o el comando no se ejecutará correctamente.
- Rmdir funciona únicamente dentro de los directorios del sistema de la instalación actual de Windows, en los medios extraíbles, en el directorio raíz de cualquier partición de disco duro o en los orígenes de la instalación local.

Set
Muestra y establece las variables de entorno de la Consola de recuperación. El comando set es un comando opcional que debe utilizarse con plantillas de seguridad.

El comando set con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando set con distintos parámetros está disponible desde el símbolo del sistema.
set [variable=[cadena]]

Parámetros

variable
Especifica la variable que desea establecer o modificar.

La Consola de recuperación admite las siguientes variables de entorno:

Variable Descripción

AllowWildCards Permite el uso de caracteres comodín con algunos comandos (como el comando del).

AllowAllPaths Permite el acceso a todos los archivos y directorios del sistema.

AllowRemovableMedia Permite copiar archivos a medios extraíbles, como un disco.

NoCopyPrompt No pregunta nada al sobrescribir un archivo existente.

cadena
Especifica la cadena que desea asociar a la variable especificada.

Ejemplos
El siguiente ejemplo le permite utilizar caracteres comodín con algunos comandos de la Consola de recuperación:
set allowwildcards=true

El siguiente ejemplo desactiva la pregunta cuando va a sobrescribir archivos:
set nocopyprompt=true

Notas
- Cuando se utiliza sin parámetros, el comando set muestra las variables de entorno actuales.

- El comando set está deshabilitado de forma predeterminada. Para habilitar el comando set, utilice las plantillas de seguridad. El atributo Habilitar el comando Set para la Consola de recuperación se encuentra en el árbol de la consola, bajo Directiva de equipo local/Configuración del equipo/Configuración de Windows/Configuración de seguridad/Directivas locales/Opciones de seguridad.
- Todas las variables de entorno están establecidas de forma predeterminada como FALSE (Falso).

Systemroot
Establece el directorio actual en la carpeta raiz del sistema de la instalación de Windows en la que inició la sesión. El comando systemroot sólo está disponible cuando se utiliza la Consola de recuperación.

systemroot
Parámetros: Ninguno

Type
Presenta el contenido de un archivo de texto. Utilice el comando type o more para examinar un archivo de texto sin modificarlo. El comando type con los parámetros que se enumeran a continuación sólo está disponible cuando se utiliza la Consola de recuperación. El comando type con distintos parámetros está disponible desde el símbolo del sistema.

type [unidad:][rutaDeAcceso] nombreDeArchivo
o bien
more [unidad:][rutaDeAcceso] nombreDeArchivo

Parámetro

[unidad:][rutaDeAcceso] nombreDeArchivo
Especifica la ubicación y el nombre del archivo que desea examinar. Si utiliza una unidad NTFS y el nombre de archivo contiene espacios en blanco, deberá escribir el nombre de archivo entre comillas.

Implantar políticas de bloqueo de cuentas

Windows XP incluye una funcionalidad de bloqueo de cuentas que desactiva una cuenta después de un número de intentos fallidos de inicio de sesión que fija el administrador. Por ejemplo, se puede indicar que se bloquee la cuenta después de 5 ó 10 intentos fallidos, resetear la cuenta no antes de 30 minutos y dejar la situación de bloqueo a “Siempre” (hasta que el administrador la desbloquee). Si es demasiado agresiva, puede considerar la posibilidad de permitir que la cuenta se desbloquee automáticamente después de un cierto tiempo.

Dos son los objetivos más comunes al utilizar los bloqueos de cuentas: el primero, poner de manifiesto que han tenido lugar un cierto número de intentos de abrir sesión con una cuenta utilizando una password no válida. El segundo, proteger las cuentas de usuario ante la posibilidad de intentar abrir sesión mediante ataques con diccionarios de claves o identificación reiterativa. No hay una receta que sea válida para todos los entornos. Considere los valores que más se ajusten a su entorno particular.

Instalar software antivirus y actualizarlo adecuadamente Una de las iniciativas más importantes a la hora de proteger sistemas informáticos es utilizar software antivirus, y asegurarse de que está correctamente actualizado. Todos los sistemas en Internet, en una intranet corporativa o en una red doméstica deberían llevar instalado software antivirus.

Mantenerse al día con las últimas actualizaciones de seguridad

La función de Actualización Automática en Windows XP puede detectar automáticamente y descargar los parches de seguridad más recientes desde Microsoft. La función de Actualización Automática te se puede configurar para descargar automáticamente los parches en tareas de segundo plano y pedir permiso al usuario para instalarlos cuando se ha completado la descarga.

Para configurar la Actualización Automática, haga clic en Sistema, dentro del Panel de Control, y seleccione la solapa Actualizaciones Automáticas. Elija la opción de notificación previa para descargar las actualizaciones automáticamente y recibirá notificación cuando estén listas para ser instaladas.

Aparte esto, Microsoft publica boletines de seguridad mediante su Servicio de Notificación de Seguridad. Estos boletines se publican para cualquier producto de Microsoft en el cual se haya

encontrado algún problema de seguridad. Cuando estos boletines recomiendan la instalación de algún parche de seguridad, Vd. Debería descargarlo a la mayor brevedad e instalarlo en sus ordenadores.

ESTUDIO DE LOS VIRUS INFORMATICOS PARTE 1

Nuevo escenario

Uno de los cambios más sorprendentes del mundo de hoy es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de conocimientos sea independiente del lugar físico en que nos encontremos. Ya no nos sorprende la transferencia de información en tiempo real o instantáneo. Se dice que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizan el comercio en forma electrónica, para ser más eficientes. Pero al unirse en forma pública, se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.
El escenario electrónico actual es que las organizaciones están uniendo sus redes internas a la Internet, la que crece a razón de más de un 10% mensual.

Al unir una red a la Internet se tiene acceso a las redes de otras organizaciones también unidas. De la misma forma en que accedemos la oficina del frente de nuestra empresa, se puede recibir información de un servidor en Australia, conectarnos a una supercomputadora en Washington o revisar la literatura disponible desde Alemania. Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que puede haber más de una persona con perversas intenciones respecto de una organización. Por eso, se debe tener nuestra red protegida adecuadamente.

Cada vez es más frecuente encontrar noticias referentes a que redes de importantes organizaciones han sido violadas por criminales informáticos desconocidos. A pesar de que la prensa ha publicitado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. A diario se reciben reportes los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada, y miles de contraseñas han sido capturadas a usuarios inocentes.

Los administradores de sistemas deben gastar horas y a veces días enteros volviendo a cargar o reconfigurando sistemas comprometidos, con el objeto de recuperar la confianza en la integridad del sistema. No hay manera de saber los motivos que tuvo el intruso, y debe suponerse que sus intenciones son lo peor. Aquella gente que irrumpe en los sistemas sin autorización, aunque sea solamente para mirar su estructura, causa mucho daño, incluso sin que hubieran leído la correspondencia confidencial y sin borrar ningún archivo.

De acuerdo a un estudio de la Consultora “Ernst and Young” abarcando más de mil empresas, un 20% reporta pérdidas financieras como consecuencia de intrusiones en sus computadoras. Ya pasaron los tiempos en que la seguridad de las computadoras era sólo un juego o diversión.

¿Cómo nacieron los virus?

Hacia finales de los años 60, Douglas McIlory, Victor Vysottsky y Robert Morris idearon un juego al

que llamaron Core War (Guerra en lo Central, aludiendo a la memoria de la computadora), que se convirtió en el pasatiempo de algunos de los programadores de los laboratorios Bell de AT&T.

El juego consistía en que dos jugadores escribieran cada uno un programa llamado organismo, cuyo hábitat fuera la memoria de la computadora. A partir de una señal, cada programa intentaba forzar al otro a efectuar una instrucción inválida, ganando el primero que lo consiguiera.

Al término del juego, se borraba de la memoria todo rastro de la batalla, ya que estas actividades eran severamente sancionadas por los jefes por ser un gran riesgo dejar un organismo suelto que pudiera acabar con las aplicaciones del día siguiente. De esta manera surgieron los programas destinados a dañar en la escena de la computación.

Uno de los primeros registros que se tienen de una infección data del año 1987, cuando en la Universidad estadounidense de Delaware notaron que tenían un virus porque comenzaron a ver © Brain como etiqueta de los disquetes.

La causa de ello era Brain Computer Services, una casa de computación paquistaní que, desde 1986, vendía copias ilegales de software comercial infectadas para, según los responsables de la firma, dar una lección a los piratas.

Ellos habían notado que el sector de booteo de un disquete contenía código ejecutable, y que dicho código se ejecutaba cada vez que la máquina se inicializaba desde un disquete.

Lograron reemplazar ese código por su propio programa, residente, y que este instalara una réplica de sí mismo en cada disquete que fuera utilizado de ahí en más.

También en 1986, un programador llamado Ralf Burger se dio cuenta de que un archivo podía ser creado para copiarse a sí mismo, adosando una copia de él a otros archivos. Escribió una demostración de este efecto a la que llamó VIRDEM, que podía infectar cualquier archivo con extensión .COM.

Esto atrajo tanto interés que se le pidió que escribiera un libro, pero, puesto que él desconocía lo que estaba ocurriendo en Paquistán, no mencionó a los virus de sector de arranque boot sector. Para ese entonces, ya se había empezado a diseminar el virus Vienna.

Actualmente, los virus son producidos en cantidades extraordinarias por muchísima gente alrededor del planeta. Algunos de ellos dicen hacerlo por divertimento, otros quizás para probar sus habilidades. De cualquier manera, hasta se ha llegado a notar un cierto grado de competitividad entre los autores de estos programas.

Con relación a la motivación de los autores de virus para llevar a cabo su obra, existe en Internet un documento escrito por un escritor freelance Markus Salo, en el cual, entre otros, se exponen los siguientes conceptos:

Algunos de los programadores de virus, especialmente los mejores, sostienen que su interés por el tema es puramente científico, que desean averiguar todo lo que se pueda sobre virus y sus usos.

A diferencia de las compañías de software, que son organizaciones relativamente aisladas unas de otras, todas tienen secretos que no querrían que sus competidores averiguaran y cuentan entre sus filas con mayoría de estudiantes graduados, las agrupaciones de programadores de virus están abiertas a cualquiera que se interese en ellas, ofrecen consejos, camaradería y pocas limitaciones. Además, son libres de seguir cualquier objetivo que les parezca, sin temer por la pérdida de respaldo económico.

El hecho de escribir programas vírales da al programador cierta fuerza coercitiva, lo pone fuera de las reglas convencionales de comportamiento. Este factor es uno de los más importantes, pues el sentimiento de pertenencia es algo necesario para todo ser humano, y es probado que dicho sentimiento pareciera verse reforzado en situaciones marginales.

Por otro lado, ciertos programadores parecen intentar legalizar sus actos poniendo sus creaciones al alcance de mucha gente, (vía Internet, BBS especializadas, etc.) haciendo la salvedad de que el material es peligroso, por lo cual el usuario debería tomar las precauciones del caso.

Existen programadores, de los cuales, generalmente, provienen los virus más destructivos, que alegan que sus programas son creados para hacer notoria la falta de protección de que sufren la mayoría de los usuarios de computadoras.

La gran mayoría de estos individuos son del mismo tipo de gente que es reclutada por los grupos terroristas: hombres, adolescentes, inteligentes.

En definitiva, sea cual fuere el motivo por el cual se siguen produciendo virus, se debe destacar que su existencia no ha sido sólo perjuicios: gracias a ellos, mucha gente ha tomado conciencia de qué es lo que tiene y cómo protegerlo.

¿Qué es un virus?

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sector es de booteo y se replica a sí mismo para continuar su esparcimiento.

Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Se ha llegado a un punto tal, que un nuevo virus llamado W95/CIH-10xx. o también como CIH.Spacefiller (puede aparecer el 26 de cada mes, especialmente 26 de Junio y 26 de Abril) ataca al BIOS de la PC huésped y cambiar su configuración de tal forma que se requiere cambiarlo. Nunca se puede asumir que un virus es inofensivo y dejarlo flotando en el sistema.

Existen ciertas analogías entre los virus biológicos y los informáticos: mientras los primeros son agentes externos que invaden células para alterar su información genética y reproducirse, los segundos son programas-rutinas, en un sentido más estricto, capaces de infectar archivos de computadoras, reproduciéndose una y otra vez cuando se accede a dichos archivos, dañando la información existente en la memoria o alguno de los dispositivos de almacenamiento del ordenador.

Tienen diferentes finalidades: Algunos sólo infectan, otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: PROPAGARSE.

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.

La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

- Es dañino
- Es autorreproductor
- Es subrepticio

El hecho de que la definición imponga que los virus son programas no admite ningún tipo de observación; está extremadamente claro que son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas.

Asimismo, se pueden distinguir tres módulos principales de un virus informático:
- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

El módulo de reproducción se encarga de manejar las rutinas de parasitación de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

El módulo de ataque es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus Michelangelo, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

El módulo de defensa tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

Tipos de virus.

Los virus se clasifican por el modo en que actúan infectando la computadora:

Programa: Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin
Boot: Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.
Múltiples: Infectan programas y sectores de "booteo".
Bios: Atacan al Bios para desde allí reescribir los discos duros.
Hoax: Se distribuyen por e-mail y la única forma de eliminarlos es el uso del sentido común.

Al respecto, se trata de virus que no existe y que se utiliza para aterrar a los novatos especialmente en la Internet a pesar que los rumores lo muestran como algo muy serio y a veces la información es tomada por la prensa especializada.

Por lo general, como ya se expresó, la difusión se hace por cadenas de e-mail con terribles e inopinadas advertencias. En realidad el único virus es el mensaje. A continuación se dan una serie de supuestos "virus", por lo que es aconsejable ignorar los mensajes que aparecen y no ayudar a replicarlos continuando con la cadena:
- 3b Trojan (alias PKZIP Virus).
- AOL4Free Virus Hoax.
- Baby New Year Virus Hoax.
- BUDDYLST.ZIP
- BUDSAVER.EXE
- Budweiser Hoax
- Death69
- Deeyenda
- E-Flu
- FatCat Virus Hoax

- Free Money
- Get More Money Hoax
- Ghost
- Good Times
- Hacky Birthday Virus Hoax
- Hairy Palms Virus Hoax
- Irina
- Join the Crew
- Londhouse Virus Hoax
- Microsoft Virus Hoax
- Millenium Time Bomb
- Penpal Greetings
- Red Alert
- Returned or Unable to Deliver
- Teletubbies
- Time Bomb
- Very Cool
- Win a Holiday
- World Domination Hoax
- Yellow Teletubbies
- A.I.D.S. hoax email virus
- AltaVista virus scare
- AOL riot hoax email
- ASP virus hoax
- Back Orifice Trojan horse
- Bill Gates hoax
- Bloat, see MPEG virus hoax
- Budweiser frogs screen-saver scare
- Good Times hoax email virus
- Irina hoax virus
- Java virus scare
- Join the Crew hoax email virus
- 'Millennium' virus misunderstanding
- MPEG virus hoax
- 'My clock says 2097/2098' virus misunderstanding
- New virus debug device hoax email virus with attached Trojan horse
- Open: Very Cool, see A.I.D.S. hoax email virus
- Penpal Greetings, see Good Times hoax email virus
- PKZ300 Trojan virus scare
- Returned or Unable to Deliver hoax email virus
- Walt Disney greeting, see Bill Gates hoax
- Win a Holiday hoax email virus
- Windows '98 MS Warning.

Por último, cabe destacar que los HOAX están diseñados únicamente para asustar a los novatos (y a los que no lo son tanto). Otros como el mensaje del carcinoma cerebral de Jessica, Jessica Mydek , Anabelle , Ana , Billy y otros personajes imaginarios tampoco son reales como tampoco lo es la dirección ACS@aol.com , ya que fueron creados para producir congestionamiento en la Internet.

Características de los virus.

El virus es un pequeño software (cuanto más pequeño más fácil de esparcir y más difícil de detectar), que permanece inactivo hasta que un hecho externo hace que el programa sea ejecutado o el sector de "booteo" sea leído. De esa forma el programa del virus es activado y se carga en la memoria de la computadora, desde donde puede esperar un evento que dispare su sistema de destrucción o se replique a sí mismo.

Los más comunes son los residentes en la memoria que pueden replicarse fácilmente en los programas del sector de "booteo", menos comunes son los no-residentes que no permanecen en la memoria después que el programa-huesped es cerrado. Los virus pueden llegar a camuflarse y esconderse para evitar la detección y reparación. Como lo hacen:

El virus re-orienta la lectura del disco para evitar ser detectado.

Los datos sobre el tamaño del directorio infectado son modificados en la FAT, para evitar que se descubran bytes extra que aporta el virus.

Encriptamiento: el virus se encripta en símbolos sin sentido para no ser detectado, pero para destruir o replicarse DEBE desencriptarse siendo entonces detectable;
Polimorfismo: mutan cambiando segmentos del código para parecer distintos en cada nueva generación, lo que los hace muy difíciles de detectar y destruir.
Gatillables: se relaciona con un evento que puede ser el cambio de fecha, una determinada combinación de tecleo; un macro o la apertura de un programa asociado al virus (Troyanos).

Los virus se transportan a través de programas tomados de BBS (Bulletin Boards) o copias de software no original, infectadas a propósito o accidentalmente. También cualquier archivo que contenga ejecutables o macros puede ser portador de un virus: Descaregas de programas de lugares inseguros; e-mail con attachments, archivos de MS-Word y MS-Excel con macros. Inclusive ya existen virus que se distribuyen con MS-Power Point. Los archivos de datos, texto o html NO PUEDEN contener virus, aunque pueden ser dañados por estos.

Los virus de sectores de booteo se instalan en esos sectores y desde allí van saltando a los sectores equivalentes de cada uno de los drivers de la PC. Pueden dañar el sector o sobrescribirlo. Lamentablemente obligan al formateo del disco del drive infectado. Incluyendo discos de 3.5" y todos los tipos de Zip de Iomega, Sony y 3M. (No crean vamos a caer en el chiste fácil de decir que el más extendido de los virus de este tipo se llama MS Windows 98).

En cambio los virus de programa, se manifiestan cuando la aplicación infectada es ejecutada, el virus se activa y se carga en la memoria, infectando a cualquier programa que se ejecute a continuación. Puede solaparse infecciones de diversos virus que pueden ser destructivos o permanecer inactivos por largos periodos de tiempo.

Daños de los virus.

Definiremos daño como acción una indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños. Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

Daños triviales.

Sirva como ejemplo la forma de trabajo del virus FORM (el más común): En el día 18 de cada mes cualquier tecla que presionemos hace sonar el beep. Deshacerse del virus implica, generalmente, segundos o minutos.

Daños menores.

Un buen ejemplo de este tipo de daño es el JERUSALEM. Este virus borra, los viernes 13, todos los programas que uno trate de usar después de que el virus haya infectado la memoria residente. En el peor de los casos, tendremos que reinstalar los programas perdidos. Esto nos llevará alrededor de 30 minutos.

Daños moderados.

Cuando un virus formatea el disco rígido, mezcla los componentes de la FAT (File Allocation Table, Tabla de Ubicación de Archivos), o sobrescribe el disco rígido. En este caso, sabremos inmediatamente qué es lo que está sucediendo, y podremos reinstalar el sistema operativo y utilizar el último backup. Esto quizás nos lleve una hora.

Daños mayores.

Algunos virus, dada su lenta velocidad de infección y su alta capacidad de pasar desapercibidos, pueden lograr que ni aún restaurando un backup volvamos al último estado de los datos. Un ejemplo de esto es el virus DARK AVENGER, que infecta archivos y acumula la cantidad de infecciones que realizó. Cuando este contador llega a 16, elige un sector del disco al azar y en él escribe la frase: Eddie lives somewhere in time (Eddie vive en algún lugar del tiempo).

Esto puede haber estado pasando por un largo tiempo sin que lo notemos, pero el día en que detectemos la presencia del virus y queramos restaurar el último backup notaremos que también él contiene sectores con la frase, y también los backups anteriores a ese.

Puede que lleguemos a encontrar un backup limpio, pero será tan viejo que muy probablemente hayamos perdido una gran cantidad de archivos que fueron creados con posterioridad a ese backup.

Daños severos.

Los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No sabemos cuándo los datos son correctos o han cambiado, pues no hay pistas obvias como en el caso del DARK AVENGER (es decir, no podemos buscar la frase Eddie lives...).

Daños limitados.

Algunos programas como CHEEBA, VACSINA.44.LOGIN y GP1 entre otros, obtienen la clave del administrador del sistema y la pasan a un tercero. Cabe aclarar que estos no son virus sino troyanos. En el caso de CHEEBA, crea un nuevo usuario con los privilegios máximos, fijando el nombre del usuario y la clave. El daño es entonces realizado por la tercera persona, quien ingresará al sistema y haría lo que quisiera.

SÍNTOMAS TÍPICOS DE UNA INFECCIÓN.

- El sistema operativo o un programa toma mucho tiempo en cargar sin razón aparente.
- El tamaño del programa cambia sin razón aparente.
- El disco duro se queda sin espacio o reporta falta de espacio sin que esto sea necesariamente así.
- Si se corre el CHKDSK no muestra "655360 bytes available".
- En Windows aparece "32 bit error".

