

## Introducción

El auge de las redes de comunicación en los últimos años y especialmente el vertiginoso crecimiento de Internet, han popularizado enormemente el uso del correo electrónico.

Una de las mayores ventajas del correo electrónico es la posibilidad de enviar y recibir ficheros. Esta, que es una de las principales ventajas del correo electrónico, se ha convertido también en una nueva puerta de entrada y salida para virus y para otros tipos de ataques, así como el aprovechamiento de fallos de seguridad que afectan a los mensajes gestionados con algunos programas de correo (generalmente, los más utilizados).

Es muy frecuente intercambiar documentos mediante el correo electrónico. Esto ha posibilitado, en gran medida, la enorme expansión de virus de Word y Excel. A pesar de esto, no hay que olvidar que mediante el correo electrónico se pueden enviar y recibir todo tipo de virus y no únicamente los de Word y Excel. También, otros tipo de ficheros (incluso aprovechando los propios mensajes de correo, sin ficheros adjuntos), pueden contener virus.

Los antivirus convencionales no están preparados para llevar a cabo una detección y desinfección eficiente de virus situados en mensajes de correo electrónico por las siguientes razones:

1. Habitualmente, los mensajes de correo electrónico se almacenan en una base de datos de correo con un formato propio y con técnicas de compresión y/o encriptación que imposibilitan el análisis de los antivirus convencionales.
2. Es muy frecuente que los mensajes de correo electrónico y sus ficheros asociados estén guardados en un servidor al que un antivirus convencional no va a poder tener acceso.

Por las razones expuestas, un antivirus para correo electrónico debe estar específicamente diseñado para detectar y eliminar virus en el ámbito del correo electrónico. Por ello, las características principales con las que debe contar un antivirus para correo electrónico son:

- Análisis de los mensajes en el mismo momento de su recepción de manera totalmente automática.
- Análisis automático de cada mensaje en el momento en el que se abre.
- Análisis automático de cada mensaje que se intente enviar. De esta manera se evita la posibilidad de enviar mensajes contaminados con virus.
- Análisis automático de cada mensaje que se guarde.
- Análisis de todos los mensajes de correo en cualquier momento a petición del usuario.
- Integración con el programa de correo electrónico.
- Posibilidad de analizar ficheros comprimidos.
- Posibilidad de analizar mensajes anidados (mensajes dentro de otros mensajes).

Panda Antivirus para Exchange/Outlook es un antivirus para correo electrónico que cuenta con todas las características descritas y con muchas otras que completan su funcionalidad y lo convierten en una herramienta potente pero muy configurable que evita todo riesgo en el trabajo con mensajes de correo electrónico.

**Nota:** en esta ayuda se explican las características de Panda Antivirus Exchange/Outlook.

Recuerda que tu Panda Antivirus Exchange/Outlook puede haber sido instalado junto Panda Antivirus Platinum, por lo que te aconsejamos consultar ambas ayudas.

## Instalación

### Requisitos

Panda Antivirus Exchange/Outlook precisa:

- **Sistema operativo:** alguno de los siguientes: Windows XP, Windows 2000 Pro, Windows NT Workstation 4.0, Windows Millennium, Windows 98, o Windows 95.
- **Disco duro:** al menos, 6 MB de espacio libre en el disco duro.
- Tener instalado Exchange y/o Outlook.

### Instalación

Para instalar Panda Antivirus Exchange/Outlook hay que introducir el CD-ROM en la unidad lectora de CD y ejecutar el programa *SETUP.EXE*. En el caso de que hayas instalado Panda Antivirus Platinum, no será necesario ya que Panda Antivirus Exchange/Outlook se habrá instalado automáticamente.

El proceso de instalación consta de una serie de ventanas en las que se preguntan los distintos datos necesarios para llevar a cabo la instalación. Si tu Panda Antivirus Exchange/Outlook se instala automáticamente junto con Panda Antivirus Platinum, consulta los pasos de instalación de Panda Antivirus Platinum.

Una vez concluida la instalación, aunque no es necesario, te recomendamos reiniciar el ordenador. El antivirus para Exchange/Outlook no se pondrá en funcionamiento hasta que se abra por primera vez la ventana Exchange/Outlook.

