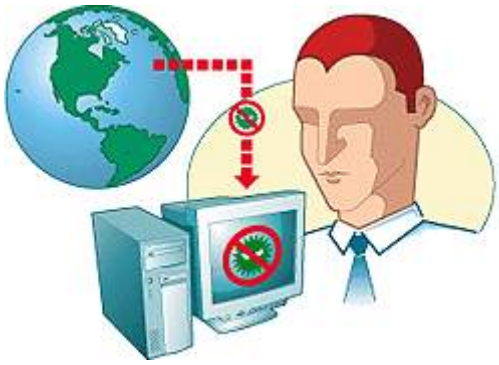
Redesna Informática S.L.

Punto de encuentro entre la Tecnología y la Creatividad.

# ALERTA ANTIVIRUS: RECOMENDACIONES

REDESNA Informática S.L. ofrece a sus clientes las siguientes recomendaciones para mantener el sistema informático alejado de los virus. Esperamos que te sea útil !

## 1.- UTILIZA SIEMPRE UN ANTIVIRUS



La mejor manera de estar protegido contra los virus es instalando un antivirus en tu ordenador (el antivirus debe incluir soporte técnico).

Un antivirus es un programa informático diseñado para detectar y eliminar virus: los reconoce, sabe cómo actúan y cómo eliminarlos.

Cada día aparecen más de 20 nuevos virus. Para la detección y eliminación de estos virus es necesario que el antivirus esté permanente actualizado.

Afortunadamente, la mayoría de los antivirus se actualizan automáticamente cada vez que nuestro ordenador se conecta a Internet. No obstante, recomendamos que por precaución se compruebe que esta actualización automática sucede realmente.

Si el antivirus no se actualizase no sería capaz de reconocer los nuevos virus que aparecen diariamente y perdería casi toda su eficacia.

Finalmente, asegúrate de que tu antivirus esté siempre activo, y muy especialmente cuando se está trabajando en Internet.

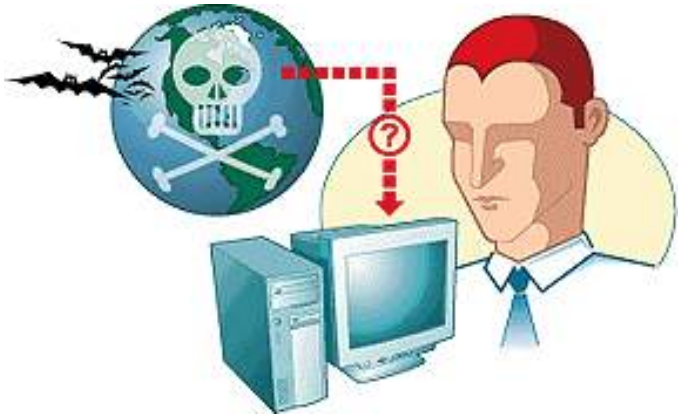
## 2.- VERIFICA, ANTES DE ABRIR, CADA MENSAJE DE CORREO RECIBIDO

El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización. Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip").

Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado. Por ejemplo, en versiones antiguas y no parcheadas del MS Internet Explorer basta únicamente con abrir el mensaje, o visualizarlo mediante la 'vista previa'.

Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente (generalmente inglés).

## 3.- EVITA LA DESCARGA DE PROGRAMAS DE LUGARES NO SEGUROS DE INTERNET



Muchas páginas de Internet permiten la descarga de programas y archivos a los ordenadores de los internautas. Cabe la posibilidad de que estos archivos estén infectados con virus.

Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de programas desde sitios web que no nos ofrezcan garantías. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.

## 4.- RECHAZA ARCHIVOS QUE NO HAYAS SOLICITADO CUANDO ESTES EN CHATS (IRC)

Gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los chats.

Un amplio número de virus utiliza precisamente estos chats para propagarse. Lo hacen enviando ficheros adjuntos (generalmente con nombres muy sugerentes). En general, si desconocemos el usuario que nos envía el fichero, debemos de rechazarlo.

## 5.-REALIZA PERIÓDICAMENTE COPIAS DE SEGURIDAD


Una muy buena forma de minimizar el impacto de un virus, tanto a nivel corporativo como particular, es restaurar las copias de seguridad de nuestra información.