- La luz del disco duro en la CPU continua parpadeando aunque no se este trabajando ni haya protectores de pantalla activados. (Se debe tomar este síntoma con mucho cuidado, porque no siempre es así).
- No se puede "bootear" desde el Drive A, ni siquiera con los discos de rescate. Aparecen archivos de la nada o con nombres y extensiones extrañas.
- Suena "clicks" en el teclado (este sonido es particularmente aterrador para quien no esta advertido).
- Los caracteres de texto se caen literalmente a la parte inferior de la pantalla (especialmente en DOS).
- En la pantalla del monitor pueden aparecen mensajes absurdos tales como "Tengo hambre. Introduce un Big Mac en el Drive A".
- En el monitor aparece una pantalla con un fondo de cielo celeste, unas nubes blancas difuminadas, una ventana de vidrios repartidos de colores y una leyenda en negro que dice Windows '98 (No puedo evitarlo, es mas fuerte que yo...!!).

Una infección se soluciona con las llamadas "vacunas" (que impiden la infección) o con los remedios que desactivan y eliminan, (o tratan de hacerlo) a los virus de los archivos infectados. Hay cierto tipo de virus que no son desactivables ni removibles, por lo que se debe destruir el archivo infectado.

VIRUS INFORMÁTICOS ARGENTINOS.

Al igual que todos los países informatizados, la Argentina cuenta con una producción local de virus informáticos.

Si bien estos no son de los más complejos (en su mayoría, buenas copias y variaciones de virus conocidos) representan un problema, ya que muchos de ellos no están incluidos en las bases de datos de los programas antivirus.

Veamos algunos ejemplos:

PING PONG:
Este virus fue el primero en hacer explosión en Argentina. Fue descubierto en marzo de 1988 y en poco tiempo estuvo en nuestro país, en donde se convirtió rápidamente en epidemia.

La falta de conocimiento sobre los virus ayudó a que se diseminara ampliamente y fuera incontrolable en un principio. En centros universitarios como la Facultad de Ciencias Exactas de la UBA o la Facultad de Informática de la Universidad de Morón era difícil encontrar un disco sin infectar.

Ese mismo desconocimiento llevó a que pasara bastante tiempo hasta que se empezaran a tomar medidas. Sólo después de algunos meses, en revistas especializadas en informática, empezaron a publicarse formas de desinfectar los discos, y como consecuencia de ello se aplicaron políticas de seguridad en las universidades.

Lo positivo de esto fue que la gente comenzara a conocer el D.O.S. más profundamente, por ejemplo el boot sector: qué es y para qué sirve, ya que las máquinas eran utilizadas pero pocos sabían cómo funcionaban realmente.

Como tenía un síntoma muy evidente (una pelotita que rebotaba), se pensó que todos los virus debían ser visibles, pero los siguientes fueron más subrepticios, y se limitaban a reproducirse o destruir sin avisar al usuario.

El Ping Pong original no podía infectar discos rígidos, pero la versión que se popularizó en el país fue la B, que sí podía hacerlo. Se creó una variante en Argentina, que probablemente fue la primera variante de virus originada en el país, el Ping Pong C, que no mostraba la pelotita en la pantalla. Este virus está extinto en este momento ya que sólo podía funcionar en máquinas con procesador 8088 ó 8086, porque ejecutaba una instrucción no documentada en estos e incorrecta en los modelos siguientes.

AVISPA:
Escrito en Noviembre de 1993 que en muy poco tiempo se convirtió en epidemia. Infecta archivos .EXE

Al ejecutarse, si no se encontraba ya residente en memoria, intenta infectar los archivos XCOPY, MEM, SETVER y EMM386 para maximizar sus posibilidades de reproducción, ya que estos archivos son de los más frecuentemente utilizados.

Este virus está encriptado siempre con una clave distinta (polimórfico), para dificultar su detección por medio de antivirus heurísticos.

MENEM TOCOTO:
Esta adaptación del virus Michelangelo apareció en 1994. En los disquetes se aloja en el boot sector, y en los discos rígidos en la tabla de particiones. Es extremadamente sencillo y, por ende, fácil de detectar.

ESTUDIO SOBRE VIRUS INFORMATICOS PARTE 2

Seguridad en Windows

CAMOUFLAGE II: Aparecido por primera vez en 1993. Infecta el boot sector de los disquetes ubicados en la unidad A y la tabla de partición de los discos rígidos. Es bastante simple y fácil de ser detectado.

LEPROSO: Creado en 1993, en Rosario, provincia de Santa Fé. Se activa el día 12 de Enero (cumpleaños del autor), y hace aparecer un mensaje que dice: Felicitaciones, su máquina está infectada por el virus leproso creado por J. P.. Hoy es mi cumpleaños y lo voy a festejar formateando su rígido. Bye... (Vamos Newell's que con Diego somos campeones).

PINDONGA: Virus polimórfico residente en memoria que se activa los días 25 de febrero, 21 de marzo, 27 de agosto y 16 de septiembre, cuando ataca, borra toda la información contenida en el disco rígido.

TEDY: Es el primer virus argentino interactivo. Apareció hace poco tiempo. Infecta archivos con extensión .EXE, y se caracteriza por hacer una serie de preguntas al usuario. Una vez activado, una pantalla muestra: ¡TEDY, el primer virus interactivo de la computación!

¿QUÉ NO ES UN VIRUS?

Existen algunos programas que, sin llegar a ser virus, ocasionan problemas al usuario.

Estos no-virus carecen de por lo menos una de las tres características identificatorias de un virus (dañino, autorreproductor y subrepticio).

Veamos un ejemplo de estos no - virus: Hace algunos años, la red de I. B. M., encargada de conectar más de 130 países, fue virtualmente paralizada por haberse saturado con un correo electrónico que contenía un mensaje de salutación navideña que, una vez leído por el destinatario, se enviaba a sí mismo a cada integrante de las listas de distribución de correo del usuario. Al cabo de un tiempo, fueron tantos los mensajes que esperaban ser leídos por sus destinatarios que el tráfico se volvió demasiado alto, lo que ocasionó la caída de la red.

Asimismo, es necesario aclarar que no todo lo que altere el normal funcionamiento de una computadora es necesariamente un virus.

Por ello, daré algunas de las pautas principales para diferenciar entre qué debe preocuparnos y qué no:

BUGS (Errores en programas).

Los bugs no son virus, y los virus no son bugs. Todos usamos programas que tienen graves errores (bugs). Si se trabaja por un tiempo largo con un archivo muy extenso, eventualmente algo puede comenzar a ir mal dentro del programa, y este a negarse a grabar el archivo en el disco. Se pierde entonces todo lo hecho desde la última grabación. Esto, en muchos casos, se debe a ERRORES del programa. Todos los programas lo suficientemente complejos tienen bugs.

Falsa alarma.

Algunas veces tenemos problemas con nuestro hardware o software y, luego de una serie de verificaciones, llegamos a la conclusión de que se trata de un virus, pero nos encontramos con una falsa alarma luego de correr nuestro programa antivirus.

Desafortunadamente no hay una regla estricta por la cual guiarse, pero contestarse las siguientes preguntas puede ser de ayuda:

¿Es sólo un archivo el que reporta la falsa alarma? o quizás varios, pero copias del mismo.

¿Solamente un producto antivirus reporta la alarma? Otros productos dicen que el sistema está limpio.

Se indica una falsa alarma después de correr múltiples productos, pero no después de bootear, sin ejecutar ningún programa.

Si al menos una de nuestras respuestas fue afirmativa, es muy factible que efectivamente se trate de una falsa alarma.

Programas corruptos.

A veces algunos archivos son accidentalmente dañados, quizás por problemas de hardware. Esto quiere decir que no siempre que encontremos daños en archivos deberemos estar seguros de estar infectados.

¿Que es un antivirus?

No para toda enfermedad existe cura, como tampoco existe una forma de erradicar todos y cada uno de los virus existentes.

Es importante aclarar que todo antivirus es un programa y que, como todo programa, sólo funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una

herramienta para el usuario y no sólo no será eficaz para el 100% de los casos, sino que nunca será una protección total ni definitiva.

La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Este es el aspecto más importante de un antivirus, independientemente de las prestaciones adicionales que pueda ofrecer, puesto que el hecho de detectar la posible presencia de un virus informático, detener el trabajo y tomar las medidas necesarias, es suficiente para acotar un buen porcentaje de los daños posibles. Adicionalmente, un antivirus puede dar la opción de erradicar un virus informático de una entidad infectada.

El modelo más primario de las funciones de un programa antivirus es la detección de su presencia y, en lo posible, su identificación. La primera técnica que se popularizó para la detección de virus informáticos, y que todavía se sigue utilizando (aunque cada vez con menos eficiencia), es la técnica de scanning. Esta técnica consiste en revisar el código de todos los archivos contenidos en la unidad de almacenamiento -fundamentalmente los archivos ejecutables- en busca de pequeñas porciones de código que puedan pertenecer a un virus informático. Este procedimiento, denominado escaneo, se realiza a partir de una base de datos que contiene trozos de código representativos de cada virus conocido, agregando el empleo de determinados algoritmos que agilizan los procesos de búsqueda.

La técnica de scanning fue bastante eficaz en los primeros tiempos de los virus informáticos, cuando había pocos y su producción era pequeña. Este relativamente pequeño volumen de virus informáticos permitía que los desarrolladores de antivirus escaneadores tuvieran tiempo de analizar el virus, extraer el pequeño trozo de código que lo iba a identificar y agregarlo a la base de datos del programa para lanzar una nueva versión. Sin embargo, la obsolescencia de este mecanismo de identificación como una solución antivirus completa se encontró en su mismo modelo.

El primer punto grave de este sistema radica en que siempre brinda una solución a posteriori : es necesario que un virus informático alcance un grado de dispersión considerable para que sea enviado (por usuarios capacitados, especialistas o distribuidores del producto) a los desarrolladores de antivirus. Estos lo analizarán, extraerán el trozo de código que lo identificará, y lo incluirán en la próxima versión de su programa antivirus. Este proceso puede demorar meses a partir del momento en que el virus comienza a tener una dispersión considerable, lapso en el cual puede causar graves daños sin que pueda ser identificado.

Además, este modelo consiste en una sucesión infinita de soluciones parciales y momentáneas (cuya sumatoria jamás constituirá una solución definitiva), que deben actualizarse periódicamente debido a la aparición de nuevos virus.

En síntesis, la técnica de scanning es altamente ineficiente, pero se sigue utilizando debido a que permite identificar rápidamente la presencia de los virus más conocidos y, como son estos los de mayor dispersión, permite una importante gama de posibilidades. Un ejemplo típico de un antivirus de esta clase es el Viruscan de McAfee, que se verá más adelante.

En virtud del pronto agotamiento técnico de la técnica de scanning, los desarrolladores de programas antivirus han dotado a sus creaciones de métodos para búsquedas de virus informáticos (y de sus actividades), que no identifican específicamente al virus sino a algunas de sus características generales y comportamientos universalizados.

Este tipo de método rastrea rutinas de alteración de información que no puedan ser controladas por el usuario, modificación de sectores críticos de las unidades de almacenamiento (master boot record, boot sector, FAT, entre otras), etc.

Un ejemplo de este tipo de métodos es el que utiliza algoritmos heurísticos.

De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, códigos de instrucciones potencialmente pertenecientes a un virus informático. Resulta eficaz para la detección de virus conocidos y es una de las soluciones utilizadas por los antivirus para la detección de nuevos virus. El inconveniente que presenta este tipo de algoritmo radica en que puede llegar a sospecharse de muchísimas cosas que no son virus. Esto hace necesario que el usuario que lo utiliza conozca un poco acerca de la estructura del sistema operativo, a fin de poseer herramientas que le faciliten una discriminación de cualquier falsa alarma generada por un método heurístico.

Algunos de los antivirus de esta clase son F-Prot, Norton Anti Virus y Dr. Solomon's Toolkit.

Ahora bien, otra forma de detectar la presencia de un virus informático en un sistema consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar los sectores críticos de los dispositivos de almacenamiento o los archivos ejecutables. Los programas que realizan esta tarea se denominan chequeadores de integridad.

Sobre la base de estas consideraciones, podemos consignar que un buen sistema antivirus debe estar compuesto por un programa detector de virus -que siempre esté residente en memoria- y un programa que verifique la integridad de los sectores críticos del disco rígido y sus archivos ejecutables. Existen productos antivirus que cubren los dos aspectos, o bien pueden combinarse productos diferentes configurados de forma que no se produzcan conflictos entre ellos.

Modelo antivirus:

La estructura de un programa antivirus, está compuesta por dos módulos principales: el primero denominado de control y el segundo denominado de respuesta. A su vez, cada uno de ellos se divide en varias partes:

Módulo de control: posee la técnica verificación de integridad que posibilita el registro de cambios en los archivos ejecutables y las zonas críticas de un disco rígido. Se trata, en definitiva, de una herramienta preventiva para mantener y controlar los componentes de información de un disco rígido que no son modificados a menos que el usuario lo requiera.

Otra opción dentro de este módulo es la identificación de virus, que incluye diversas técnicas para la detección de virus informáticos. Las formas más comunes de detección son el scanning y los algoritmos, como por ejemplo, los heurísticos.

Asimismo, la identificación de código dañino es otra de las herramientas de detección que, en este caso, busca instrucciones peligrosas incluidas en programas, para la integridad de la información del disco rígido.

Esto implica descompilar (o desensamblar) en forma automática los archivos almacenados y ubicar sentencias o grupos de instrucciones peligrosas.

Finalmente, el módulo de control también posee una administración de recursos para efectuar un monitoreo de las rutinas a través de las cuales se accede al hardware de la computadora (acceso a disco, etc.). De esta manera puede limitarse la acción de un programa restringiéndole el uso de estos recursos, como por ejemplo impedir el acceso a la escritura de zonas críticas del disco o evitar que se ejecuten funciones de formato del mismo.

Módulo de respuesta: la función alarma se encuentra incluida en todos los programas antivirus y consiste en detener la acción del sistema ante la sospecha de la presencia de un virus informático, e informar la situación a través de un aviso en pantalla.

Algunos programas antivirus ofrecen, una vez detectado un virus informático, la posibilidad de erradicarlo. Por consiguiente, la función reparar se utiliza como una solución momentánea para mantener la operatividad del sistema hasta que pueda instrumentarse una solución adecuada. Por otra parte, existen dos técnicas para evitar el contagio de entidades ejecutables: evitar que se contagie todo el programa o prevenir que la infección se expanda más allá de un ámbito fijo.

Aunque la primera opción es la más adecuada, plantea grandes problemas de implementación.

Detección y prevención.

Debido a que los virus informáticos son cada vez más sofisticados, hoy en día es difícil sospechar su presencia a través de síntomas como la pérdida de performance. De todas maneras la siguiente es una lista de síntomas que pueden observarse en una computadora de la que se sospeche esté infectada por alguno de los virus más comunes:

Operaciones de procesamiento más lentas.

Los programas tardan más tiempo en cargarse.

Los programas comienzan a acceder por momentos a las disqueteras y/o al disco rígido.

Disminución no justificada del espacio disponible en el disco rígido y de la memoria RAM disponible, en forma constante o repentina.

Aparición de programas residentes en memoria desconocidos.

La primera medida de prevención a ser tenida en cuenta es, como se dijo anteriormente, contar con un sistema antivirus y utilizarlo correctamente. Por lo tanto, la única forma de que se constituya un bloqueo eficaz para un virus es que se utilice con determinadas normas y procedimientos. Estas normas tienden a controlar la entrada de archivos al disco rígido de la computadora, lo cual se logra revisando con el antivirus todos los disquetes o medios de almacenamiento en general y, por supuesto, disminuyendo al mínimo posible todo tipo de tráfico.

Además de utilizar un sistema antivirus y controlar el tráfico de archivos al disco rígido, una forma bastante eficaz de proteger losarchivos ejecutables es utilizar un programa chequeador de integridad que verifique que estos archivos no sean modificados, es decir, que mantengan su estructura. De esta manera, antes que puedan ser parasitados por un virus convencional, se impediría su accionar.

Para prevenir la infección con un virus de sector de arranque, lo más indicado es no dejar disquetes olvidados en la disquetera de arranque y contar con un antivirus. Pero, además, puede aprovecharse una característica que incorpora el setup de las computadoras más modernas: variar la secuencia de arranque de la PC a primero disco rígido y luego disquetera (C, A). De esta manera, la computadora no intentará leer la disquetera en el arranque aunque tenga cargado un disquete.

Algunos distribuidores o representantes de programas antivirus envían muestras de los nuevos virus argentinos a los desarrolladores del producto para que los estudien o incluyan en sus nuevas versiones o upgrades, con la demora que esto implica.

En consecuencia, la detección alternativa a la de scanning y las de chequeo de actividad e integridad resultan importantes, ya que pueden detectar la presencia de un virus informático sin la necesidad de identificarlo. Y esta es la única forma disponible para el usuario de detectar virus nuevos, sean nacionales o extranjeros.

De todas maneras, existe una forma de actualizar la técnica de scanning. La misma consiste en incorporarle al antivirus un archivo conteniendo cadenas de caracteres ASCII que sean trozos de código (strings) significativos del sector vital de cada nuevo virus que todavía no esté incorporado en la base de datos del programa.

De todas formas, esta solución será parcial: la nueva cadena introducida sólo identificará al virus, pero no será capaz de erradicarlo.

Es muy importante que los strings que se vayan a incorporar al antivirus provengan de una fuente confiable ya que, de lo contrario, pueden producirse falsas alarmas o ser ineficaces.

Algunos de los antivirus que soportan esta cualidad de agregar strings son Viruscan, F-Prot y Thunderbyte.

La NCSA (National Computer Security Association, Asociación Nacional de Seguridad de Computadoras) es la encargada de certificar productos antivirus.

Para obtener dicha certificación los productos deben pasar una serie de rigurosas pruebas diseñadas para asegurar la adecuada protección del usuario.

Antiguamente el esquema de certificación requería que se detectara (incluyendo el número de versión) el 90 % de la librería de virus del NCSA, y fue diseñado para asegurar óptimas capacidades de detección. Pero esta metodología no era completamente eficiente.

Actualmente, el esquema de certificación enfoca la amenaza a las computadoras empresariales. Para ser certificado, el producto debe pasar las siguientes pruebas:

Debe detectar el 100% de los virus encontrados comúnmente. La lista de virus comunes es actualizada periódicamente, a medida que nuevos virus son descubiertos.

Deben detectar, como mínimo, el 90% de la librería de virus del NCSA (más de 6.000 virus). Estas pruebas son realizadas con el producto ejecutándose con su configuración por defecto.

Una vez que un producto ha sido certificado, la NCSA tratará de recertificar el producto un mínimo de cuatro veces. Cada intento es realizado sin previo aviso al desarrollador del programa. Esta es una buena manera de asegurar que el producto satisface el criterio de certificación.

Si un producto no pasa la primera o segunda prueba, su distribuidor tendrá siete días para proveer de la corrección. Si este límite de tiempo es excedido, el producto será eliminado de la lista de productos certificados.

Una vez que se ha retirado la certificación a un producto la única forma de recuperarla es que el distribuidor envíe una nueva versión completa y certificable (no se aceptará sólo una reparación de la falla.

Acerca de la lista de virus de la NCSA, aclaremos que ningún desarrollador de antivirus puede obtener una copia. Cuando un antivirus falla en la detección de algún virus incluido en la lista, una cadena identificatoria del virus le es enviada al productor del antivirus para su inclusión en futuras versiones.

En el caso de los virus polimórficos, se incluyen múltiples copias del virus para asegurar que el producto testeado lo detecta perfectamente. Para pasar esta prueba el antivirus debe detectar cada mutación del virus.

La A. V. P. D. (Antivirus Product Developers, Desarrolladores de Productos Antivirus) es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software
- I. B. M.
- Intel
- McAfee Associates
- ON Tecnology
- Stiller Research Inc.
- S&S Internacional
- Symantec Corp.
- ThunderByte

Algunos antivirus.

DR. SOLOMON'S ANTIVIRUS TOOLKIT.

Certificado por la NCSA. Detecta más de 6.500 virus gracias a su propio lenguaje de detección llamado VirTran, con una velocidad de detección entre 3 y 5 veces mayor que los antivirus tradicionales.

Uno de los últimos desarrollos de S&S es la tecnología G. D. E. (Generic Decription Engine, Motor de Desencriptación Genérica) que permite detectar virus polimórficos sin importar el algoritmo de encriptación utilizado.

Permite detectar modificaciones producidas tanto en archivos como en la tabla de partición del disco rígido. Para ello utiliza Checksumms Criptográficos lo cual, sumado a una clave personal de cada usuario, hace casi imposible que el virus pueda descubrir la clave de encriptación.

Elimina virus en archivos en forma sencilla y efectiva con pocas falsas alarmas, y en sectores de buteo y tablas de partición la protección es genérica, es decir, independiente del virus encontrado.