### Desinstalación

Para desinstalar Panda Antivirus Exchange/Outlook hay que seguir estos pasos:

1. Cerrar el programa de correo Exchange/Outlook.
2. Pulsa el botón **Inicio** de Windows.
3. Selecciona la opción **Programas**.
4. Accede al grupo de programas **Panda Antivirus Platinum**.
5. Selecciona la opción **Desinstalar - Reparar**. Esto muestra un cuadro de diálogo, con dos botones: **Reparar** (permite restaurar el antivirus) y **Eliminar** (desinstala el antivirus).
6. Si realmente deseas desinstalar el antivirus, pulsa el botón **Eliminar**.
7. Se pide confirmación para eliminar la aplicación y todos sus componentes. Pulsa el botón **Aceptar** para eliminar el antivirus.
8. Existen dos posibilidades: **Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**. Marca una de ellas y pulsa el botón **Finalizar**.

**Nota:** recuerde que una vez ejecutados estos pasos habrá desinstalado Panda Antivirus Exchange Outlook junto con Panda Antivirus Platinum. Por lo tanto, no estará protegido contra los virus.

## Cómo Analizar con Panda Antivirus Exchange/Outlook

### Análisis Inmediatos



Para analizar una **carpeta de correo**, haz lo siguiente:

1. Selecciona la carpeta que deseas analizar. Si eliges una carpeta que contenga otras carpetas (por ejemplo, un buzón), se analizarán todas las carpetas dependientes de la elegida.
2. Analízala utilizando una de las siguientes posibilidades:

Pulsa el botón **Analizar carpeta o mensajes seleccionados** en la barra de botones estándar de Exchange/Outlook.

Despliega el menú **Herramientas**, en la ventana de Exchange/Outlook y selecciona la opción **Analizar en busca de virus...**

Una vez terminado el análisis, podrás ver el informe de resultados en el que se detalla cualquier incidencia encontrada durante el análisis.

Para analizar uno o varios **mensajes de correo**, haz lo siguiente:

1. Selecciona los mensajes que deseas analizar. Puedes seleccionar varios mensajes, pulsando con el puntero del ratón sobre uno de ellos, manteniendo pulsada la tecla *CTRL* (*control*) y pulsando los restantes. Para seleccionar un grupo de mensajes, pulsa sobre el primero de ellos, mantén pulsada la tecla *SHIFT* y pulsa sobre el último del grupo.
2. Analízalo/s utilizando una de las siguientes posibilidades:

Pulsa el botón **Analizar carpeta o mensajes seleccionados** en la barra de botones estándar de Exchange/Outlook.

Despliega el menú **Herramientas**, en la ventana de Exchange/Outlook y selecciona la opción **Analizar en busca de virus...**

## **Protección Permanente (en Tiempo Real)**

La protección permanente te permite trabajar con toda tranquilidad con tu correo sin preocuparte por los virus, ya que Panda Antivirus Exchange/Outlook vigilará todas las operaciones sospechosas por ti.

La protección permanente se encarga de analizar en busca de virus:

- Todos los nuevos mensajes que se reciban.
- Todos aquellos mensajes que se quieran enviar.
- Todos los mensajes que se abran independientemente de si se recibieron antes o después de la instalación del antivirus.
- Todos los mensajes que se quieran guardar.

La protección permanente se puede activar o desactivar fácilmente mediante el botón habilitado a tal efecto en la barra de botones estándar de Exchange/Outlook (Activar/Desactivar Panda Antivirus). Si pulsas este botón y queda pulsado, la protección permanente estará activa. Si no lo dejas pulsado, la protección permanente no estará activa y como consecuencia, no te protegerá de los virus que te lleguen a través del correo electrónico de Exchange/Outlook.



Panda Antivirus Exchange/Outlook es capaz de analizar ficheros comprimidos y mensajes anidados (mensajes dentro de otros mensajes) ofreciendo así los mayores niveles de protección.

## Funcionamiento de Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook se integra con Exchange/Outlook completamente. Por tanto, todo el manejo del antivirus se lleva a cabo desde el propio programa de correo.

Panda Antivirus Exchange/Outlook añade cuatro botones a la barra de botones estándar de Exchange/Outlook. Esos cuatro botones son:



 Botón **Analizar (Panda Antivirus - Analizar carpetas o mensajes seleccionados)**: cuando pulses este botón comenzará un análisis de la carpeta o mensajes seleccionados. Se analizarán todas las subcarpetas que se encuentren dentro de la mencionada carpeta. Una ventana permite el seguimiento del proceso del análisis mostrando el conjunto de carpetas que se van a analizar, la carpeta que se está analizando en cada momento y una barra de progreso.

 Botón **Panda Antivirus - Mostrar reporte**: este botón muestra el informe de incidencias que ha encontrado el antivirus. Este informe se conserva de sesión en sesión hasta que decidas borrarlo.