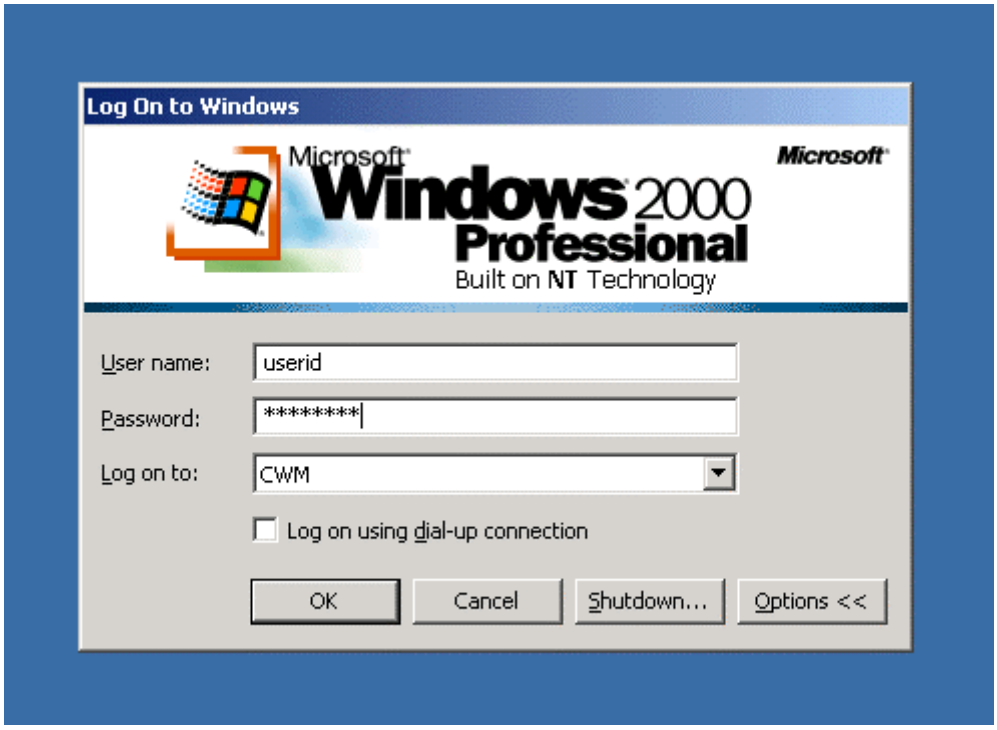
Realizar copias periódicas y frecuentes de nuestra información más importante es una magnífica política de seguridad. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

## 6.-MANTENTE INFORMAD@


Una buena manera de protegerse contra los nuevos virus es estar continuamente informado sobre lo que acontece en el sector de la Seguridad Informática.

Sin embargo, ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinados organismos y compañías: nuestro centro de Alerta Antivirus, empresas antivirus, organismos gubernamentales, universidades, etc.

## 7.-UTILIZA USUARIOS SIN PRIVILEGIOS PARA TAREAS COMUNES




Esto es algo que saben muy bien los usuarios de Unix/Linux y otros sistemas operativos multiusuario; es recomendable utilizar las cuentas de superusuario sólo para las tareas que lo requieran, como instalar programas y modificar la configuración del sistema.

También es ahora posible para usuarios de Windows (2000 y XP). Windows 95, 98 y Me no disponen de esta característica. Windows NT también tiene un diseño multiusuario, pero al ser poco amigable y limitado en capacidades multimedia ha tenido poco uso doméstico.

### ¿Qué es una cuenta de usuario?

En un sistema operativo multiusuario existen identidades (cuentas de usuario) con las que se pueden ejecutar programas. A cada cuenta de usuario se le asignan unos privilegios (por ejemplo ficheros que puede modificar, posibilidad de instalar dispositivos, apagar el ordenador, etc.).

Para facilitar la gestión se crean **grupos** que contienen usuarios, y a los que se puede asignar privilegios. En las versiones de Windows basadas en NT (NT, 2000,XP) Se crean siempre por defecto el usuario "Administrador" (control total del ordenador) y el usuario "Invitado" (muy pocos privilegios).

También se crean los grupos "Administradores", "Usuarios Avanzados" (*Power Users* en las versiones en inglés) y "Usuarios"; es recomendable usar normalmente uno de los dos últimos. Para saber más recomendamos que lea la ayuda de windows sobre cuentas de usuario.

**¿Por qué es recomendable usar usuarios regulares?**

Para la mayoría de las tareas comunes (programas de oficina, navegar por Internet, leer correo, chatear, etc) no hace falta usar un usuario con privilegios. En primer lugar no se podrá "romper algo" por error (hasta los usuarios más experimentados pueden equivocarse de vez en cuando).

Desde el punto de vista de los virus, hay que tener en cuenta cualquier programa que se ejecute bajo la identidad de un usuario lo hace con sus privilegios. Por tanto si ejecuta un virus u otro programa malicioso siendo un usuario normal, este se verá muy limitado en su capacidad para causar daño: no podrá modificar ficheros del sistema, para dejar inutilizado el ordenador o reiniciarse con Windows.

En caso de que necesite ejecutar un programa con privilegios administrativos (por ejemplo un instalador), en Windows XP haciendo click derecho (Mayúsculas + click derecho en Windows 2000) sobre el icono de un programa o acceso directo aparece la opción "Ejecutar Como...", que nos permite, dentro de una sesión, correr un programa bajo un usuario distinto.

El problema de esta práctica es que hay programas viejos, escritos antes del 2000, que necesitan ejecutarse con privilegios, normalmente debido a que guardan información de configuración en la carpeta de instalación del programa, y que además se caerán sin dar mucha información.

Normalmente no hay más remedio que ejecutarlos como un usuario con privilegios. Los programas bien escritos para entornos multiusuario guardan su información en las carpetas del usuario (Bajo "Documents and Settings", o en "Mis Documentos") .