Otras características que presenta este antivirus, son:

- Ocupa 9K de memoria extendida o expandida.
- Documentación amplia y detallada en español y una enciclopedia sobre los virus más importantes.
- Actualizaciones mensuales o trimestrales de software y manuales.
- Trabaja como residente bajo Windows.
- H. A. (Advanced Heuristic Analysis, Análisis Heurístico Avanzado).

NORTON ANTIVIRUS.

Certificado por la NCSA. Posee una protección automática en segundo plano. Detiene prácticamente todos los virus conocidos y desconocidos (a través de una tecnología propia denominada NOVI, que implica control de las actividades típicas de un virus, protegiendo la integridad del sistema), antes de que causen algún daño o pérdida de información, con una amplia línea de defensa, que combina búsqueda, detección de virus e inoculación (se denomina 'inoculación' al método por el cual este antivirus toma las características principales de los sectores de booteo y archivos para luego chequear su integridad. Cada vez que se detecta un cambio en

dichas áreas, NAV avisa al usuario y provee las opciones de Reparar - Volver a usar la imagen guardada - Continuar - No realiza cambios - Inocular - Actualizar la imagen.

Utiliza diagnósticos propios para prevenir infecciones de sus propios archivos y de archivos comprimidos.

El escaneo puede ser lanzado manualmente o automáticamente a través de la planificación de fecha y hora. También permite reparar los archivos infectados por virus desconocidos. Incluye información sobre muchos de los virus que detecta y permite establecer una contraseña para aumentar así la seguridad.

La lista de virus conocidos puede ser actualizada periódicamente (sin cargo) a través de servicios en línea como Internet, América On Line, Compuserve, The Microsoft Network o el BBS propio de Symantec, entre otros.

VIRUSSCAN.

Este antivirus de McAfee Associates es uno de los más famosos. Trabaja por el sistema de scanning descrito anteriormente, y es el mejor en su estilo.

Para escanear, hace uso de dos técnicas propias: CMS (Code Matrix Scanning, Escaneo de Matriz de Código) y CTS (Code Trace Scanning, Escaneo de Seguimiento de Código).

Una de las principales ventajas de este antivirus es que la actualización de los archivos de bases de datos de strings es muy fácil de realizar, lo cual, sumado a su condición de programa shareware, lo pone al alcance de cualquier usuario. Es bastante flexible en cuanto a la configuración de cómo detectar, reportar y eliminar virus.

CONCLUSIONES.

En razón de lo expresado pueden extraerse algunos conceptos que pueden considerarse necesarios para tener en cuenta en materia de virus informáticos:

No todo lo que afecte el normal funcionamiento de una computadora es un virus.
TODO virus es un programa y, como tal, debe ser ejecutado para activarse.
Es imprescindible contar con herramientas de detección y desinfección.

NINGÚN sistema de seguridad es 100% seguro. Por eso todo usuario de computadoras debería tratar de implementar estrategias de seguridad antivirus, no sólo para proteger su propia información sino para no convertirse en un agente de dispersión de algo que puede producir daños graves e indiscriminados.

Para implementar tales estrategias deberían tenerse a mano los siguientes elementos:

UN DISCO DE SISTEMA PROTEGIDO CONTRA ESCRITURA Y LIBRE DE VIRUS: Un disco que contenga el sistema operativo ejecutable (es decir, que la máquina pueda ser arrancada desde este disco) con protección contra escritura y que contenga, por lo menos, los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes del MS-DOS).

POR LO MENOS UN PROGRAMA ANTIVIRUS ACTUALIZADO: Se puede considerar actualizado a un antivirus que no tiene más de tres meses desde su fecha de creación (o de actualización del archivo de strings). Es muy recomendable tener por lo menos dos antivirus.

UNA FUENTE DE INFORMACIÓN SOBRE VIRUS ESPECÍFICOS: Es decir, algún programa, libro o archivo de texto que contenga la descripción, síntomas y características de por lo menos los cien virus más comunes.

UN PROGRAMA DE RESPALDO DE ÁREAS CRÍTICAS: Algún programa que obtenga respaldo (backup) de los sectores de arranque de los disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos rígidos. Muchos programas antivirus incluyen funciones de este tipo.

LISTA DE LUGARES DÓNDE ACUDIR: Una buena precaución es no esperar a necesitar ayuda para comenzar a buscar quién puede ofrecerla, sino ir elaborando una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y lugares que puedan servirnos más adelante. Si se cuenta con un antivirus comercial o registrado, deberán tenerse siempre a mano los teléfonos de soporte técnico.

UN SISTEMA DE PROTECCIÓN RESIDENTE: Muchos antivirus incluyen programas residentes que previenen (en cierta medida), la intrusión de virus y programas desconocidos a la computadora.

TENER RESPALDOS: Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables. Para archivos muy importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.

REVISAR TODOS LOS DISCOS NUEVOS ANTES DE UTILIZARLOS: Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas originales (pocas veces sucede que se distribuyan discos de programas originales infectados, pero es factible) y los que se distribuyen junto con revistas de computación.

REVISAR TODOS LOS DISCOS QUE SE HAYAN PRESTADO: Cualquier disco que se haya prestado a algún amigo o compañero de trabajo, aún aquellos que sólo contengan archivos de datos, deben ser revisados antes de usarse nuevamente.

REVISAR TODOS LOS PROGRAMAS QUE SE OBTENGAN POR MÓDEM O REDES: Una de las grandes vías de contagio la constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos, pero no siempre se sabe desde dónde se está recibiendo información.

REVISAR PERIÓDICAMENTE LA COMPUTADORA: Se puede considerar que una buena frecuencia de análisis es, por lo menos, mensual.

Finalmente, es importante tener en cuenta estas sugerencias referentes al comportamiento a tener en cuenta frente a diferentes situaciones:

Cuando se va a revisar o desinfectar una computadora, es conveniente apagarla por más de 5 segundos y arrancar desde un disco con sistema, libre de virus y protegido contra escritura, para eliminar virus residentes en memoria. No se deberá ejecutar ningún programa del disco rígido, sino que el antivirus deberá estar en el disquete. De esta manera, existe la posibilidad de detectar virus stealth.

Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema

operativo instalado. Además, los virus no siempre dejan un respaldo del sector original donde el antivirus espera encontrarlo.

Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.

Cuando se encuentran archivos infectados, es preferible borrarlos y restaurarlos desde respaldos, aún cuando el programa antivirus que usemos pueda desinfectar los archivos. Esto es porque no existe seguridad sobre si el virus detectado es el mismo para el cual fueron diseñadas las rutinas de desinfección del antivirus, o es una mutación del original.

Cuando se va a formatear un disco rígido para eliminar algún virus, debe recordarse apagar la máquina por más de cinco segundos y posteriormente arrancar el sistema desde nuestro disquete limpio, donde también debe encontrarse el programa que se utilizará para dar formato al disco.

Cuando, por alguna causa, no se puede erradicar un virus, deberá buscarse la asesoría de un experto directamente pues, si se pidiera ayuda a cualquier aficionado, se correrá el riesgo de perder definitivamente datos si el procedimiento sugerido no es correcto.

Cuando se ha detectado y erradicado un virus es conveniente reportar la infección a algún experto, grupo de investigadores de virus, soporte técnico de programas antivirus, etc. Esto que en principio parecería innecesario, ayuda a mantener estadísticas, rastrear focos de infección e identificar nuevos virus, lo cual en definitiva, termina beneficiando al usuario mismo.

HIJACKTHIS, ELIMINAR SPYWARE, ADWARE, HIJACKERS, BHO...

HijackThis
Introducción

Ultimamente cada vez es más frecuente la aparición de morralla en los ordenadores. La palabra morralla aparecerá con frecuencia en este artículo y estará referida a toda esa fauna, con frecuencia no detectada por muchos antivirus (este aspecto está cambiando y,probablemente, más lo hará en el futuro), conocida como spyware,adware, hijackers, BHO, etc.

Para defendernos de su existencia disponemos de excelentes soluciones gratuitas, caso de Spybot Search & Destroy y la protección preventiva de Spywareblaster (ambos programas muy recomendables). Sin embargo, no siempre es posible eliminarla a posteriori con las medidas habituales y para esos casos puede ser bastante útil emplear, a modo de bisturí, la herramienta que se comentará en este artículo: HijackThis (HJT) de Merijn.org.

Antes de continuar, mencionaré algunas denominaciones dentro de esta fauna (suele ser motivo de confusión), unas más genéricas, otras más específicas, pero bastante típicas en los tiempos actuales:

Spyware: son programas que, sin conocimiento por parte del usuario, corren en segundo plano recolectando información sobre éste y sus hábitos de navegación. Esta información puede abarcar desde el navegador que utilizamos, páginas visitadas, duración de nuestra estancia en ellas, nuestra IP... inclusive el SO y la CPU que utilizamos. Dicha información es enviada a los responsables del programa y con ello no sólamente atentan contra nuestra privacidad, también hacen uso del ancho de banda de nuestra conexión para llevar a cabo su propósito. En resumen:no existe conocimiento ni consentimiento por parte del usuario.

Adware: (ADvertising-Supported softWARE): muy similar a lo anterior. La diferencia estriba en que suele venir incluido en programas shareware y por tanto,al aceptar los términos legales durante la instalación de dichos programas, estamos consintiendo su ejecución en nuestros equipos y afirmando que estamos informados de ello (aunque en la práctica no sea así, ya que pocas personas prestan atención a los contratos licencias de uso mostradas durante la instalación). Un ejemplo de ésto pueden ser los banners publicitarios que aparecen en software diverso y que, en parte, suponen una forma de pago por emplear dichos programas de manera pseudogratuita.

Hijackers: se encargan de modificar las opciones de configuración del navegador (tradicionalmente, Internet Explorer de MS) para apuntar hacia otros sitios,cambiar nuestra página de inicio, la página de error, etc. Habitualmente capturan nuestras peticiones de navegación, de manera que ralentizan el comportamiento del navegador, aparte de obligar a éste a obedecer a sus propósitos. Para comprender mejor el término es bastante descriptivo mencionar que, en otros ámbitos, esta palabra es empleada para definir a personas que empleando la fuerza, secuestran/roban un vehículo (típicamente un avión) para obligar a cambiar su ruta y lugar de destino. Vendría a ser lo mismo, aplicado a los navegadores. Suelen valerse de ActiveX maliciosos o de agujeros de seguridad del navegador, por ello es conveniente protegernos de ellos con la protección preventiva de Spybot S&D y Spywareblaster.

BHO (Browser Helper Object): se podría dar una definición técnica al estilo de es un objeto COM dentro de una DLL que se carga automáticamente con el IE... si buscáis algo así, mejor os remito a la amplia exposición de un artículo de MS. Para el objetivo de este artículo, es mucho más asequible decir que es un pequeño programa que se ejecuta automáticamente cada vez que abrimos el navegador de Internet. Suele instalarse a la vez que instalamos otros programas (como se mencionaba en el caso del adware, por ejemplo) o también mediante ActiveX y sus funciones pueden ser muy diversas, desde capturar eventos, lanzar pop ups, ventanas de mensajes, cambiar nuestra página de inicio, páginas de búsqueda, banners adware, crear toolbars, monitorizar y reportar nuestros hábitos, etc. En ocasiones pueden provocar errores en nuestro sistema, conflictos con otras aplicaciones, disminuir el rendimiento del navegador... poco agradable, ¿verdad? Hay que reseñar que este tipo de aplicaciones no son frenadas por los cortafuegos ya que, por sus características, son vistas como si fueran el propio navegador (ver símil con dll/code injection en nuestra guía del SSM, programa cada vez más recomendable).

Toolbars: grupo de botones situados generalmente bajo la barra de herramientas del navegador. Pueden deberse a aplicaciones normales (limpias) que tengamos instaladas, al integrarse de esa manera en nuestro navegador, aunque en ocasiones pueden ser producto de la presencia de BHO maliciosos.

Hay muchos más, pero esta muestra sirve de ejemplo para ver cómo esta fauna cada vez posee más elementos específicos, adquiriendo protagonismo propio por encima de denominaciones genéricas como spyware/adware. De la misma manera, hay que decir que no es infrecuente que se presenten simultáneamente en un mismo spyware, cada vez más complejos y con más ramificaciones por nuestros sistemas.

RECOMENDACIONES PREVIAS

Una vez descargado a nuestro HD, es conveniente emplazarlo en una carpeta que le hayamos creado ex profeso (en ella alojará los backups previos).

hjt1
Nos vamos al botón Config...

hjt2
Emplear esta herramienta no está exento de riesgo. Si se nos va la mano en la limpieza, podemos obtener resultados no deseables como puede ser mal funcionamiento del sistema e inclusive, problemas en su arranque. Es por ello sumamente importante indicarle que realice backups previos a su acción; por ese motivo nos aseguraremos de tildarle el casillero Make backups before fixing items desde el apartado Main. Si más adelante nos es preciso restaurarlo,acudimos a Backups, seleccionamos el correspondiente y pulsamos Restore (si hemos comprobado que no es necesario, desde aquí podemos también eliminar los backups ya inútiles, mediante el botón Delete).

hjt3
En ningún caso, ni los responsables del programa ni el que subscribe este artículo se hacen responsables de problemas derivados de su uso; ya se sabe que trastear en el registro puede traer consecuencias de diverso tipo y sólo usuarios con ciertos conocimientos deben aventurarse en determinadas labores, siempre bajo su propia responsabilidad. No obstante y teniendo en cuenta que desde un sistema con problemas en el arranque nos sería difícil la restauración de los backups propios de HJT,la recomendación es, antes de utilizar HJT, llevar a cabo backups plenos del registro mediante ERUNT y saber cómo restaurarlos en caso de problemas. En su artículo correspondiente de Nautopía, tenéis información sobre cómo crearlos y restaurarlos aun cuando el sistema se haya visto dañado en su arranque. Aseguraros de tener este aspecto bajo control y haber comprendido su manejo antes de meteros en faena ;-)

Más recomendaciones antes de emplear HJT: es conveniente capar todas las aplicaciones posibles antes de scanear con HJT. La explicación es sencilla: todo el trabajo a realizar se basa en el estudio del log resultante tras el escaneo; si tenemos numerosos servicios superfluos y aplicaciones conocidas iniciándose junto al sistema, el log va a ser muy extenso y por tanto más laborioso de analizar (todo lo superfluo sencillamente nos estorbaría a la hora de localizar a los culpables que andamos buscando para la ocasión).

Para capar lo superfluo suele bastar acudir a Inicio > Ejecutar > msconfig y desde las pestañas Services y StartUp, desmarcar lo no imprescindible.

¿Qué es lo superfluo? ...bueno, es más sencillo decir los que debemos dejar activos, que serían sólo servicios básicos del sistema y algunos elementos pertenecientes a la tarjeta gráfica. Para lo primero suele ser útil revisar alguna guía al respecto como puede ser la de Wininfo (que de paso, os servirá para mejorar vuestro sistema).

Aparte de eso, capar todo lo correspondiente a aplicaciones que hayáis instalado (antivirus, antispy, cortafuegos, elementos del adobe acrobat, de sistemas multimedia -quicktime, realplayer, etc.-, utilidades de grabación, etc.) porque recalco que para el objetivo que nos traemos entre manos, sólo servirán para estorbar a la hora de analizar el log resultante. Sed meticulosos con estos detalles, merece la pena.

Por supuesto, en esas condiciones es totalmente desaconsejable que os conectéis a Internet; antes de ello -y siempre después de que hayamos escaneado y obtenido un log de HJT libre de elementos superfluos-, deberéis activar nuevamente vuestra protección habitual de antivirus-cortafuegos. No olvidéis por tanto anotar los cambios que llevéis a cabo en Services y StartUp para, más adelante, poder volver a dejarlos como estaban.

Si por cualquier razón no os es posible acceder mediante Inicio > Ejecutar > msconfig, es posible acceder a los Servicios desde Panel de Control > Herramientas Administrativas > Servicios. Y para ver de manera alternativa otros elementos que se cargan en el arranque, suele ser bastante útil una herramienta como StartupCPL.

...ACCION!
Una vez llevadas a cabo las medidas previas (muy recomendable), estamos en condiciones de emplear HJT. Volvemos a la imagen inicial y pulsamos el botón Scan:

hjt1
En breves instantes, obtendremos un resultado visible en su propia ventana. Para analizar el log suele ser bastante cómodo utilizar el botón Save Log, de manera que indicándole una ubicación, lo tendremos disponible en nuestro bloc de notas.

hjt4
Una vez con el log a nuestro alcance, llega el momento clave: analizarlo.

Como se puede observar en el log, cada línea o ítem va precedida de una letra más uno ó dos números y hacen referencia a lo sgte:

R0, R1, R2, R3: URLs de páginas de inicio/búsqueda en el navegador Internet Explorer (IE).
F0, F1, F2, F3: Programas cargados a partir de ficheros *.ini (system.ini, win.ini...).
N1, N2, N3, N4: URLs de páginas de inicio/búsqueda en Netscape/Mozilla.
O1: Redirecciones mediante modificación del fichero HOSTS.
O2: BHO (Browser Helper Object); pueden ser plugins para aumentar las funcionalidades de nuestro navegador, pero también pueden deberse a aplicaciones maliciosas.
O3: Toolbars para IE.
O4: Aplicaciones que se cargan automáticamente en el inicio de Windows, bien mediante las claves oportunas en el registro, bien por aparecer en la carpeta del grupo Inicio.
O5: Opciones de IE no visibles desde Panel de Control.
O6: Acceso restringido -por el Administrador- a las Opciones de IE.
O7: Acceso restringido -por el Administrador- al Regedit.
O8: Items extra encontrados en el menú contextual de IE.
O9: Botones extra en la barra de herramientas de IE, así como ítems extra en el apartado Herramientas de IE (no incluídas en la instalación por defecto).
O10: Winsock hijackers.
O11: Adición de un grupo extra en las Opciones Avanzadas de IE (no por defecto).
O12: Plugins para IE.
O13: Hijack del prefijo por defecto en IE.
O14: Hijack de la configuración por defecto de IE.
O15: Sitios indeseados en la zona segura de IE.
O16: Objetos ActiveX
O17: Hijack de dominio / Lop.com
O18: Protocolos extra / Hijack de protocolos
O19: Hijack de la hoja de estilo del usuario.

Veamos cada ítem con algo más de detalle:

Grupo R0, R1, R2, R3:
URLs de páginas de inicio/búsqueda en el navegador Internet Explorer (IE).

Si reconocemos las URL hacia las que apuntan R0 y R1 (R2 ya no es utilizado) como válidas, podemos dejarlas tal cual. Si por el contrario son nocivas o tenemos fundadas sospechas de que puedan serlo, es conveniente seleccionarlas y aplicar el "fix" de HJT.

Ejemplo de válidas:
R0 - **HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.google.com/**
R1-
HKLM\Software\Microsoft\InternetExplorer\Main,Default_Page_URL=http://www.google.com

Si veis que aparece un valor con "(obfuscated)" final, como puede ser el del sgte. ejemplo:

R1 - **HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = res://C:\WINDOWS\System32\mbnmmc.dll/sp.html (obfuscated)**

...es muy posible que se deba a algún spyware, empleando algún método de ocultación para dificultar el reconocimiento. En estos casos suele ser conveniente aplicar el "fix".

R3 hace referencia a Url Search Hook, que es usado cuando en el recuadro de direcciones del navegador introducimos alguna pero sin especificar su protocolo (http://, ftp://). En estas ocasiones, el navegador trata de utilizar el protocolo adecuado por sí mismo, pero si el intento no es exitoso, acude a Url Search Hook para tratar de resolver los datos que le hemos introducido como URL. Esta información se encuentra en la sgte. clave del registro: **HKCU\Software\Microsoft\Internet Explorer\URLSearchHooks**

Si el valor que os sale en esa clave es del tipo R3 - URLSearchHook: (no name) - {CFBFAE00-17A6-11D0-99CB-00C04FD64497}_ - (no file) ...con ese guión bajo final (_ , resaltado en color para el ejemplo), suele ser conveniente hacer uso de Regedit para reparar a mano el nombre del valor, ya que HJT no puede solucionarlo en esos casos. No quitéis el valor numérico mostrado arriba, ya que es el empleado por defecto.

Como norma general para R3, en caso de aparecer en el log, deberíamos indagar sobre la información mostrada. Si es referente a un programa que nosotros hemos instalado (el multibuscador Copernic, por ejemplo) y fuera de confianza, no pasa nada; pero en caso de ser algo sospechoso, lo indicado es aplicarle el "fix".

Grupo F0, F1, F2, F3:

Programas cargados a partir de ficheros *.ini (system.ini, win.ini...).

Hay reportados problemas graves para arrancar el sistema si tras fijar uno de estos ítems (especialmente F2) se ha llevado a cabo la restauración de un backup propio de HJT en su versión 1.98.2 (la actual) ...sed muy cautos por tanto y valorad los riesgos previamente. Aunque desde Nautopía recomendamos el uso de ERUNT para tales fines y probablemente solventase el problema, no nos hemos visto en situación de poder comprobarlo en la práctica ante esta situación concreta. Ahí queda el aviso...

F0: en caso de que aparezcan, desde Merijn.org recomiendan aplicarles siempre el "fix". Su información procede de shell= en system.ini. En condiciones normales, esta ubicación indica el gestor del entorno gráfico del sistema, el responsable de cargar el escritorio al inicio del windows y permitir manejarnos con ventanas (si se me permite la licencia del símil, "las X" del mundo linux). Como habréis adivinado, nos referimos al explorer.exe ...pero (y este es el quid de la cuestión), si tras explorer.exe tenemos un morralla.exe, se cargará igalmente al iniciar nuestro win. Todo lo que encontréis aquí tras explorer.exe, se convierte en altamente sospechoso.

F1: suelen deberse a programas muy antiguos y lo indicado es buscar información sobre ellos para decidir si son sospechosos o no. Su información procede del win.ini, concretamente de Run= o Load=; el primero se empleaba con antiguos programas para que se cargaran con el arranque de win (hablamos de Win 3.1/95/98), pero hoy no es habitual; el segundo se empleaba para cargar controladores de hardware.
El listado Pacman's Startup List os puede servir a nivel orientativo para identificar ejecutables.

F2 y F3 vienen a utilizar el equivalente de los anteriores pero en los windows de núcleo NT (Win

NT/2000/XP), que no suelen hacer uso de system.ini/win.ini del modo tradicional; estamos hablando de entradas en el registro:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

La primera se emplea para permitir la compatibilidad hacia atrás con aplicaciones de uso en los Win 9x. Mediante la función IniFileMapping se ha colocado en el registro cada línea aparecida en el fichero .ini, de manera que al utilizar un programa que haga uso de él, va a buscarse primero la equivalencia en el registro.

La segunda cadena nos habla de lo que se carga inmediatamente después de que el usuario se loguea al iniciar el sistema. Userinit.exe se encuentra en C:\WINNT\system32 o en C:\WINDOWS\system32, según el Win que empleemos (a lo largo del artículo, indicaremos C:\WINNT o C:\WINDOWS como [**]); su función es meter el perfil de cada usuario tras el login. En este caso el problema viene si aparece un morralla.exe (treta frecuente de ver en troyanos) tras userinit:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit =[**]\system32\userinit.exe,[**]\morralla.exe

Esto se ve en la información del valor userinit, picando dos veces sobre él desde regedit; estaría de la sgte.manera, separado simplemente por una coma (resaltada en amarillo):

Userinit = [**]\system32\userinit.exe, [**]\morralla.exe

No preocuparos si bajo Win NT encontráis el valor por defecto: userinit,nddeagnt.exe, es normal bajo ese sistema. Pero cualquier otro ejecutable es altamente probable que se trate de morralla y/o troyano.

Grupo N1, N2, N3, N4:

URLs de páginas de inicio/búsqueda en Netscape/Mozilla.

N1, N2, N3, N4 corresponden respectivamente a las páginas de inicio/búsqueda de Netscape v4, v6, v7 y Mozilla. Estos datos se encuentran en el fichero prefs.js, habitualmente localizado en el directorio del navegador.

El uso de estos navegadores no está tan extendido como el de IE y por tanto, están menos expuestos a la acción de morralla especializada; sin embargo, haberla hayla (de la extensa familia Lop.com por ejemplo). Si os aparece una entrada de este nivel y no la reconocéis como vuestra página deseada de inicio/búsqueda, lo indicado es marcarla y aplicarle el "fix" de HJT.

O1: Redireccionamientos por modificación del fichero HOSTS

El fichero HOSTS lo podemos encontrar en diversas ubicaciones según el windows empleado. Se localiza en C:\WINDOWS\ en los Win 9x/Me y en [**]\SYSTEM32\DRIVERS\ETC\ en los Win NT/2000/XP/2003.

Mediante el fichero HOSTS es posible asociar IPs con dominios. En condiciones normales, puede ser empleado si queremos evitar el acceso a determinados dominios que sabemos problemáticos, simplemente editando a mano el fichero HOSTS y asociando nuestra dirección localhost 127.0.0.1 con el dominio indeseable. Ejemplo: 127.0.0.1 www.dominioindeseable.com...al hacerlo, si introducimos esa dirección en el navegador, nuestro equipo primero la buscará en el fichero

HOSTS y al encontrarla, se evitará resolverla externamente mediante DNS. De esta manera evitamos que se pueda acceder a dicho dominio indeseable.

Sin embargo, puede ser empleado con fines maliciosos por la morralla que tratamos de combatir en este artículo, sencillamente dándole la vuelta a la tortilla: si en lugar de localhost se emplea una IP determinada (llamémosla IP morralla) para direcciones de uso habitual, por ejemplo www.google.com, cada vez que introduzcamos la dirección de google en nuestra barra de direcciones, seremos llevados a la página de la IP morralla. Esto redireccionamiento suele ser frecuente de ver por parte de los hijackers.

Si el ítem O1 nos muestra una IP que no se corresponde con la dirección, podemos marcarla y aplicarle el "fix" de HJT.

Si nos muestra O1 - Hosts file is located at C:\Windows\Help\hosts ...casi con toda probabilidad estamos delante de una infección por CoolWebSearch (CWS), en cuyo caso conviene aplicarle el "fix", aunque mejor si previamente lo intentamos con herramientas específicas contra CWS como pueden ser (en este orden)delcwssk y CWShredder.

O2: BHO (Browser Helper Object)

Pueden ser plugins para aumentar las funcionalidades de nuestro navegador, perfectamente normales, pero también pueden deberse a aplicaciones morralla. Es preciso por tanto que el usuario investigue para comprobar el grado de sospecha. En el listado de Tony Klein y colaboradores en Sysinfo, podréis encontrar referenciadas numerosas CLSID (class ID, el número entre llaves: {número class ID}). Las allí señaladas en Status como "X" son catalogadas de spyware, las "L" como normales o limpias.

Ejemplo normal:

O2 - BHO: (no name) - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Archivos de programa\Adobe\Acrobat 5.0\Reader\ActiveX\AcroIEHelper.ocx
...si introducís ese CLSID (06849E9F-C8D7-4D59-B87D-784B7D6BE0B3) en el buscador del listado, os lo mostrará catalogado como "L", es decir, normal, ya que está originado por nuestro Adobe Acrobat Reader.

Si por el contrario el resultado de vuestra búsqueda os lo mostrara como "X", ya sabéis que se trata de spyware y conviene aplicarle el "fix". Es preciso que en ese momento no tengáis abierta ninguna ventana del navegador e incluso así, a veces hay casos rebeldes. Si tras aplicar el "fix" veis que vuelve a salir en el listado, será preciso reiniciar en modo a prueba de fallos (modo seguro) para erradicarlo.

O3: Toolbars para IE

Recordamos la definición de Toolbar: suelen ser un grupo de botones situados generalmente bajo la barra de herramientas del navegador, que pueden deberse a aplicaciones normales que tengamos instaladas, al integrarse de esa manera en nuestro navegador, aunque en ocasiones pueden ser producto de la presencia de BHO maliciosos.
Su ubicación en el resgistro depende de esta cadena: HKLM\Software\Microsoft\Internet Explorer\Toolbar

Ejemplo normal:

O3 - Toolbar: Web assistant - {0B53EAC3-8D69-4b9e-9B19-A37C9A5676A7} - C:\Archivos de programa\Archivos comunes\Symantec Shared\AdBlocking\NISShExt.dll

...como se ve en el ejemplo, esa toolbar está originada por el Norton Internet Security de Symantec. Sin embargo, en caso de no reconocer el nombre mostrado, se puede acudir al mismo listado reseñado para los ítems O2 para tratar de salir de dudas respecto a su identidad. El procedimiento es el mismo: buscar en función del CLSID y comprobar si está referenciado como "X" (spyware) o "L" (limpio). En caso de ser spyware, conviene marcar el ítem y aplicar el "fix" de HJT.

O4: Aplicaciones de carga automática en inicio de Windows por Registro/grupo Inicio

La carga automática de estas aplicaciones viene dada por ciertas claves en el registro o por aparecer en directorios del grupo Inicio.

* Claves del registro implicadas:
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- \RunServices
- \Run
- \RunOnce
- \RunOnceEx
- \Policies\Explorer\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion \RunServicesOnce
- \RunServices
- \Run
- \RunOnce
- \RunOnceEx
- \Policies\Explorer\Run
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
- \RunServicesOnce
- \RunServices
- \Run
- \RunOnce
- \Policies\Explorer\Run

Ejemplo: O4 - HKCU\..\Run: [SystemSafe] C:\Archivos de programa\SSM\SysSafe.exe

* Los directorios del grupo Inicio pueden tener estas ubicaciones:

* C:\Documents and Settings\All Users\Menú Inicio\Programas\Inicio...reflejado en el log de HJT como Global Startup; son programas que se cargan para el perfil de todos los usuarios.

Ejemplo: O4 - Global Startup: TeleSA.lnk = C:\Archivos de programa\AVer Teletext\AVerSA.exe

* R:\Documents and Settings\USUARIO\Menú Inicio\Programas\Inicio...reflejado en el log de HJT como Startup: programas que se cargan sólo para el perfil de ese USUARIO.

Ejemplo: O4 - Startup: Microsoft Office.lnk = C:\Archivos de programa\Microsoft Office\Office10\OSA.EXE

Al igual que para el Grupo F, ante la duda, el Pacman's Startup List os podría servir a nivel orientativo para identificarlos.

Si os encontráis con un ítem indeseable y deseáis aplicarle el "fix", no será exitoso mientras el proceso esté activo en memoria. En esos casos, primero debéis acudir al Administrador de Tareas para cerrar dicho proceso y poder luego actuar con HJT.

O5: Opciones de IE no visibles desde Panel de Control

En condiciones normales, las Opciones de Internet de IE son accesibles desde Panel de Control. Existe la posibilidad de no permitirlo (desaparecer su icono), añadiendo una entrada en el fichero control.ini ubicado en [**] (C:\WINNT o C:\WINDOWS, según versión del SO), lo que se reflejaría en el sgte. ítem del log de HJT:

O5 - control.ini: inetcpl.cpl=no

...pero este hecho, a menos que sea una acción intencionada del Administrador del Sistema (en cuyo caso lo dejaríamos tal cual), podría deberse a la acción de alguna aplicación morralla que de esta manera trate de dificultar que cambiemos las Opciones del IE. Si se trata de esto último, es conveniente aplicarle el "fix" de HJT.

O6: Acceso restringido -por el Administrador- a las Opciones de IE

Si el acceso está restringido por el Administrador o bien porque empleamos Spybot S&D y aplicamos su protección-bloqueo de las Opciones del IE (en Herramientas > Modificaciones de IE: Bloquear la configuración de la pág. de Inicio...), aparecerá un ítem como el sgte.:

O6 - HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions present

Si por ejemplo en ese mismo apartado de Spybot S&D no hemos marcado el casillero Bloquear el acceso..., observaríamos este otro:

O6 - HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel present

Si el acceso restringido (primer ítem de ejemplo) aparece y no se debe a medidas intencionadas por parte del Administrador y/o la acción preventiva de Spybot, suele ser conveniente aplicarle el "fix".

O7: Acceso restringido -por el Administrador- a Regedit

Cuando el acceso a Regedit está bloqueado mediante la correspondiente clave del registro (no es infrecuente en políticas de seguridad corporativas), se refleja en un ítem como el sgte.:

O7 - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System, DisableRegedit=1

Salvo que lo anterior se deba a medidas tomadas intencionadamente por el Administrador (en cuyo caso ignoraríamos el ítem), es conveniente aplicarle el "fix" de HJT.

O8: Items extra en el menú contextual de IE

El menú contextual en IE es el que obtenéis al picar con el botón derecho sobre la web que estáis viendo. Os muestra diferentes ítems o líneas de selección y pueden deberse a aplicaciones normales, pero también a spyware. Las diferentes opciones en ese menú se albergan en la sgte. cadena del registro:

HKCU\Software\Microsoft\Internet Explorer\MenuExt

Ejemplo normal: O8 - Extra context menu item: E&xportar a Microsoft Excel - res://C:\ARCHIV~1\MICROS~3\OFFICE11\EXCEL.EXE/3000

Pero si no reconocéis la aplicación responsable del ítem extra en el menú contextual y sospecháis que sea por morralla, podéis aplicarle el "fix" de HJT.

O9: Botones extra en la barra de herramientas de IE / Items extra en el apartado Herramientas de IE (no incluídas en la instalación por defecto)

Si tenéis botones extra en la barra de herramientas principal de IE o bien ítems extra en el menú Herramientas de IE (que no sean los incluídos en la instalación por defecto) y queréis deshaceros de ellos por sospechar que provengan de morralla, deberéis fijaros en este ítem O9 del log de HJT, que obtiene los datos de la sgte. cadena del registro: **HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions**

Ejemplos normales:
O9 - Extra button: Messenger (HKLM)
O9 - Extra 'Tools' menuitem: Windows Messenger (HKLM)
O9 - Extra button: AIM (HKLM)

En los normales no es preciso hacer nada, pero ante casos indeseables que queráis hacerlos desaparecer, el "fix" de HJT debería poder con ellos sin problemas.

O10: Winsock hijackers

En este apartado hay que ser extremadamente cautos o podéis dañar vuestra conexión a Internet. Desde la propia Merijn.org recomiendan, en caso de necesitar resolver reseñas mostradas en este ítem O10, emplear versiones modernas de Spybot S&D o la herramienta LSPFix de Cexx.org mejor que actuar con HJT. Es por ello que os remitimos a esas dos alternativas en vez de profundizar en este punto.

No os preocupéis si veis aquí referencias a algún módulo de vuestro antivirus. Puede ser normal en aquellos que actúan a nivel del winsock.

O11: Adición de un grupo extra en las Opciones Avanzadas de IE (no por defecto)

Estamos hablando de IE > Herramientas > Opciones > pestaña Opciones Avanzadas. Si ahí apareciera algún grupo extra, no perteneciente a los que trae por defecto, vendría reflejado (como los originales) en la sgte. cadena del registro: HKLM\SOFTWARE\Microsoft\Internet Explorer\AdvancedOptions

Desde Merijn.org comentan que, de momento, sólo el hijacker CommonName añade sus propias opciones en la pestaña de avanzadas. En ese caso el ítem mostrado (morralla) sería como sigue:

O11 - Options group: [CommonName] CommonName

...si tenéis ese caso, marcadlo y aplicar el "fix" de HJT. Si es otro distinto, en principio se convierte en sospechoso y requerirá que busquéis información por la red acerca de su procedencia.

O12: Plugins para IE

En condiciones normales, la mayoría de plugins son de aplicaciones legítimas y están ahí para ampliar funcionalidades de IE.

Ejemplos normales:
O12 - Plugin for .spop: C:\Archivos de programa\Internet Explorer\Plugins\NPDocBox.dll
O12 - Plugin for .PDF: C:\Archivos de programa\Internet Explorer\Plugins\nppdf32.dll

Generalmente son normales, pero ante la duda, conviene buscar por la red su procedencia.

No obstante, se tiene reportado algún caso claro de morralla en este apartado como es el plugin de OnFlow, que se detecta fácil por su extension *.ofb; si os lo encontráis, conviene marcarlo y aplicar el "fix".

O13: Hijack del prefijo por defecto en IE

El prefijo por defecto en IE (IE DefaultPrefix), hace referencia a cómo son manejadas las URLs que introducimos en el casillero de direcciones del navegador IE, cuando no especificamos el protocolo (http://, ftp://, etc.). Por defecto IE tratará de emplear http://, pero es posible modificar este valor en el registro mediante la sgte. cadena:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix

De hecho, existen aplicaciones morralla que lo llevan a cabo, obligando al navegante incauto a llegar hacia donde no desea. Una de ellas, muy conocida, es el hijacker CoolWebSearch (CWS), que sustituye el DefaulPrefix por "http://ehttp.cc/?", de manera que cuando el usuario introduce "www.google.com", automáticamente es derivado a "http://ehttp.cc/?www.google.com", que es un site perteneciente a CWS. Como veis, avispados son.

Ejemplo nocivo de CWS:
O13 - WWW. Prefix: http://ehttp.cc/?

...en estos casos, antes de emplear HJT, conviene utilizar herramientas específicas contra CWS como pueden ser delcwssk primero y CWShredder después (no olvidéis actualizarlo antes de aplicarlo). Pasar tras reiniciar el scan de HJT y comprobad si ha sido suficiente con ellas, aplicando finalmente el "fix" de HJT en caso necesario.

CWS tiene muchísimos dominios y es un listado en continua expansión; sed cuidadosos ahí fuera.

Otros ejemplos morralla a los que podéis aplicar el "fix":
O13 - DefaultPrefix: http://www.pixpox.com/cgi-bin/click.pl?url=
O13 - WWW Prefix: http://prolivation.com/cgi-bin/r.cgi?

O14: Hijack de la configuración por defecto de IE

Hay una opción entre las muchas del IE, que es resetear los valores presentes y volver a la configuracion por defecto. Los valores de esta última, se guardan en el fichero iereset.inf, ubicado en [**]\inf y el problema puede aparecer si un hijacker modifica la información de dicho fichero porque, de esa manera, al resetear a la configuración por defecto, lo tendríamos presente de nuevo. En estos casos es conveniente aplicar el "fix".

Ejemplo morralla: O14 - IERESET.INF: START_PAGE_URL=http://www.searchalot.com

No obstante, tened cuidado porque no todo lo que aparece en este ítem tiene que ser nocivo. A

veces puede deberse a manipulaciones legítimas del Administrador de Sistemas, manufactura de equipos de ciertas marcas, corporativos, etc. En estos casos seguramente reconoceréis la URL mostrada y no será necesario ningún procedimiento.

O15: Sitios indeseados en la zona segura de IE

En IE la seguridad se establece por medio de zonas o y según éstas, la permisividad en términos de seguridad es mayor o menor. En niveles bajos de seguridad, es posible ejecutar scripts o determinadas aplicaciones que no están permitidos en niveles altos.
Es posible añadir dominios a unas zonas u otras (sitios de confianza/sitios restringidos), según nuestro grado de confianza en ellos y esto se recoge en la sgte. cadena del registro: **HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains**

Si por ejemplo hemos añadido www.nautopia.net a los sitios de confianza, nos aparecería reflejado de esta manera en el ítem correspondiente de HJT:

O15 - Trusted Zone: www.nautopia.netDe igual manera puede aparecer, por ejemplo, el dominio de empresa de nuestro puesto de trabajo o cualquier otro que hayamos añadido conscientemente.

Pero puede darse el caso de que alguna compañía como AOL o morralla como CWS, introduzcan silentemente sus dominios dentro de los sitios de confianza, lo que podría verse reflejado de la sgte. manera:

O15 - Trusted Zone: http://free.aol.com
O15 - Trusted Zone: *.coolwebsearch.com

En el caso de CWS o en el de cualquier otro que no deseemos tener como sitio de confianza, le indicaremos a HJT su "fix".

O16: Objetos ActiveX

Los objetos ActiveX son programas descargados de alguna web y guardados en nuestro ordenador; por ello también se les denominan Downloaded Program Files. La ubicación de almacenamiento es [**]\Downloaded Program Files

Podemos encontrar ítems normales como el del sgte. ejemplo:

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://download.macromedia.com/pub/shockwa...ash/swflash.cab

Y otros típicos de morralla que, con suerte, serán fácilmente identificables si muestran nombres sospechosos relacionados con porno, dialers, toolbars indeseadas o palabras claves como casino, sex, adult, etc. Ejemplo:

O16 - DPF: {12398DD6-40AA-4C40-A4EC-A42CFC0DE797} (Installer Class) - http://www.xxxtoolbar.com/ist/softwares/v4...006_regular.cab

En casos de morralla, podemos emplear tranquilamente el "fix" de HJT, pero si tras volver a escanear viéramos casos rebeldes que siguen presentes, sería necesario reiniciar en modo seguro (pulsando F8...) para proceder con su eliminación.

Spywareblaster de JavaCool cuenta en su base de datos con un numeroso listado de ActiveX maliciosos. Volvemos a recomendar su utilización preventiva.

O17: Hijack de dominio / Lop.com

En condiciones normales, cuando introducimos el nombre de un site en el navegador en lugar de su dirección IP, nuestro PC contacta con un servidor DNS para que resuelva correctamente el nombre del dominio. Sin embargo, puede darse el caso de que un hijacker cambie las DNS para que empleemos su propio servidor en lugar del servidor DNS habitual. Si lo llevan a cabo podrán redireccionarnos a donde les apetezca, apuntando nuestras peticiones hacia los dominios de su elección (no la nuestra).

Ejemplo normal:

O17 - HKLM\System\CCS\Services\Tcpip\..\{41BAB21B-F197-471E-8B00-F28668AB8782}: NameServer = 194.224.52.36,194.224.52.37

...decimos normal porque esas IPs corresponden a servidores DNS de un conocido ISP español y en estos casos no es preciso hacer nada. Es la situación más habitual, encontrar las DNS que nos proporciona nuestro ISP.

Para comprobar si son buenas o no, podéis hacer un whois con aplicaciones ex profeso o acudir a sites de fiar que ofrezcan ese servicio, como RIPE, ARIN, inclusive el propio Google. Ahora bien, si los resultados de nuestras pesquisas apuntan hacia morralla, les aplicaremos el "fix" con HJT.

O18: Protocolos extra / Hijack de protocolos

Es difícil explicar este apartado de una manera sencilla. A grosso modo, decir que nuestro SO emplea unos protocol drivers estándar para enviar/recibir información, pero algunos hijackers pueden cambiarlos por otros (protocolos "extra" o "no estándar") que les permitan en cierta manera tomar el control sobre ese envío/recepción de información.

HJT primero busca protocolos "no estándar" en HKLM\SOFTWARE\Classes\PROTOCOLS\ y si los encuentra, mediante la CLSID trata de obtener la información del path, también desde el registro: HKLM\SOFTWARE\Classes\CLSID

Ejemplo morralla:
O18 - Protocol: relatedlinks - {5AB65DD4-01FB-44D5-9537-3767AB80F790} - C:\ARCHIV~1\ARCHIV~1\MSIETS\msielink.dll
Esta técnica no es de las más frecuentes de ver, pero puede ser empleada por conocida morralla como Huntbar -RelatedLinks- (la del ejemplo), CommonName -cn-, Lop.com -ayb-, inclusive CWS. Si los veis reseñados como tal en el ítem O18 de HJT, aplicadles el "fix".

O19: Hijack de la hoja de estilo del usuario

Según Merijn.org, en caso de aparecer en el log de HJT este ítem O19, coincidente con un navegador ralentizado y frecuentes pop-ups, podría ser conveniente aplicarle el "fix". Sin embargo, dado que hasta el momento sólo se tiene reportado a CWS como responsable, la recomendación es emplear contra él las herramientas específicas citadas anteriormente.

Señalar que puede haber usuarios que tengan prefijada una hoja de estilo a su gusto, en cuyo caso no deberían prestar atención a este ítem.

LOS SERVICIOS EN XP

¿Qué es un servicio?

Los servicios no son nada mas ni nada menos que programas o aplicaciones cargadas por el propio sistema operativo. Estas aplicaciones tienen la particularidad que se encuentran corriendo en segundo plano (Background).

Con la instalación, se instalan por defecto y ejecutan una cierta cantidad de servicios. Dependiendo de nuestras necesidades, podemos deshabilitar o no algunas de ellas.

Mientras mas aplicaciones tengamos ejecutándose consumimos mas recursos, por lo tanto, vamos a tratar de deshabilitar lo que no utilizamos.

¿Dónde veo los servicios?

Debemos abrir la consola de Microsoft.

Esto lo hacemos yendo a:

- Inicio -> Panel de control ->Herramientas Administrativas ->Servicios ,o de esta otra manera:
- Inicio-> Ejecutar, escribimos services.msc y presionamos Enter

¿Cómo inicio o detengo un servicio?

Una vez en la consola, nos posicionamos arriba del servicio que queremos iniciar o detener y haciendo click con el boton derecho vamos a ver las acciones correspondientes.

¿Diferentes estados?

Los servicios pueden encontrarse en dos estados posibles. Pueden estar iniciados, es decir, se encuentra ejecutándose/corriendo o puede estar detenido.

Y tenemos tres opciones posibles de inicio:

- Automático: Se inician junto con el sistema operativo.
- Manual: Podemos iniciarlo y detenerlo manualmente cuando querramos u otro servicio puede hacerlo automáticamente. En un principio estaría detenido.
- Deshabilitado: No se puede iniciar manualmente ni otro servicio puede hacerlo.

Para cambiar la manera en que se inicia un servicio, debemos dirigirnos a la consola. Una vez ahi elegimos el servicio con el cual vamos a trabajar, hacemos click con el boton derecho del mouse y elegimos propiedades.

Recuperando un servicio

Supongamos que necesitamos recuperar la manera de inicio de alguno de los servicios, pero por alguna razón, no podemos iniciar la consola. ¿Qué podemos hacer?

No dirigimos a Inicio->Ejecutar-> escribimos regedit y presionamos Enter
Expandimos la siguiente clave:
HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices y buscamos el servicio en cuestión. Luego seleccionamos la clave Start y con click derecho elegimos modificar.

Las opciones que tenemos son:
1 – Automático
2 – Manual
3 – Deshabilitado
Por último, aceptamos y reiniciamos la computadora.

Administración de aplicaciones
Ofrece servicios de instalación de software como Asignar, Publicar y Quitar.

Se recomienda modo Manual, Iniciarlo cuando sea necesario.

Nombre del servicio: Application Management (AppMgmt)
Ejecutable o DLL: svchost.exe

Cliente DNS
Resuelve y almacena en caché los nombres del sistema de nombres de dominio (DNS) para este equipo. Si se detiene este servicio, este equipo no podrá resolver nombres DNS ni ubicar controladores de dominio en Active Directory. Si se deshabilita este servicio, no se podrá iniciar ninguno de los servicios que dependen explícitamente de él.Requerido si usás IPSEC.

Si tu máquina esta en red, Automático. De lo contrario Manual.

Nombre del servicio: DNS Client (Dnscache)
Ejecutable o DLL: svchost.exe

Cola de impresión
Carga archivos en la memoria para imprimirlos después. Este servicio es requerido si utilizamos impresoras, incluso las que están en red. Se recomienda tener en modo Automático, salvo que no necesitemos imprimir.

Nombre del servicio: Print Spooler (Spooler)
Ejecutable o DLL: spoolsv.exe

Configuración inalámbrica rápida
Proporciona configuración automática para los adaptadores 802.11 dispositivos de redes sin cable (Wireless).
Si no tenemos este tipo de hardware, nos conviene Deshabilitarlo.

Nombre del servicio: Wireless Zero Configuration (WZCSVC)
Ejecutable o DLL: svchost.exe

Cliente Web
Habilita los programas basados en Windows para que creen, tengan acceso y modifiquen archivos basados en Internet. Si este servicio se detiene, estas funciones no estarán disponibles. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse.

Por razones de seguridad se aconseja poner en Manual.

Nombre del servicio: WebClient (WebClient)
Ejecutable o DLL: svchost.exe

Conexiones de red
Administra objetos en la carpeta Conexiones de red y acceso telefónico, donde se pueden ver conexiones de red de área local y remota.

Se aconseja poner Atomatico si estamos en red o nos conectamos a través de un módem. De lo contrario Manual.

Nombre del servicio: Network Connections (Netman)
Ejecutable o DLL: svchost.exe

Detección de hardware shell
Detección de hardware shell como algunas lectoras de CD o DVD.

Se aconseja poner Automático.

Nombre del servicio: Shell Hardware Detection (ShellHWDetection)
Ejecutable o DLL: svchost.exe

DDE de red
Ofrece transporte y seguridad en la red para el Intercambio dinámico de datos (DDE) para los programas que se ejecutan en el mismo equipo o en diferentes equipos. Si este servicio se detiene, se deshabilitarán el transporte y la seguridad DDE. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse.

Si estás en red y utilizás datos compartidos, Automático. De lo contrario Manual.

Nombre del servicio: Network DDE (NetDDE)
Ejecutable o DLL: netdde.exe

DSDM de DDE de red
Administra los recursos de red Intercambio dinámico de datos (DDE). Si este servicio se detiene, se deshabilitarán los recursos compartidos de red DDE. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse.
Se aconseja poner Manual.

Nombre del servicio: Network DDE DSDM (NetDDEdsdm)
Ejecutable o DLL: netdde.exe

Escritorio remoto compartido de NetMeeting
Permite a los usuarios autorizados acceder remotamente a su escritorio Windows usando NetMeeting. Si detenemos este servicio, no podremos utilizar el escritorio remoto compartido.

Por seguridad lo vamos a Deshabilitar.

Nombre del servicio: NetMeeting Remote Desktop Sharing (mnmsrvc)
Ejecutable o DLL: mnmsrvc.exe

Enrutamiento y acceso remoto
Ofrece servicios de enrutamiento a empresas en entornos de red de área local y extensa. Provee LAN-to-LAN, LAN-to-WAN, VPN, NAT, etc..

Este servicio viene Deshabilitado y por seguridad lo vamos a dejar así.

Nombre del servicio: Routing and Remote Access (RemoteAccess)
Ejecutable o DLL: svchost.exe

Estación de trabajo
Crea y mantiene conexiones de cliente de red a servidores remotos. Si se detiene el servicio, estas conexiones no estarán disponibles. Si se deshabilita el servicio, no se podrá iniciar ninguno de los servicios que dependan explícitamente de él, por lo tanto es conviente dejarlo en modo Automático.

Nombre del servicio: Workstation (lanmanworkstation)
Ejecutable o DLL: svchost.exe

Extensiones de controlador de Instrumental de administración de Windows

Proporciona información de administración de sistemas a y desde controladores. Nuevas prestaciones e implementaciones a WMI. No tan importante como el anterior, conviene ponerlo en modo Manual.

Nombre del servicio: Windows Management Instrumentation Driver Extensions (Wmi)
Ejecutable o DLL: svchost.exe

Examinador de equipos

Mantiene una lista actualizada de equipos en la red y proporciona esta lista a los equipos designados como exploradores. Si se detiene este servicio, esta lista no se actualizará o mantendrá. Si se deshabilita el servicio, no se podrá iniciar ninguno de los servicios que dependan explícitamente de él.

No es necesario si no estas dentro de una red; tampoco en las que se conectan a internet a traves de un Módem.

Se recomienda modo Manual. Automático si estamos en red y no usamos WINS.

Nombre del servicio: Computer Browser (Browser)
Ejecutable o DLL: svchost.exe

Horario de Windows

Mantiene la sincronización de fecha y hora en todos los clientes y servidores de la red. Si se detiene este servicio, no estará disponible la sincronización de fecha y hora. Si se deshabilita este servicio, no se podrá iniciar ninguno de los servicios que dependen explícitamente de él.

Se recomienda Automatico.

Nombre del servicio: Windows Time (W32Time)
Ejecutable o DLL: svchost.exe

Host de dispositivo Plug and Play universal

Proporciona compatibilidad para albergar dispositivos Plug and Play universales.
Se recomienda Deshabilitar.

Nombre del servicio: Universal Plug and Play Device Host (UPNPhost)
Ejecutable o DLL: svchost.exe

Instantáneas de volumen

Administra e implementa Instantáneas de volumen usadas para copias de seguridad y otros propósitos. Si este servicio se detiene, las instantáneas se deshabilitarán para la copia de seguridad y ésta dará un error. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse. Poner en modo Manual.

Nombre del servicio: Volume Shadow Copy (VSS)
Ejecutable o DLL: vssvc.exe

Inicio de sesión en red

Admite la autenticación de paso de sucesos de inicio de sesión de cuenta para los equipos en un dominio.
Se utiliza para autentificarse en un Controlador de Dominio

Se recomienda Deshabilitar a no ser que nuestra computadora pertenezca a un dominio.

Nombre del servicio: Net Logon (Netlogon)
Ejecutable o DLL: lsass.exe

Instrumental de administración de Windows
Proporciona una interfaz común y un modelo de objeto para tener acceso a la información de administración acerca de un sistema operativo, dispositivos, aplicaciones y servicios.

WMI es una parte vital del sistema operativo de Microsoft. Por lo tanto, debe estar en modo Automático, para que éste funcione de manera adecuada.

Nombre del servicio: Windows Management Instrumentation (winmgmt)
Ejecutable o DLL: svchost.exe

Inicio de sesión secundario

Habilita los procesos de inicio en credenciales alternas. Si se detiene este servicio, se deshabilitará este tipo de acceso de inicio de sesión. Si este servicio está deshabilitado, cualquier servicio que explícitamente dependa de él no podrá iniciarse.
Se recomienda Manual.

Nombre del servicio: Secondary Logon (seclogon)
Ejecutable o DLL: svchost.exe

Llamada a procedimiento remoto (RPC)
Ofrece el asignador de punto final y otros servicios RPC diversos. Este servicio es fundamental. La mayoría de las cosas dependen de este servicio para funcionar. Asi que en Automático. Si lo detenemos, nuestra computadora no va a poder bootear.

Nombre del servicio: Remote Procedure Call (RPC) (RpcSs)
Ejecutable o DLL: svchost.exe

Localizador de llamadas a procedimiento remoto (RPC)
Administra la base de datos de servicios de nombres RPC.no es necesario que este servicio se encuentre funcionando. Así que lo ponemos en modo Deshabilitado.

Este es el servicio por el cual nos ha entrado el famoso Blaster.

Nombre del servicio: Remote Procedure Call Locator (RpcLocator)
Ejecutable o DLL: locator.exe

Mensajero
Transmite mensajes del servicio de alertas y el comando net send entre clientes y servidores. Este servicio no está relacionado con Windows Messenger. Si se detiene el servicio, no se transmitirán los mensajes de alerta. Si se deshabilita el servicio, no se podrá iniciar ninguno de los servicios que dependan explícitamente de él.

Si alguna vez ta a aparecido el mensaje famoso de que te ha tocado un viaje a Florida etc, el culpable es este servicio.

Te recomiendo Deshabilitado.

Nombre del servicio: Messenger (Mensajero)
Ejecutable o DLL: svchost.exe

MS Software Shadow Copy Provider
Administra instantáneas de volumen basadas en software y tomadas por el Servicio de instantáneas de volumen. Si se detiene el servicio, no se podrán administrar las instantáneas de volumen basadas en software. Si se deshabilita el servicio, no se podrá iniciar ninguno de los servicios que dependen explícitamente de él.

Lo podemos Manual.

Nombre en Inglés: MS Software Shadow Copy Provider (SwPrv)
Ejecutable o DLL: dllhost.exe

Medios de almacenamiento extraíbles
Se utiliza para la administración de medios removibles como ser Tape Backups, Jaz, Zip, LS120, SyQuest, etc.
Manua,l se detiene automáticamente cuando termina la tarea.

Nombre del servicio: Removable Storage (NtmsSvc)
Ejecutable o DLL: svchost.exe

(NLA) Network Location Awareness
Recopila y almacena información de configuración y ubicación de redes, e informa a las aplicaciones cuando esta información cambia.
Se recomienda poner en modo Manual.

Plug and Play
Habilita un equipo para que reconozca y adapte los cambios de hardware con el menor esfuerzo por parte del usuario. Si se detiene o deshabilita este servicio, el sistema se volverá inestable. Sel encarga de reconocer los dispositivos Plug and Play de nuestra máquina.

COMO RECUPERAR UN REGISTRO DAÑADO QUE IMPIDE QUE WINDOWS XP SE INICIE

En este artículo se describe cómo recuperar un sistema Windows XP que no se inicia debido a que el Registro está dañado. Este procedimiento no garantiza la recuperación completa del sistema a su estado anterior; sin embargo, al utilizarlo debería ser posible recuperar los datos.

En Windows XP es posible recuperar un Registro dañado. Los archivos de Registro dañados producen diferentes mensajes de error. Consulte en Knowledge Base los artículos acerca de mensajes de error relativos a problemas del Registro.

En este artículo se asume que los métodos de recuperación normales no han solucionado el problema y que sólo se puede tener acceso al sistema mediante la consola de recuperación. Si existe una copia de seguridad de Recuperación automática del sistema (ASR, Automatic System Recovery), es la mejor opción para la recuperación; se recomienda que utilice la copia de seguridad ASR antes de intentar el procedimiento descrito en este artículo.

Nota: asegúrese de reemplazar completamente las cinco secciones del Registro. Si sólo reemplaza una o dos secciones, podrían surgir problemas adicionales, ya que el software y el hardware almacenan su configuración en múltiples ubicaciones del Registro.

Al iniciar o reiniciar un equipo basado en Windows XP, puede aparecer uno de los mensajes de error siguientes:

No se puede iniciar Windows XP porque el siguiente archivo está dañado o no se encuentra:
\WINDOWS\SYSTEM32\CONFIG\SYSTEM

No se puede iniciar Windows XP porque el siguiente archivo está dañado o no se encuentra:
\WINDOWS\SYSTEM32\CONFIG\SOFTWARE

Stop: c0000218 {Error del archivo de Registro} El Registro no puede cargar la sección (archivo):
\SystemRoot\System32\Config\SOFTWARE o su registro o alternativo

En el procedimiento descrito en este artículo se utiliza la consola de recuperación (Restaurar sistema) y se indican por orden todos los pasos para garantizar que el proceso se complete correctamente. Una vez finalizado este procedimiento, el sistema debería volver a un estado muy similar a aquel en el que se encontraba antes de producirse el problema. Si ha ejecutado alguna vez NTBackup y ha completado una recuperación del estado del sistema, no necesita seguir los procedimientos de las partes dos y tres; puede pasar a la parte cuatro.

Parte uno

En esta parte, iniciará la consola de recuperación, creará una carpeta temporal, hará una copia de seguridad de los archivos existentes del Registro en una nueva ubicación, eliminará los archivos del Registro de su ubicación actual y, por último, copiará los archivos del Registro desde la carpeta de recuperación a la carpeta System32\Config.

Una vez finalizado este procedimiento, se crea un Registro que puede utilizar para volver a iniciar Windows XP. Ese Registro se creó y guardó durante la instalación inicial de Windows XP; por tanto, perderá los cambios y configuraciones realizados después de la instalación.

Para completar la parte uno, siga estos pasos:

Inicie la consola de recuperación.
En el símbolo del sistema de la consola de recuperación, escriba las líneas siguientes y presione Entrar cuando finalice cada una de ellas:

md tmp
copy c:\windows\system32\config\system c:\windows\tmp\system.bak
copy c:\windows\system32\config\software c:\windows\tmp\software.bak
copy c:\windows\system32\config\sam c:\windows\tmp\sam.bak
copy c:\windows\system32\config\security c:\windows\tmp\security.bak
copy c:\windows\system32\config\default c:\windows\tmp\default.bak

delete c:\windows\system32\config\system
delete c:\windows\system32\config\software
delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\default

copy c:\windows\repair\system c:\windows\system32\config\system
copy c:\windows\repair\software c:\windows\system32\config\software
copy c:\windows\repair\sam c:\windows\system32\config\sam
copy c:\windows\repair\security c:\windows\system32\config\security
copy c:\windows\repair\default c:\windows\system32\config\default

Escriba exit para salir de la consola de recuperación. El equipo se reinicia.

Nota: en este procedimiento se asume que Windows XP está instalado en la carpeta C:\Windows. Si se encuentra en una ubicación diferente, asegúrese de cambiar C:\Windows por la carpeta Windows apropiada.

Si tiene acceso a otro equipo, para ahorrar tiempo copie el texto del paso dos y, a continuación, cree un archivo de texto llamado, por ejemplo, CopiaReg1.txt. Para crear este archivo, ejecute el comando siguiente al iniciar el equipo en la consola de recuperación:
batch copiareg1.txt

El comando batch de la consola de recuperación permite procesar de forma secuencial todos los comandos escritos en un archivo de texto. Cuando se utiliza el comando batch, no es necesario escribir manualmente tantos comandos.

Parte dos

Para completar el procedimiento descrito en esta sección, debe iniciar sesión como administrador o como usuario administrativo (un usuario que dispone de una cuenta en el grupo Administradores). Si utiliza Windows XP Home Edition, puede iniciar sesión como usuario administrativo. En tal caso, debe iniciar Windows XP Home Edition en Modo a prueba de errores. Para iniciar el equipo con Windows XP Home Edition en Modo a prueba de errores, siga estos pasos:

Nota: imprima estas instrucciones antes de continuar. No podrá verlas después de iniciar el equipo en Modo a prueba de errores. Si utiliza el sistema de archivos NTFS, imprima también las instrucciones del artículo de Knowledge Base Q309531, al que se hace referencia en el paso siete.

Haga clic en **Inicio-> Apagar -> Reiniciar -> Aceptar.**

Presione la tecla F8.

En un equipo configurado para iniciarse en varios sistemas operativos, puede presionar F8 cuando aparezca el menú Inicio.

Utilice las teclas de dirección para seleccionar la opción apropiada del Modo a prueba de errores y, a continuación, presione ENTRAR.

Si dispone de un sistema de inicio dual o múltiple, utilice las teclas de dirección para seleccionar la instalación a la que desea tener acceso y, a continuación, presione ENTRAR.

En la parte dos, va a copiar los archivos de Registro desde la ubicación en la que se ha realizado la copia de seguridad mediante Restaurar sistema. Esta carpeta no está disponible en la consola de recuperación y no suele estar visible durante el uso normal. Antes de iniciar este procedimiento, debe cambiar algunas opciones de configuración para poder ver la carpeta:

Inicie el Explorador de Windows.

En el menú Herramientas, haga clic en Opciones de carpeta->Pestaña Ver-> Archivos y carpetas ocultos, haga clic para activar Mostrar archivos y carpetas ocultos y, después clic para desactivar la casilla de verificación Ocultar archivos protegidos del sistema operativo (recomendado).

Haga clic en Sí cuando aparezca el cuadro de diálogo que pide confirmación de que desea mostrar estos archivos.

Haga doble clic en la letra de la unidad en la que instaló Windows XP para obtener una lista de las carpetas. Es importante hacer clic en la unidad correcta.

Abra la carpeta System Volume Information. Esta carpeta aparece atenuada porque se trata de una carpeta ultra-oculta.

Nota: esta carpeta contiene una o más carpetas _restore {GUID}, como _**restore{87BD3667-3246-476B-923F-F86E30B3E7F8}.**

Nota: es posible que aparezca el mensaje de error siguiente:
No se puede tener acceso a C:\System Volume Information. Acceso denegado.

Si aparece este mensaje, consulte el artículo siguiente en Microsoft Knowledge Base para ver las instrucciones de acceso a la carpeta y poder continuar con el procedimiento:

309531 How to Gain Access to the System Volume Information Fólder

Abra una carpeta que no se haya creado en este momento. Quizás tenga que hacer clic en Detalles en el menú Ver para mostrar la fecha y hora de creación de las carpetas. Bajo esta carpeta puede haber más de una subcarpeta que comience por "RP x. Se trata de puntos de restauración.

Abra una de las carpetas para localizar la subcarpeta Snapshot; la ruta de acceso siguiente es una ubicación de la carpeta Snapshot de ejemplo:

C:\System Volume Information_restore{D86480E3-73EF-47BC-A0EB-A81BE6EE3ED8}\RP1\Snapshot

Copie los archivos siguientes de la carpeta Snapshot a la carpeta C:\Windows\Tmp:

_REGISTRY_USER_.DEFAULT

_REGISTRY_MACHINE_SECURITY

_REGISTRY_MACHINE_SOFTWARE

_REGISTRY_MACHINE_SYSTEM

_REGISTRY_MACHINE_SAM

Éstos son los archivos de Registro de los que se hizo una copia de seguridad en Restaurar sistema. Como se utilizó el archivo de Registro creado por el programa de instalación, ese Registro no sabe que los puntos de restauración existen y están disponibles. Se crea una nueva carpeta con un nuevo GUID en System Volume Information, así como un punto de restauración que incluye una copia de los archivos del Registro copiados durante la parte uno. Esto se debe a que es importante no utilizar la carpeta más actual, especialmente si la marca de fecha y hora de la carpeta es la misma que la fecha y hora actual.

La configuración actual del sistema no conoce los puntos de restauración anteriores. Para que los puntos de restauración anteriores estén disponibles, se necesita una copia anterior del Registro efectuada desde un punto de restauración anterior.

Los archivos de Registro que se copiaron a la subcarpeta Tmp de la carpeta C:\Windows se mueven para garantizar que estén disponibles en la consola de recuperación. Necesita utilizar

esos archivos para reemplazar los archivos del Registro almacenados actualmente en la carpeta C:\Windows\System32\Config. De forma predeterminada, la consola de recuperación no tiene acceso a todas las carpetas y no puede copiar archivos de la carpeta System Volume.

Nota: en el procedimiento descrito en esta sección se asume que se ejecuta el sistema de archivos FAT32 en el equipo.

Parte tres

En esta parte, va a eliminar los archivos del Registro existentes y, después, va a copiar los archivos de Registro de restauración del sistema en la carpeta C:\Windows\System32\Config:

Inicie la consola de recuperación.

En el símbolo del sistema de la consola de recuperación, escriba las líneas siguientes y presione ENTRAR cuando finalice cada una de ellas:

del c:\windows\system32\config\sam
del c:\windows\system32\config\security
del c:\windows\system32\config\software
del c:\windows\system32\config\default
del c:\windows\system32\config\system
copy c:\windows\tmp_registry_machine_software c:\windows\system32\config\software
copy c:\windows\tmp_registry_machine_system c:\windows\system32\config\system
copy c:\windows\tmp_registry_machine_sam c:\windows\system32\config\sam
copy c:\windows\tmp_registry_machine_security c:\windows\system32\config\security
copy c:\windows\tmp_registry_user_.default c:\windows\system32\config\default

Nota: algunas de las líneas de comandos anteriores se han ajustado para que resulten legibles.

Nota: en este procedimiento se asume que Windows XP está instalado en la carpeta C:\Windows. Si se encuentra en una ubicación diferente, asegúrese de cambiar C:\Windows por la carpeta Windows apropiada.

Si tiene acceso a otro equipo, para ahorrar tiempo copie el texto del paso dos y, a continuación, cree un archivo de texto llamado CopiaReg1.txt, por ejemplo.

Parte cuatro

Haga clic en Inicio-> Todos los programas-> Accesorios ->Herramientas del sistema-> Restaurar sistema y en Restaurar mi equipo a un momento anterior.

Referencias

Para obtener información adicional acerca de Cómo utilizar la consola de recuperación

La información de este artículo se refiere a:
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional

COMO USAR LA FUNCION ÚLTIMA CONFIGURACION VALIDA CONOCIDA EN WINDOWS XP

Cómo usar la función Última configuración válida conocida en Windows XP.

La función Última configuración válida conocida es una opción de recuperación que puede usar para iniciar el equipo con la configuración más reciente que funcionó.

La función Última configuración válida conocida restaura la información del Registro y los valores de configuración del controlador que estaban en vigor en la última ocasión en que se inició el equipo con éxito.

Use la función Última configuración válida conocida cuando no pueda iniciar Windows XP después de hacer un cambio en el equipo o cuando sospeche que un cambio reciente puede causar un problema. Por ejemplo, puede usar esta configuración si no pudo iniciar Windows XP después de instalar un nuevo controlador para el adaptador de vídeo, o si instaló un controlador incorrecto, y no ha reiniciado el equipo.

Cuando inicia el equipo utilizando la última configuración válida conocida, Windows XP restaura la información en la siguiente clave del Registro:
HKEY_LOCAL_MACHINE\System\CurrentControlSet

Tenga en cuenta que cualquier otro cambio que se hiciera en las claves del Registro permanecerá.

Cómo iniciar su equipo con la Última configuración válida conocida

Para iniciar el equipo utilizando la última configuración válida conocida:

Inicie el equipo. Cuando vea el mensaje Seleccione el sistema operativo que desea iniciar, presione la tecla F8. Cuando se muestre el menú Opciones avanzadas de Windows, utilice las teclas de dirección para seleccionar Última configuración válida conocida (la configuración más reciente que funcionó) y, a continuación, presione Entrar.

Si está ejecutando otros sistemas operativos en el equipo, use las teclas de dirección para seleccionar Microsoft Windows XP y presione Entrar.

Solución de problemas

La función Última configuración válida conocida proporciona una manera de recuperarse de problemas de configuración, como controladores recién instalados que puedan ser incorrectos para el hardware de su equipo. No corrige problemas causados por archivos o controladores perdidos o corruptos. La función Última configuración válida conocida usa la información que se guardó la última vez que cerró el equipo para restaurar los controladores y la configuración del Registro.

Por ello, sólo puede usar esta función si pudo iniciar el equipo con éxito antes de restaurar el sistema utilizando la última configuración válida conocida. Después de iniciar el equipo utilizando la última configuración válida conocida, se pierden los cambios que se hicieron desde el último inicio.

La información de este artículo se refiere a:
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional

El arranque del ordenador y sus pitidos

Se explican el arranque del ordenador y las diferentes posibles causas de que nuestro ordenador emita ciertos pitidos al encenderse.

¿¿Que ocurre desde que le damos al botón de Power hasta que aparece nuestro sistema operativo cargando??

Cuando encendemos el ordenador, nuestra placa base hace una especie de escaneo a todo el sistema para comprobar si todo está en regla y continuar cargando.

Lo iremos marcando por pasos:

1. POWER, llega el voltaje a placa base
2. Seguidamente alimenta a los dispositivos de almacenamiento
3. El microprocesador, resetea todos los contadores y registros para partir de 0.
4. Busca una dirección de BIOS para testear la máquina, y también busca el test (Comprobación de dispositivos conectados)
5. POST (Power On Self Test): Son un conjunto de rutinas y programas que chequean el hardware.
   Aquí es donde se producen los pitidos que indican el estado del ordenador
6. La BIOS envía al micro señales y asigna canales DMA y IRQ
7. Inicializa la BIOS de la VGA
8. Testeo y cuenta de memoria
9. Habilita Teclado Led's y genera entradas
10. Busca el sector de arranque
11. Carga el boot manager y cede el control al sistema operativo.

Siempre que lo encendamos el modo que tiene la placa base de transmitir el estado del sistema es por medio de pitidos. Aquí tenemos algunos:

Ningún pitido: No hay suministro eléctrico (vamos que el cable está sin enchufar, el cable en sí falla, o la caja de suministro eléctrico está deteriorada, la cuestión es que no llega corriente) o también puede ser que el “Speaker”, lo que emite los pitidos, falle (lo podréis comprobar si a continuación funciona correctamente).

Tono continuo: Error en el suministro eléctrico (llega mal la corriente, o la caja de suministro esta fastidiada, no hay más que cambiarla).

Tonos cortos constantes: La placa madre está defectuosa, es decir, está rota, es de lo peor que nos puede ocurrir.

Un tono largo: Error de memoria RAM, lo normal es que esté mal puesta o que esté fastidiada.

Un tono largo y otro corto: Error el la placa base o en ROM Basic. Esto suele ocurrir mucho en placas base viejas, la gente las suele tirar.

Un tono largo y dos cortos: Error en la tarjeta gráfica. Puede que el puerto falle, por lo que no habría más que cambiarla de puerto, pero también puede ser que la tarjeta gráfica sea defectuosa.

Dos tonos largos y uno corto: Error en la sincronización de las imágenes. Seguramente problema de la gráfica.

Dos tonos cortos: Error de la paridad de la memoria. Esto ocurre sobretodo en ordenadores viejos que llevaban la memoria de dos módulos en dos módulos. Esto significaría que uno de los módulos falla, o que no disponemos de un número par de módulos de memoria.

Tres tonos cortos: Esto nos indica que hay un error en los primeros 64Kb de la memoria RAM.

Cuatro tonos cortos: Error en el temporizador o contador.

Cinco tonos cortos: Esto nos indica que el procesador o la tarjeta gráfica se encuentran bloqueados. Suele ocurrir con el sobrecalentamiento.

Seis tonos cortos: Error en el teclado. Si ocurre esto yo probaría con otro teclado. Si aun así no funciona se trata del puerto receptor del teclado.

Siete tonos cortos: Modo virtual de procesador AT activo.

Ocho tonos cortos: Error en la escritura de la video RAM.

Nueve tonos cortos: Error en la cuenta de la BIOS RAM.

Muchas veces nos suenan muchos de estos pitidos por cosas que no entendemos pero luego sigue funcionando con normalidad. En ese caso sería problema del detector de errores o de esa especie de escaneo que nos hace al encender el ordenador.

Que sistema de archivos escojer para instalar XP: NTFS, FAT o FAT32

Puede elegir entre tres sistemas de archivos diferentes para las particiones de disco en un equipo que ejecuta Windows 2000 -XP: NTFS, FAT y FAT32

El sistema recomendado es NTFS.

FAT y FAT32 son similares entre sí, excepto en que FAT32 está diseñado para discos de mayor tamaño que FAT. El sistema de archivos que funciona mejor con discos de gran tamaño es NTFS.

NTFS siempre ha sido un sistema de archivos más eficaz que FAT y FAT32.

Windows 2000 - XP incluye una versión nueva de NTFS, con compatibilidad para una gran variedad de características, incluido Active Directory, que es necesario para los dominios, cuentas de usuario y otras características de seguridad importantes.

El programa de instalación facilita la conversión de la partición a la nueva versión de NTFS, incluso si antes utilizaba FAT o FAT32. Este tipo de conversión mantiene intactos los archivos (a diferencia de cuando se da formato a una partición). Si no necesita mantener intactos los archivos y dispone de una partición FAT o FAT32, se recomienda que dé formato a la partición con NTFS en lugar de convertirla desde FAT o FAT32. El hecho de dar formato a una partición borra todos los datos de la partición, pero una partición a la que se da formato con NTFS en vez de convertirla desde FAT o FAT32 tendrá menos fragmentación y mejor rendimiento.

Sin embargo, sigue siendo más ventajoso utilizar NTFS, independientemente de si se dio formato a la partición con NTFS o se convirtió. Una partición también puede convertirse después de la instalación mediante Convert.exe. Para obtener más información acerca de Convert.exe, después de finalizar la instalación, haga clic en Inicio, haga clic en Ejecutar, escriba cmd y, a continuación,

presione Entrar, en la ventana de comandos, escriba help convert y, a continuación, presione Entrar.

Nota:
Únicamente puede utilizar características importantes como Active Directory y la seguridad basada en dominios si elige NTFS como el sistema de archivos.

Existe una situación en la que es posible que desee seleccionar FAT o FAT32 como sistema de archivos.

Si es necesario disponer de un equipo que a veces ejecute un sistema operativo de una versión anterior y otras veces ejecute Windows 2000-XP, deberá tener una partición FAT o FAT32 como partición principal (o de inicio) en el disco duro.

Esto se debe a que los sistemas operativos anteriores, con una excepción, no pueden tener acceso a una partición si utiliza la última versión de NTFS. La única excepción es Windows NT versión 4.0 con Service Pack 4 o posterior, que tiene acceso a particiones con la última versión de NTFS, pero con algunas limitaciones. Windows NT 4.0 no puede tener acceso a archivos que se han almacenado mediante características de NTFS que no existían cuando se publicó Windows NT 4.0.

Sin embargo, para cualquier otra situación en la que no existan varios sistemas operativos, el sistema de archivos recomendado es NTFS.

La tabla siguiente describe la compatibilidad de cada sistema de archivos con varios sistemas operativos.

	NTFS	FAT32	FAT
Windows XP	X	X	X
Windows 2000	X	X	X
Windows NT 4	X*	X	X
Windows NT			X
Windows 98		X	X
Windows 95 (OSR2)		X	X
OS/2			X
MS-DOS			X
Windows NT 4.0 uso NTFS 4. Windows 2000 y XP usan el más reciente NTFS 5.Windows NT 4.0 con Service Pack 4 puede accesar a algunos archivos, pero no a todos, en volumen NTFS 5.			

- Un equipo que ejecuta Windows 2000 puede tener acceso a los archivos de una partición NTFS.
- Un equipo que ejecuta Windows NT 4.0 con Service Pack 4 o posterior puede tener acceso a algunos archivos.
- Otros sistemas operativos no permiten el acceso.
- Es posible tener acceso a través de MS-DOS, todas las versiones de Windows, Windows NT, Windows 2000 y OS/2.

- Es posible tener acceso a través de Windows 95 OSR2, Windows 98 y Windows 2000.

La tabla siguiente compara el disco y los posibles tamaños de archivo con cada sistema de archivos.

	NTFS	FAT32	FAT
Tamaño Máximo de Volumen	2 TB	32 GB	4 GB
Tamaño Máximo de Archivo	Sin Límite	2 GB	4 GB
Drive de Compresión	SI	No	No
Servicio de Indexación	SI	No	No
Encriptación	SI	No	No
Controladores Montados	SI	No	No
Cuotas de Disco	SI	No	No
Dominios NT	SI	No	No
Directorio Activo	SI	No	No
	NTFS	FAT32	FAT

[*]TB es el standard para terabytes, un trillón de bytes, o aproximadamente 1,000 gigabytes.
[**]El tamaño máximo de archivo es igual al tamaño del volumen.

Lista de Puertos

0
ICMP
Click attack

19
UDP
Chargen

21
TCP
Detects if someone is trying to FTP to you.

23
TCP
Detects if someone is trying to Telnet to you.

25 *
TCP
Several trojans use this port.

31 *
TCP
Agent 31, Hacker's Paradise, Master's Paradise

41 *
TCP
Deep Throat

53
TCP
DNS

58 *
TCP
DM Setup

80 *
TCP
Executor

110 *
TCP
ProMail Trojan

121 *
TCP
Jammer Killah

129
TCP
Password Generator Protocol

137
TCP
Netbios name (DoS attacks)

138
TCP
Netbios datagram (DoS attacks)

139
TCP
Netbios session (DoS attacks)

456 *
TCP
Hacker's Paradise

555
TCP
Stealth Spy, Phaze

666

TCP
Attack FTP

1001 *
TCP
Silencer, WebEx

1011 *
TCP
Doly Trojan

1012 *
TCP
Doly Trojan

1024 *
TCP
NetSpy

1027
TCP
ICQ

1029
TCP
ICQ

1032
TCP
ICQ

1080
TCP
Used to detect Wingate sniffers.

1170 *
TCP
Voice Streaming Audio

1243
TCP
Sub Seven

1245 *
TCP
VooDoo Doll

1492 *
TCP
FTP99CMP

1981
TCP
Shockrave

1999 *
TCP
BackDoor

2001 *
TCP
Trojan Cow

2023 *
TCP
Ripper

2115 *
TCP
Bugs

2140 *
TCP
Deep Throat

2140
UDP
Deep Throat

2565 *
TCP
Striker

2583 *
TCP
WinCrash

2801 *
TCP
Phineas Phucker

2989
UDP
Rat

3024 *
TCP
WinCrash

3129 *
TCP
Master's Paradise

3150 *
TCP
Deep Throat

3150

UDP
Deep Throat

3389 3 *
TCP
See footnote 3 at the bottom of this table.

3700 *
TCP
Portal of Doom

4092 *
TCP
WinCrash

4590 *
TCP
ICQ Trojan

5000 2
TCP
Detects & blocks Sokets de Trois v1.

5001
TCP
Detects & blocks Sokets de Trois v1.

5400 *
TCP
Blade Runner

5401 *
TCP
Blade Runner

5402 *
TCP
Blade Runner

5569 *
TCP
Robo-Hack

5742 *
TCP
WinCrash

6400 *
TCP
The Thing

6670 *

TCP
Deep Throat

6711
TCP
Sub Seven

6712 *
TCP
Sub Seven

6713 *
TCP
Sub Seven

6771 *
TCP
Deep Throat

6776
TCP
Sub Seven

6939 *
TCP
Indoctrination

6969
TCP
Gate Crasher, Priority

6970 *
TCP
Gate Crasher

7000 *
TCP
Remote Grab

7300
TCP
Net Monitor

7301
TCP
Net Monitor

7306 *
TCP
Net Monitor

7307 *
TCP
Net Monitor

7308 *
TCP
Net Monitor

7789 *
TCP
ICKiller

9872 *
TCP
Portal of Doom

9873 *
TCP
Portal of Doom

9874 *
TCP
Portal of Doom

9875 *
TCP
Portal of Doom

9989 *
TCP
iNi-Killer

10067 *
TCP
Portal of Doom

10067
UDP
Portal of Doom

10167 *
TCP
Portal of Doom

10167
UDP
Portal of Doom

10520 *
TCP
Acid Shivers

10607 *
TCP
Coma

11000 *

TCP
Senna Spy

11223 *
TCP
Progenic Trojan

12076
TCP
GJamer

12223 *
TCP
Hack'99, KeyLogger

12345
TCP
Netbus, Ultor's Telnet Trojan

12346
TCP
Netbus

12456 *
TCP
NetBus

13000 *
TCP
Senna Spy

16969 *
TCP
Priority

20000
TCP
Millennium

20001
TCP
Millennium

20034 *
TCP
NetBus 2 Pro

21554
TCP
GirlFriend

22222 *
TCP
Prosiak

23456
TCP
EvilFTP, UglyFTP

26274 *
TCP
Delta Source

26274 *
UDP
Delta Source

29891 *
TCP
The Unexplained

30100
TCP
NetSphere

30101 *
TCP
NetSphere

30102
TCP
NetSphere

30303 *
TCP
Sockets de Troie

31337
UDP
Backorifice (BO)

31337
TCP
Netpatch

31338 *
TCP
NetSpy DK

31338
UDP
Deep BO

31339 *
TCP
NetSpy DK

31785
TCP
Hack'a'Tack

31789
UDP
Hack'a'Tack

31791
UDP
Hack'a'Tack

33333 *
TCP
Prosiak

40421
TCP
Master's Paradise – Hacked

40412 *
TCP
The Spy

40422
TCP
Master's Paradise – Hacked

40423
TCP
Master's Paradise – Hacked

40425
TCP
Master's Paradise – Hacked

40426 *
TCP
Master's Paradise

47252 *
TCP
Delta Source

47262 *
UDP
Delta Source

50505
TCP
Detects & blocks Sokets de Trois v2.

50776 *

TCP
Fore

53001 *
TCP
Remote Windows Shutdown

54320
TCP
Back Orifice 2000

54320 *
UDP
Back Orifice

54321 *
TCP
School Bus, Back Orifice

54321
UDP
Back Orifice 2000

60000 *
TCP
Deep Throat

61466 *
TCP
Telecommando

65000
TCP
Devil

Puertos de entrada

Master Paradise
31

BO jammerkillahV
121

Hackers Paradise
456

NeTadmin
555

Phase0
555

Stealth Spy

555

Attack FTP
666

AimSpy
777

Der Spaeher 3
1000

Der Spaeher 3
1001

Silencer
1001

Silencer
1001

WebEx
1001

Doly trojan v1.35
1010

Doly Trojan
1011

Doly trojan v1.5
1015

Netspy
1033

Bla1.1
1042

Wingate (Socks-Proxy)
(No es un troyano)
1080

Streaming Audio Trojan
1170

SoftWar
1207

SubSeven
1243

Vodoo
1245

Maverick's Matrix
1269

FTP99CMP
1492

Psyber Streaming Server
1509

Shiva Burka
1600

SpySender
1807

ShockRave
1981

Backdoor
1999

Transcout 1.1 + 1.2
1999

Der Spaeher 3
2000

Der Spaeher 3
2001

TrojanCow
2001

Pass Ripper
2023

The Invasor
2140

HVL Rat5
2283

Striker
2565

Wincrash2
2583

Phineas
2801

Total Eclypse 1.0

3791

FileNail
4567

IcqTrojan
4950

IcqTrojen
4950

OOTLT + OOTLT Cart
5011

NetMetro 1.0
5031

NetMetropolitan 1.04
5031

NetMetropolitan 1.04
5032

Firehotcker
5321

BackConstruction1.2
5400

BladeRunner
5400

Illusion Mailer
5521

Xtcp
5550

RoboHack
5569

Wincrash
5742

TheThing 1.6
6000

The tHing
6400

Vampire
6669

Deep Throath 1,2,3.x

6670

DeltaSource (
6883

Shitheep
6912

Indoctrination
6939

Gatecrasher
6969

NetMonitor
7306

ICQKiller
7789

InCommand 1.0
9400

PortalOfDoom
9872

Portal of Doom
9875

InIkiller
9989

iNi-Killer
9989

Coma
10607

Ambush
10666

Senna Spy Trojans
11000

ProgenicTrojan
11223

Gjamer
12076
Hack´99 KeyLogger

12223
NetBus 1.x (avoiding Netbuster)

12346
Eclipse 2000

12701
Priotrity

16969
Kuang2 theVirus

17300
Millenium

20000
NetBus Pro

20034
Chupacabra

20203
Logged!

20203
Bla

20331
GirlFriend

21554
Schwindler 1.82

21554
Prosiak 0.47

22222
UglyFtp

23456
WhackJob

23456
The Unexplained

29891
AOLTrojan1.1

30029
NetSphere

30100
Socket23

30303
Kuang

30999
Back Orifice (primer versión)

31337
NetSpy DK

31339
Hack'a'tack

31787
Trojan Spirit 2001 a

33911
BigGluck, aka TN

34324
Tiny Telnet Server

34324
TheSpy

40412
Master Paradise

40423
Fore, Schwindler

50766
Remote Windows Shutdown

53001
RemoteWindowsShutdown

53001
Schoolbus 1.6

54321
Schoolbus 2.0

54321
Telecommando

61466
Devil 1.03

65000
ShitHeep

69123
Back Orifice 2000

****** LISTA DE PUERTOS *******

echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
systat 11/tcp users
daytime 13/tcp
daytime 13/udp
netstat 15/tcp
qotd 17/tcp quote
chargen 19/tcp ttytst source
chargen 19/udp ttytst source
ftp-data 20/tcp
ftp 21/tcp
telnet 23/tcp te dice la version del sistema operativo
smtp 25/tcp mail Un tio jose@ctv.es. Pues poneis; telnet pop.ctv.es 25 -- luego, vrfy jose
time 37/tcp timserver
time 37/udp timserver
rlp 39/udp resource # resource location
name 42/udp nameserver
whois 43/tcp nicname # usually to sri-nic
domain 53/tcp
domain 53/udp
mtp 57/tcp # deprecated
bootps 67/udp # bootp server
bootpc 68/udp # bootp client
tftp 69/udp
gopher 70/tcp # gopher server
rje 77/tcp
#finger 79/tcp TEST
#http 80/tcp # www is used by some broken
#www 80/tcp # progs, http is more correct
link 87/tcp ttylink
kerberos 88/udp kdc # Kerberos authentication—udp
kerberos 88/tcp kdc # Kerberos authentication—tcp
supdup 95/tcp # BSD supdupd(8)
hostnames 101/tcp hostname # usually to sri-nic
iso-tsap 102/tcp
x400 103/tcp # x400-snd 104/tcp
csnet-ns 105/tcp
#pop-2 109/tcp # PostOffice V.2
#pop-3 110/tcp # PostOffice V.3
#pop 110/tcp # PostOffice V.3
sunrpc 111/tcp
sunrpc 111/tcp portmapper # RPC 4.0 portmapper UDP
sunrpc 111/udp
sunrpc 111/udp portmapper # RPC 4.0 portmapper TCP
auth 113/tcp ident # User Verification
sftp 115/tcp
uucp-path 117/tcp
nntp 119/tcp usenet # Network News Transfer
ntp 123/tcp # Network Time Protocol
ntp 123/udp # Network Time Protocol

#netbios-ns 137/tcp nbns
#netbios-ns 137/udp nbns
#netbios-dgm 138/tcp nbdgm
#netbios-dgm 138/udp nbdgm
#netbios-ssn 139/tcp nbssn
#imap 143/tcp # imap network mail protocol
NeWS 144/tcp news # Window System
snmp 161/udp
snmp-trap 162/udp
exec 512/tcp # BSD rexecd(8)
biff 512/udp comsat
login 513/tcp # BSD rlogind(8)
who 513/udp whod # BSD rwhod(8)
shell 514/tcp cmd # BSD rshd(8)
syslog 514/udp # BSD syslogd(8)
printer 515/tcp spooler # BSD lpd(8)
talk 517/udp # BSD talkd(8)
ntalk 518/udp # SunOS talkd(8)
efs 520/tcp # for LucasFilm
route 520/udp router routed # 521/udp too
timed 525/udp timeserver
tempo 526/tcp newdate
courier 530/tcp rpc # experimental
conference 531/tcp chat
netnews 532/tcp readnews
netwall 533/udp # -for emergency broadcasts
uucp 540/tcp uucpd # BSD uucpd(8) UUCP service
klogin 543/tcp # Kerberos authenticated rlogin
kshell 544/tcp cmd # and remote shell
new-rwho 550/udp new-who # experimental
remotefs 556/tcp rfs_server rfs # Brunhoff remote filesystem
rmonitor 560/udp rmonitord # experimental
monitor 561/udp # experimental
pcserver 600/tcp # ECD Integrated PC board srvr
mount 635/udp # NFS Mount Service
pcnfs 640/udp # PC-NFS DOS Authentication
bwnfs 650/udp # BW-NFS DOS Authentication
kerberos-adm 749/tcp # Kerberos 5 admin/changepw
kerberos-adm 749/udp # Kerberos 5 admin/changepw
kerberos-sec 750/udp # Kerberos authentication—udp
kerberos-sec 750/tcp # Kerberos authentication—tcp
kerberos_master 751/udp # Kerberos authentication
kerberos_master 751/tcp # Kerberos authentication
krb5_prop 754/tcp # Kerberos slave propagation
listen 1025/tcp listener RFS remote_file_sharing
nterm 1026/tcp remote_login network_terminal
#kpop 1109/tcp # Pop with Kerberos
ingreslock 1524/tcp
tnet 1600/tcp # transputer net daemon
cfinger 2003/tcp # GNU finger
nfs 2049/udp # NFS File Service
eklogin 2105/tcp # Kerberos encrypted rlogin
krb524 4444/tcp # Kerberos 5 to 4 ticket xlator
irc 6667/tcp # Internet Relay Chat

Explicación y definición de puertos para RED

echo (7/tcp,udp)
Se utiliza únicamente para depuración. Sin embargo, un atacante puede realizar "labores de depuración" creando bucles en la red a partir de este puerto (véase udp chargen/19).
BLOQUEAR.

systat (11/tcp/udp)
Muestra información acerca del host como usuarios conectados, carga del sistema, procesos en funcionamiento, etc...
BLOQUEAR.

chargen (19/tcp,udp)
Se utiliza únicamente para depuración. Basta con enviar un paquete a este puerto aparentemente originado en el puerto de echo (7/udp) para provocar un bucle en la red.
BLOQUEAR.

telnet (23/tcp,udp)
Vulnerable a "toma de sesiones". Es preferible utilizar en su lugar otras soluciones como SSH.

smtp (25/tcp,udp)
Históricamente la mayoría de las entradas en hosts han venido a través de este puerto. Se debe FILTRAR este puerto y mantener SIEMPRE la última versión estable conocida de cualquier programa de correo, especialmente si trabajamos con sendmail.

time (37/tcp,udp)
Devuelve la hora del sistema en un formato legible por la máquina (4 bytes mas o menos). Puede ser accedido tras un ataque vía ntp(123/tcp,udp).

nameserver (42/tcp,udp)
Si dispone de una red privada, debe instalar un servidor de nombres para ella. Bloquee el acceso a dicho servidor desde el exterior, y utilice siempre la última versión de BIND para resolver nombres. En este caso, puede cortar sin excesivos problemas el acceso al DNS sobre UDP.

tftp (69/tcp,udp)
Falta de autentificación. Bloquear si no se dispone de máquina alguna con arranque remoto.

private dialout (75/tcp,udp) - - - [RFC1700]
Si encontramos una traza de este puerto en los diarios del sistema (logs), en el mejor de los casos estaremos siendo analizados por un scanner de puertos.
BLOQUEAR.

finger (79/tcp,udp)
Puede obtenerse información acerca de usuarios concretos, información que puede utilizarse para adivinar claves de acceso. BLOQUEAR o SUSTITUIR por una política coherente de asignación de direcciones de correo (Juan Fernadez - - -> juan.fernandez@host.com) y un mensaje advirtiendo de dicha política.

http (80/tcp,udp)
¡¡¡Cuidado!!! Los servidores web son cada vez más complejos y permiten demasiadas cosas. Conviene redirigir el acceso a un puerto no privilegiado en maquinas unix. A ser posible, utilice servidores http específicos para la tarea a realizar (servir archivos, acceso a Bases de datos, etc...).

npp (92/tcp,udp) - [Network Printing Protocol]
Nadie quiere imprimir documentos ajenos ¿verdad?

objcall (94/tcp,udp) - [Tivoli Object Dispatcher]
Utilizado por la herramienta de Gestión de redes Tivoli. Si utilizamos tivoli, aplicar las mismas precauciones que con SNMP.

sunrpc (111/tcp,udp)
Especialmente peligroso sobre UDP. No autentifica fuentes, y es la base para otros servicios como NFS.

auth (113/tcp,udp)
No debería permitirse obtener información acerca de puertos privilegiados (puede utilizarse para realizar un portscan). No se utiliza mas que en Unix.

ntp (123/tcp,udp) [Network Time Protocol]
Se utiliza para sincronizar los relojes de las máquinas de una subred. Un ejemplo de ataque clásico consiste en enviar paquetes a este puerto para distorsionar los logs de la máquina.

netbios (137,138,139/tcp,udp)
No dispone de suficiente autenticación. Afortunadamente según los RFC2001 y 2002 NetBIOS es capaz de funcionar correctamente a pesar de que se estén enviando bloques de datos con información errónea o corrompida.

snmp (161/tcp,udp) –
¿Quién puede querer administrar nuestra red desde el exterior? Se puede obtener mucha información a través de este servicio, como por ejemplo estado de los interfaces de red, conexiones concurrentes en la máquina, etc...
BLOQUEAR.

snmp-trap (162/tcp,udp)
Traps de SNMP. A través de este puerto se realizan solicitudes que pueden cambiar la configuración del host.
BLOQUEAR.

irc (194/tcp,udp) –
No es peligroso en sí; sin embargo sus usuarios suelen divertirse atacando los hosts de otras personas con el fin de echarlos cuando no pueden hacer uso de la orden 'kick'. Generalmente conviene bloquear los puertos 6666, 6667 y 6668 ya que son a los que se enganchan los servidores de IRC.

exec (512/tcp)
Ejecuta ordenes en estaciones remotas. Como todos los comandos 'r' (rexec, rcp, rlogin) en la otra partes cuando se accede desde un conjunto de direcciones IP definidas por el usuario. No se realiza más autentificación que la basada en dirección IP y usuario remoto. MUY PELIGROSO (aunque muy potente).
BLOQUEAR.

biff (512/udp)
Notifica de la llegada de correo. Buen candidato para posibles desbordamientos de buffer, o simplemente para obligar a abandonar la sesión a un usuario debido a la llegada masiva de mensajes de correo. (biff suele funcionar incluso con mesg n)
BLOQUEAR.

login (513/tcp) - rlogin. (ver exec)
BLOQUEAR.

who (513/udp)
Muestra quien está utilizando el host remoto. Se puede obtener información bastante detallada acerca de quién utiliza una máquina y desde que terminal, uptime (tiempo que lleva en funcionamiento), carga de la máquina, etc...
BLOQUEAR.

cmd (514/tcp) –
Similar a exec (512/tcp), mismas precauciones.
BLOQUEAR.

syslog (514/udp)
BLOQUEAR a menos que existan suficientes razones como para mantenerlo. Suele atacarse para corromper los diarios (logs) del sistema con entradas falsas.

printer (515/tcp,udp)
router (520/tcp,udp) - Local routing process.
BLOQUEAR

ingreslock (1524/tcp) –
En la mayoría de los Un*x se puede encontrar esta entrada en /etc/services. Ya que está dado de alta y es un puerto no privilegiado es un buen lugar para una puerta trasera (no sería la primera vez que ocurre).

Las 50 herramientas de seguridad más utilizadas

Según una encuesta hecha por Insecure.com a 1200 usuarios del NMAP en su lista de correo, las herramientas de seguridad preferidas e independientemente de la plataforma, son las siguientes:

Ordenadas empezando por la más popular, se agrupan utilidades como scanners, sniffers y demás programas de seguridad. Se incluye el enlace para descargarlas y una breve explicación sobre su uso y/o utilidad teniendo en cuenta que hay algunas que no conocía.
*
Nessus (http://www.nessus.org): este programa es un scanner de seguridad empleado para hacer más de una auditoría en busca de vulnerabilidades. Consta de dos partes, cliente y servidor (nessusd) con versiones para Windonws, Java y Unix (la parte cliente) y sólo para Unix el servidor. El servidor /daemon realiza los ataques mientras que el cliente interactúa con el usuario a través de un interface gráfico. Pros: desarrolla una completa exploración de todos los puertos y servicios y presenta los puntos vulnerables que encuentra y sus posibles soluciones. Contras: es un poco lento. Como comentario decir que es comparable al Retina.
*
Netcat (http://www.atstake.com/research/tools/nc11nt.zip): esta sencilla utilidad para Windows y Unix sirve para escuchar y analizar las conexiones de red usando los protocolos TCP o UDP. Se ha usado bastante para explotar el bug del Isapi en los servidores IIS (ref. Desbordamiento de búfer en el IIS del 21 de junio).
*
TCPDump (http://www.tcpdump.org): este sniffer para Unix sirve para monitorizar todo el tráfico de una red, recolectar toda la información posible y detectar así posibles problemas como ataques ping. Combinado con SNORT se convierte en una poderosa herramienta solventando las carencias que ambos porgramas tienen por separado. Es curioso porque podemos servirnos del

propio TCPDump para evadir IDSs de los que forma parte porque presenta una vulnerabilidad en las capacidades de decodificación de DNS y puede entrar en un loop infinito que nos permita saltarnos ese IDS (Sistema de Detección de Intrusos).
*

Snort (http://www.snort.org): sniffer/logger, Snort sirve para detectar intrusiones y ataques tipo búfer overflows, CGI, SMB, scanneo de puertos, etc. Snort puede enviar alertas en tiempo real, enviándolas directamente al archivo de Unix syslog o incluso a un sistema Windows mediante SAMBA. Las versiones anteriores a la 1.8.1 presentan una vulnerabilidad en la codificación Unicode que posibilita que un atacante evada dicha detección.
*

Saint (http://www.wwdsi.com/saint): Security Administrator's Integrated Network Tool (SAINT) es una evolución del conocido SATAN para plataformas Unix que sirve para evaluar toda la seguridad de un sistema recibiendo incluso múltiples updates desde el CERT y CIAC.
*

Ethereal (http://ethereal.zing.org): este sniffer de red para Unix tiene un entorno gráfico y soporta decodificación de diversos protocolos pero presenta una vulnerabilidad de búfer overflow (versiones anteriores a la 0.8.14).
*

Whisker (http://www.wiretrip.net/rfp/bins/whisker/whisker.zip): buen scanner de vulnerabilidades CGI.
*

ISS (http://www.iss.net): Internet Security Scanner es una herramienta comercial de análisis de vulnerabilidades para Windows.
*

Abacus Portsentry (http://www.psionic.com/abacus/portsentry): demonio de Unix para detectar scanneos de puertos contra nuestros sistemas capaz de bloquear al atacante mediante host.deny, filtrar las rutas o reglar el firewall.
*

DSniff (http://naughty.monkey.org/~dugsong/dsniff): el nombre ya lo dice todo... este es un sniffer para buscar passwords y el resto de información de una red incluyendo técnicas sofisticadas para defender la "protección" de los switchers de red.
*

Tripwire (http://www.tripwire.com): esta es una utilidad para el análisis de red que sirve de gran ayuda a los adminsitradores de red.
*

Cybercop (http://www.pgp.com/products/cybercop-scanner/default.asp): este es un scanner de agujeros de seguridad comercial que tiene versiones para Windows y Unix y que es capaz de auditar servidores, estaciones de trabajo, hubs, routers, firewalls, etc.
*

Hping2 (http://www.hping.org): este programa basado en el comando ping de Unix sirve para enviar paquetes ICMP,UDP y TCP hechos a medida para mostrar las respuestas del obejtivo como replicas ICMP echo (ping). Con hping conseguimos testar firewalls, scannear puertos, etc. Nota: ICMP (Protocolo de Mensajes de Control Internet).
*

SARA (http://www-arc.com/sara): Security Auditor's Research Assistant es la tercera generación de herramientas para el análisis de seguridad en plataformas Unix. La primera fue el SATAN (Security Administrator's Tool for Analizing Networks) y la segunda el SAINT.
*

Sniffit (http://reptile.rug.ac.be/~coder/sniffit.html): otro sniffer de paquetes TCP/UDP e ICMP capaz de obtener información técnica muy detallada.
*

SATAN (http://www.fish.com/satan): hace falta decir algo sobre el más famoso scanneador de vulnerabilidades y analizador de red.
*

IPFilter (http://coombs.anu.edu.au/ipfilter): este es un filtro de paquetes TCP/IP indicado para el uso con un firewall en plataformas Unix. Puede trabajar como un módulo cargable del kernel o incorporado en él directamente. Curiosamente, las versiones previas a la 3.4.17 presentan una vulnerabilidad que permite alcanzar puertos TCP y UDP teóricamente protegidos.
*

IPtables/netfilter/ipchains/ipfwadm (http://netfilter.kernelnotes.org): herramientas para filtrar los paquetes IP bajo Linux.
*

Firewalk (http://www.packetfactory.net/Projects/Firewalk): programa para analizar las respuestas a los paquetes IP con la técnica del Firewalking con una interface gráfica (opcional) para determinar los filtros ACL de los gateways y los mapeos de red.
*

Strobe (http://www.insecure.org/nmap/index.html#other): scanneador de puertos de gran velocidad.
*

L0pht Crack (http://www.l0pht.com/l0phtcrack): Esta es la conocida herramienta de auditoría para los passwords bajo Windows. La última versión es la LC3.
*

John the Ripper (http://www.openwall.com/join): esta es una de esas utilidades que, yo por lo menos, recuerdo de toda la vida. Es uno de los programas que yo utilizaba cuando empecé a hacer mis primeros pinitos en esto del hack y la verdad es que era el mejor crackeador de passswords para Unix.
*

Hunt (http://www.cri.cz/kra/index.html#HUNT): este es un sniffer avanzado que funciona bajo redes ethernet pero que no conocía así que poca cosa puedo decir.
*

SSH (http://www.ssh.com/commerce/index.html): Tenemos dos opciones usar el SSH que es de pago o utilizar en cambio el OpenSSH que es una evolución del ssh para OpenBSD. SSH o Secure Shell, es un protocolo o programa que se sirve de dicho protocolo, que permite una conexión cifrada y protegida entre dos máquinas (normalmente cliente servidor) que sirve para substituir al telnet y poder acceder y administrar sistemas remotos de manera segura.
*

TCP Wrappers (ftp://ftp.porcupine.org/pub/security/index.html): pequeños programas que permiten una conexión controlada, restringiendo determinados servicios del sistema. Se pueden monitorizar y filtrar las peticiones de entrada de servicios como Systar, Finger, FTP, Telnet, Rlogin, RSH, TFTP, etc. El wrapper reporta el nombre del cliente y del servicio que ha solicitado pero no intercambia información con el cliente o el servidor de la aplicación/servicio solicitado porque lo que hace es comprobar si el cliente tiene permiso para utilizar el servicio que está pidiendo y si no es así, corta la conexión.
*

NTOP (http://www.ntop.org): utilidad para Unix que permite visualizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto. Tiene como un microservidor web que permite que cualquier usuario que sepa la clave pueda ver la salida NTOP de forma remota con cualquier navegador.
*

Traceroute/ping/telnet (http://www.linux.com): herramientas de Unix y Windows (en este sistema operativo el comando treceroute se denomina tracert).
*

NAT (http://www.tux.org/pub/security/secnet/tools/nat10): NetBios Auditing Tool sirve para explorar los recursos compartidos a través del protocolo NetBios en un sistema windows.
*

Scanlogd (http://www.openwall.com/scanlogd): programita que detecta los scanneos de puertos que alguien pueda hacer contra tu sistema.
*

Sam Spade (http://www.samspade.org): herramientas online para investigar una dirección IP y encontrar spammers.
*

NFR (http://www.nfr.org): Network Flight Recorder es un sniffer comercial para detectar intrusiones en los sistemas.
*

Logcheck (http://www.psionic.com/abacus/logcheck): es parte del proyecto Abacus de utilidades de seguridad que ayuda a mostrar los problemas y violaciones de seguridad en los archivos log del sistema, analizando cada línea y clasificándola según diferentes niveles de alerta (ignorar, actividad inusual, violación de seguridad y ataque) para luego enviar los resultados al administrador por e-mail.
*

Perl (http://www.perl.org): Practical Extraction and Report Language es un lenguaje de scripts que corre en cualquier sistema operativo y que sirve, entre otras múltiples cosas, para crear exploits y explotar las vulnerabilidades de los sistemas.
*

Ngrep (http://www.packetfactory.net/Projects/ngrep): herramienta sensible a pcap que permite especificar expresiones regulares extendidas contra la carga de datos de los paquetes. Actualmente reconoce TCP, UDP e ICMP sobre ethernet a través de PPP, SLIP e interfaces nulos.
*

Cheops (http://www.marko.net/cheops): sirve para mapear redes locales o remotas y muestra qué Sistema Operativo (SO) tienen las máquinas de la red.
*

Vetescan (http://www.self-evident.com): es un scanneador de vulnerabilidades que contiene programas para comprobar y/o explotar exploits conocidos de redes para Windows y Unix y corregirlos.
*

Retina (http://www.eeye.com/html/Products/Retina.html): este programa es un conocido scanneador de vulnerabilidades que es comercial y que incluye la forma de arreglar todos los agujeros de seguridad que encuentre. Es para Windows.
*

Libnet (http://www.packetfactory.net/libnet): conjunto de rutinas para la construcción y guía de una red.
*

Crack (ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack/): este programa es un password cracker.
*

Cerberus Internet Scanner (http://www.cerberus-infosec.co.uk/cis.shtml): CIS es otro scanner de seguridad destinado a ayudar a los administradores de red de Windows a detectar y corregir agujeros de seguridad.
*

Swatch (http://www.stanford.edu/~atkins/swatch): utilidad para monitorizar los mensajes de los archivos log de Unix mediante el comando syslog lanzando eventos con múltimples métodos de alarma.
*

OpenBSD (http://www.openbsd.org): OpenBSD es una distribución libre de sistemas Unix multiplataforma basada en 4.4BSD. OpenBSD incluye emulación de binarios para la mayoría de los programas de los sistemas SVR4 (Solaris), Linux, SunOS, HP-UX, etc e incluye también OpenSSH con soporte para SSH1 y SSH2.
*

Nemesis (http://www.packetninja.net/nemesis).
*

LSOF (http://vic.cc.purdue.edu/pub/tools/unix/lsof): herramienta de diágnostico de sistemas Unix que lista la información de cualquier archivo que es abierto por un proceso que se esté ajecutando. Muy útil para detectar troyanos y sniffers.
*

LIDS (http://www.turbolinux.com.cn/lids): este es un sistema de detección/defensa para Linux contra intrusiones de root deshabilitando algunas llamadas del sistema al kernel.
*

IPTraf (http://www.mozcom.com/riker/iptraf): monitor de red que genera multitud de estadísticas como información TCP, contador UDP, información ICMP y OSPF, estado de los nodos, errores IP, etc.
*

IPLog (http://ojnk.sourceforge.net): logger del tráfico TCP/IP, UDP e ICMP que detecta scanneos y posibles ataques para sistemas Unix.
*

Fragrouter (http://www.anzen.com/research/nidsbench): ni idea.
*

QueSO (http://www.apostols.org/projects/queso): utilidad para averiguar qué Sistema operativo corre en una máquina remota analizando las respuestas TCP. Funciona bajo Unix (Linux) y algunas de sus pruebas de detección han sido incluidas al famoso programa NMAP.
*

GPG/PGP (http://www.gnupg.org y http://www.pgp.com): substituto del PGP con licencia GNU desarrollado en Europa que no utiliza ni el algoritmo RSA ni IDEA y que por ello no tiene ningún tipo de restricción. PGP o Pretty Good Privacy es el famoso sistema de encriptación que ayuda a asegurar y codificar la información contra posibles "escuchas".

TRUCOS PARA MESSENGER

Como poner un Nick vacío

Si te haz dado cuenta cada vez que deseas dejar tu Nick en blanco no se puede, para que esto no te pase de nuevo haz lo siguiente; donde se escribe el Nick dejando presionada la tecla Alt escribes con el teclado numérico 0160, verás como se crea un vacío en tu Nick.

Evitar conversaciones con personas que no tenemos en la lista

Abre el menú Herramientas del MSN, pulsa en Opciones, se te abre una ventanita, pulsa en Privacidad, y ahora en la lista de personas que pueden ver nuestro estado de conexión, seleccionamos "Los demás usuarios" y pulsamos en No admitir.

Enviar un mensaje a alguien que te tenga omitido

Primero, hay que ponerle a la persona que nos omite Sin Admisión. Ahora, lo que hay que hacer es ponernos como Nick el mensaje que queremos mandarle. Y por último, lo volvemos a admitir. Desde luego que no podremos hablar con él, pero le saldrá al momento una ventanita con nuestro Nick (que en realidad será el mensaje que queramos decirle) diciendo que acabamos de iniciar sesión. Por que lo hemos omitido primero?? porque así el mensaje solo le saldrá a el, y no a toda la lista de contactos, al Admitirlo de nuevo, solo le saldrá a el la ventanita.

Cambiar de línea en la ventana del chat

Si te das cuenta que cada vez que queremos escribir en una línea nueva presionamos enter y la tenemos, pero en el MSN al hacerlo nos envía el mensaje sin querer, para poder cambiar la línea solo debemos tener presionado SHIFT y la tecla Enter.

Chatear con alguien sin necesidad de agregarlo a tu lista

Pones el mail de una persona que tenga MSN y puedes chatear con ella sin tener que agregarla a la lista. Es perfecto para evitar que nos añadan a nosotros, o para evitar que a la otra persona le

salga el mensajito de que alguien la ha añadido al MSN, ideal para bromas...

Cambiar la frase que dice "No revele contraseña...." al comenzar una conversación

Para poder cambiar esta frase debemos ir a INICIO-EJECUTAR ahí tipeamos REGEDIT presionamos ENTER, se abrirá una nueva ventana y seguimos estas opciones:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService\Policies

Luego sobre la cadena "IMWarning" hacemos click derecho y damos en modificar, nos aparecerá la famosa frase y escribiendo cualquier otra sobre esta ¡ya estará hecho!, verás que fácil que es.

Cambiar imagen de fondo

Esta imagen se encuentra dentro de la carpeta donde tengamos instalados el mensajero, generalmente esta dentro de: C:/Archivos De Programa/Messenger dentro de esta carpeta existe una imagen llamada lvback.gif, que es la que contiene la imagen que se encuentra de fondo, 160x140 pixeles generalmente aunque no se confíen de este dato...prueben, abranla en el paint o en alguno parecido y miren, luego solo basta con crear una imagen de igual tamaño y reemplazarla con el mismo nombre, antes hacer un backup (resguardo) de la imagen.

Cambiar sonidos en Msn

Bien, si queremos cambiar los sonidos que trae por defecto el mensajero solo basta con ir a MI PC->PANEL DE CONTROL->SONIDOS, allí veremos una lista de eventos, debemos encontrar una llamada: MSN MESSENGER y allí hacemos los cambios que creamos necesarios.

Quitar Windows Messenger de XP

A veces nos resulta molesto el windows messenger que viene en xp o queremos instalar otra versión, bueno lo que debemos hacer es esto: Haz click en el botón Inicio y selecciona Ejecutar. Teclea RunDll32 advpack.dll,LaunchINFSection %windir%\INF\msmsgs.inf,BLC.Remove en la caja de diálogo y clickea en OK. Aparecerá una barra de progreso donde puedes seguir el proceso de desinstalación. Es posible que te pida reiniciar el equipo. Si es así, lo reinicias.

Averiguar la IP de la persona con la que hablas

Es muy sencillo, solo tienes que enviar un archivo a esta persona (o que te lo envíe ella a ti) puedes enviar cualquier cosa, pon alguna excusa buena bueno la cuestión es que cuando se esté transfiriendo el archivo, vas al MS-DOS y escribes: c:\netstat -a Te saldrán una serie de ip's y servidores, pero no te será dificil reconocer la Ip de tu amigo. Para reconocerla mas fácilmente, intenta no tener paginas web abiertas, ya que de esta forma te saldrán mas Ip's y te será mas dificil encontrarla.

Si escribes: c:\netstat -a > archivo.txt te creará un archivo.txt con el contenido del netstat, aso lo podrás analizar más fácilmente.

Guardar lista de contactos

Hay una opcion en el MSN que poca gente la ha visto, y es bastante útil cuando nos hacemos una cuenta nueva y queremos añadir todos los contactos que teníamos en la otra. Para ello, solo tienes que ir a: >>Archivo >>Guardar Lista de Contactos se guardara un archivo con todos tus contactos y sus direcciones, para recuperar esa lista de contactos en otra cuenta que tengas, solo tienes que ir a: >>Archivo >>Importar contactos de un archivo y aqui, seleccionas el archivo que guardaste antes!!

Ventana sin datos (ni mail, ni nick...)

Con este truco puedes hacer que al abrir una ventana de chat a alguien este no sepa con quien habla ya que no le aparece arriba el mail ni el nick, jeje. Se hace de la siguiente manera: En el menú de cambiar el nick, escribes lo siguiente, mantienes pulsada la tecla ALT y luego presionas los números 0160 del teclado numérico (ALT+0160) se creará un "vació" en blanco,

ahora seleccionas ese "vació" con el ratón, y haces COPIAR, y luego lo PEGAS muchísimas veces más en el nick hasta que te canses jeje (puedes hacer Ctrl+C para copiar, y Ctrl+V para pegar).

Escribir mensaje en dos colores y fuentes distintas

1. mantenemos pulsado alt y tecleamos 3012
2. soltamos alt y escribimos
3. mantenemos pulsado shift y pulsamos intro
4. repetimos el paso nº1 y nº2 y mandamos el mensaje

En vez de escribir 3012 podemos usar:4562, 85421, 1478, 3692 e incluso en el paso 1 poner uno de los numeros y en el paso 4 poner otro.
¿Que hace? pues bien, el primer texto que escribimos sale con la letra y el color que tengamos puesto, el segundo texto saldra en negro y la letra depende del numero que usemos.

Encriptar tus conversaciones con el Messenger

Seguro que estas cansado de ver cada vez que inicias una nueva conversación, un aviso de Microsoft advirtiéndote:"Nunca revele sus contraseñas o números de tarjetas de crédito en una conversación de mensajes instantáneos."

Desde luego ésto da qué pensar... así que vamos a explicar una forma de conseguir mejorar un poco la seguridad de nuestras conversaciones.

Tanto si nos conectamos a una red local (y no queremos que el administrador de la red, lea nuestras coversaciones), como si nos conectamos desde nuestro pc directamente a la Red (y queremos evitar que un hacker intercepte de forma limpia nuestros mensajes y pueda leerlos fácilmente) vamos a utilizar un programa que les hará más difícil entender una coversación: vamos a encriptarla.

Para conseguirlo, vamos a utilizar SPYSHIELD un accesorio para Msn Messenger que es compatible con PGP.

El PGP (Pretty Good Privacy ó Encriptación bastante buena) es un sistema de encriptación por llave pública escrito por Philip Zimmermann, y sirve para que nadie salvo uno mismo y el destinatario o destinatarios a los que vaya dirigido el mensaje puedan leerlo, al ir los mensajes codificados.

También puede usarse para comprobar la autenticidad del mensaje asegurándonos que lo ha escrito el remitente en realidad, realmente es muy bueno y es prácticamente indescifrable.

El funcionamiento es muy sencillo, cada usuario tiene dos llaves una pública y otra privada, la pública es la que distribuye a la gente y sirve para que ellos puedan enviarle un mensaje codificado que solo él mediante su llave privada podrá descifrar, también puede servir para firmar un mensaje poniendo una parte de su llave privada (irreconocible claro) en una firma, esto es como un certificado de autenticidad, ya que al recibir el mensaje el PGP comprueba la firma y texto y lo compara con la llave pública que tenemos del remitente dando un error si se ha cambiado algo en el texto o la firma no corresponde a la persona que nos envía el mensaje.

Sirve también para enviar ficheros a través de correo electrónico codificados en formato ascii y mucho mejor que otros sistemas como el uuencode ya que el PGP usa antes de codificar una compresión zip al documento o programa que va a codificar.

Tienes toda la información que quieras sobre este tema en la web en castellano _http://pagina.de/pgp

Es importante saber, que el SPYSHIELD parece no fucionar con las nuevas versiones del PGP, así que tenéis que aseguraros que instaláis la versión de PGP 6.5.8. Todo esto lo tenéis disponible en la sección accesorios de esta web.

Modificar el historial de usuarios en MSN Messenger

Precisamente en esta oportunidad presentaré un truco que permite eliminar nuestra dirección de correo electrónico de la lista de direcciones de correo que aparece en el historial de MSN Messenger de Microsoft®, logrando de esta manera mantener privada nuestra dirección cuando iniciamos sesión en algún MSN Messenger de un Cybercafé, Universidad, o cualquier centro de computación público.

El problema principal es que al iniciar sesión nuestra dirección de e-mail (que deseamos mantener privada) queda almacenada automáticamente y el próximo usuario que haga uso de la PC podrá observar nuestro email.

Para lograr este truco se deben seguir los siguientes pasos:

1. Hacer click en "Inicio", luego en "Ejecutar"
2. Escribir en la caja de texto: control userpasswords2
3. Luego, al presionar el botón Aceptar aparecerá la ventana de "Cuentas de usuario"
4. Posteriormente se selecciona la pestaña "opciones avanzadas"
5. Hacer click en "Administrar contraseñas" y luego seleccionar la dirección que deseamos mantener privada.
6. Ahora se presiona el botón "Quitar"

ATAJOS DEL TECLADO PARA INTERNET

Bueno la idea es dejar estos atajos de teclado y los que sepan mas los van dejando abajo, espero que les sean de utilidad.

Internet Explorer:

- Ctrl + R: Actualiza la página actual.
- Ctrl + O: Abre la ventana Organizar Favoritos.
- Ctrl + P: Abre la ventana Imprimir.
- Ctrl + D: Agrega la página actual a Favoritos.
- Ctrl + F: Abre el cuadro Buscar en esta Página.
- Ctrl + H: Abre la barra Historial.
- Ctrl + I: Abre la barra Favoritos.
- Ctrl + Tab: Avanzar entre marcos.
- Ctrl+ F5: Forzar actualización.
- Mays + Crtl + Tab: Retroceder entre marcos.
- Mays + F10: Mostrar menú contextual de vínculo.
- Mays + F1: Abre el índice de ayuda.
- F11: Abre el explorador a pantalla completa.
- F4: Muestra la lista de direcciones.
- Alt + Flecha derecha: Ir a la página siguiente en el historial.
- Alt + Flecha izquierda: Ir a la página anterior en el historial.
- Ctrl + L: Va a una nueva ubicación.

Opera:

Gestión de documentos

- CTRL+O Leer documento del disco local
- CTRL+S Grabar el documento activo
- CTRL+P Imprimir el documento activo
- CTRL+F3 Ver código fuente del documento en HTML
- ALT+F3 Ver código fuente del frame en HTML

Navegando y visualizando

- Q o CTRL+Up Enlace previo en un documento
- A o CTRL+Down Próximo enlace en un documento
- Z o CTRL+Left o ALT+Left Documento anterior en el historial
- X o CTRL+Right o ALT+Right Documento siguiente del historial
- F7 Activa la lista de marcadores para la navegación con el teclado
- F8 Ir al campo de dirección URL
- F9 Restore focus on current window
- ESC Detiene la carga del documento en la ventana activa
- F5 o CTRL+R Recargar documento
- ALT+F5 Recargar frame
- Enter or Space Carga documento bajo el link activo
- SHIFT+Enter or SHIFT+Space Carga documento bajo el link activo en una nueva ventana
- SHIFT+CTRL+Enter or SHIFT+CTRL+Space Carga documento bajo el link activo en una nueva ventana de fondo
- G Toggle the graphic loading of the active window between: load and show all graphics; show only loaded graphics; don't show any graphics
- CTRL+G Toggle the display between document and user settings. Very helpful for badly legible pages.
- CTRL+M Display local window menu
- CTRL+L Visualiza el menú para el link elegido
- W/S Jump between all headers
- E/D Jump between all elements

Hot List and Direct Access

- CTRL+Home o CTRL+Space Go to the homepage (window's homepage if defined, or the global homepage)
- F2 Display direct addressing window / Enter URL directly
- SHIFT+F2 Activate the nickname window for quick Hot List access
- CTRL+F2 o SHIFT+F7 Hide/Display the Hot List window
- F7 Activate the Hot List for keyboard navigation
- CTRL+M Activate the Hot List menu
- CTRL+T Add active document to the (sub)folder
- Tab Jump between elements in (sub)folder
- Alt+Enter Open the items or (sub)folder's properties dialog box
- CTRL+X Cortar
- CTRL+C Copiar
- CTRL+V Pegar

Sup Suprimir la entrada de la lista

- CTRL+A Selecciona todas las entradas de la lista
- ALT+1 Change sort order on Hot List 'Title' column (toggle)

- ALT+2 Change sort order on Hot List 'Last Visited' column (toggle)
- ALT+3 Change sort order on Hot List 'Created' column (toggle)
- F8 Ir al campo de dirección URL
- H Visualiza el histórico para la ventana activa window
- CTRL+J Opens 'Links in Frame' dialog box

Editando y buscando
- CTRL+C Copia el texto marcado
- CTRL+X Corta el texto marcado del área de texto
- CTRL+V Pegar
- CTRL+A Selecciona todo el texto
- F3 Busca en el documento activo

Scrolling
- Flecha arriba Una línea hacia arriba
- Flecha abajo Una línea hacia abajo
- Flecha izquierda Un carácter a la derecha
- Flecha derecha Un carácter a la izquierda
- Av Pág Una ventana abajo
- Re Pág Una ventana arriba
- CTRL+Av Pág Ventana a la izquierda
- CTRL+Re Pág Ventana a la derecha
- CTRL+F7 Oculta / muestra la barra de scroll

Zoom
- + o 0 Aumenta el zoom un 10%
- - o 9 Disminuye el zoom un 10%
- 6 or * Restaura el zoom al 100%
- 7 o CTRL+"+" Disminuye el zoom un 100%
- 8 o CTRL+"-" Aumenta el zoom un 100%

Lector de noticias o News overview window
- I Subscribe o cancela una subscripción a un grupo
- CTRL+Up o Q Va al grupo anterior
- CTRL+Down o A Va al grupo siguiente
- Intro Abre o cierra un grupo de un grupo de temas o artículos

Single Group window
- K Marca un artículo en una ventana de grupo como leido o sin leer
- Enter Recupera un artículo
- Q o CTRL+Up Va al artículo anterior
- A o CTRL+Down Va al siguiente artículo
- PageUp Scroll one window up in article window
- PageDown Scroll one window down in article window
- U Read previous article
- J Read next article
- V Post a new news article
- T Post a followup news article
- R Reply to the person who posted the article
- F Forward the article via e-mail

Gestión de ventanas

- SHIFT+F5 Coloca las ventanas en cascada
- SHIFT+F6 Coloca las ventanas en mosaico verticamente hasta rellenar el espacio de trabajo
- F6 Coloca las ventanas en mosaico horizontalmente hasta rellenar el espacio de trabajo
- 1 o SHIFT+CTRL+TAB Cambia a la ventana anterior
- 2 o CTRL+Tab Cambia a la siguiente ventana
- CTRL+F7 Oculta/visualiza la barra de "scroll"
- CTRL+F8 Oculta/visualiza la barra de "progreso"
- F11 Oculta la barra de título de la ventana de Opera
- CTRL+F11 Oculta/visualiza la barra de munú principal (File | Edit | View)
- 3 Frame siguiente
- 4 Minimiza la ventana actual
- 5 Maximiza la ventana actual
- CTRL+W Cierra la actual ventana

Ayuda

- F1 Visualiza el fichero de ayuda cuyo contenido depende del contexto
- CTRL+B Visualiza la página de atajos de teclado

Firefox:

- Volver una Página Shift+Scroll down
- Achicar tamaño de letra Ctrl+Scroll up
- Adelandar una Pagina Shift+Scroll up
- Incrementar tamaño de texto Ctrl+Scroll down
- Nuevo Tab Doble Click en la barra de Tabs
- Abrir en Tab de fondo Ctrl+Click Izquierdo
- Abrir en Tab al frente Shift+Ctrl+Click Izquierdo
- Abrir en Nueva Ventana Shift+Click Izquierdo
- Refrescar (ignorar cache) Shift+Botón de Recargar
- Guardar página como Alt+Click Izquierdo
- Bajar linea por linea Alt+Scroll.

Editado, Corregido y revisado por Ozharu
raza Comunicaciones™ 2005
Recopilado por Sansuito