 Botón **Activar/Desactivar Panda Antivirus**: este botón permite activar o desactivar la protección permanente de Panda Antivirus. Si se desactiva la mencionada protección, Panda Antivirus Exchange/Outlook no analizará los nuevos mensajes que se reciban o envíen en busca de virus. Tampoco analizará en busca de virus aquellos mensajes que se abran para ser leídos. Sin embargo, sí que podrá analizar una determinada carpeta o mensaje en cualquier momento mediante el botón **Analizar**. El análisis en el arranque de Exchange/Outlook se llevará a cabo aunque se haya desconectado la protección permanente.

 Botón **Configurar Panda Antivirus**: este botón muestra la ventana de configuración de Panda Antivirus Exchange/Outlook (podrás realizar cambios en la configuración siempre que tu Panda Antivirus Exchange/Outlook no tenga establecida una contraseña para impedirlo). A través de esta ventana, se puede configurar el comportamiento general del antivirus, su comportamiento en el arranque del programa de correo y su comportamiento como protección permanente y como protección bajo demanda. También puedes acceder a la configuración de Panda Antivirus Exchange/Outlook, desplegando el menú **Herramientas** (en la ventana de Exchange/Outlook) y seleccionando **Opciones**. En dicha ventana de opciones aparece una página llamada Panda Antivirus Exchange/Outlook mediante la cual se puede configurar el antivirus.

### Configuración de Panda Antivirus Exchange/Outlook

Panda Antivirus Exchange/Outlook permite una amplia configuración para cada una de sus funciones. La ventana de configuración está dividida en varias páginas (fichas o pestañas) cada una de ellas referida a una parte concreta del antivirus.

Puedes ampliar esta información sobre la configuración de Panda Antivirus Exchange/Outlook, consultando los siguientes apartados de esta ayuda:

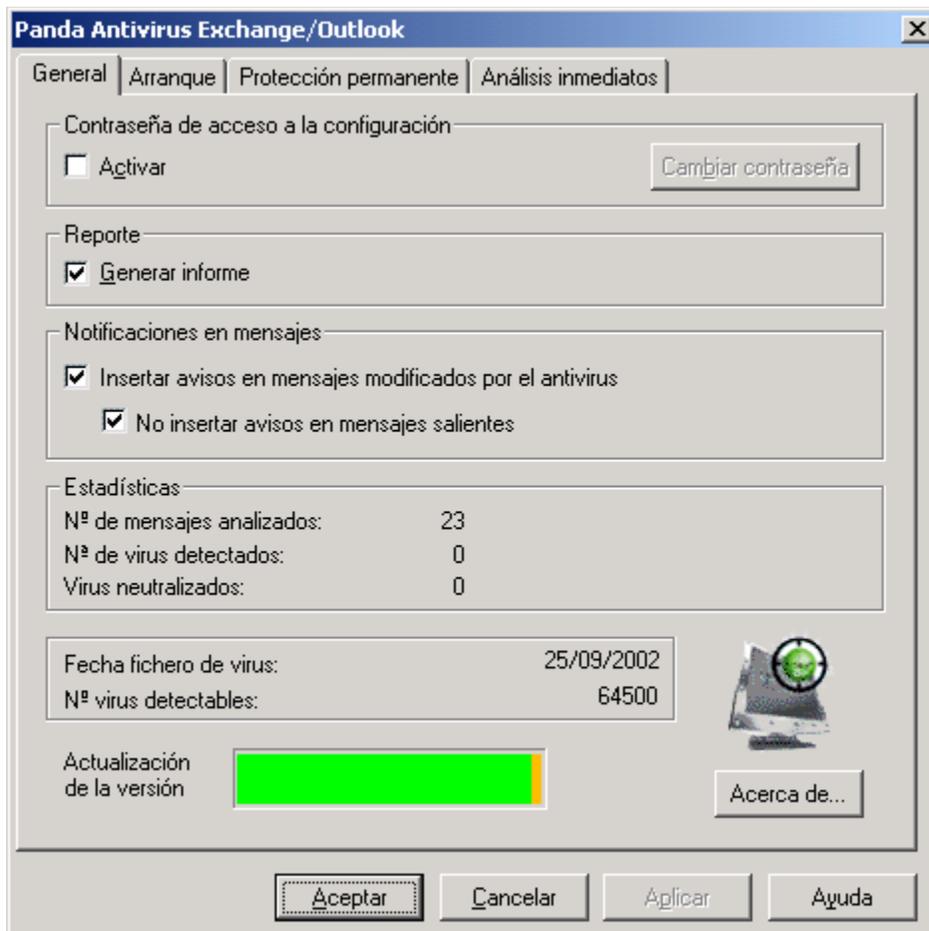
[General](#)

[Arranque](#)

Protección Permanente  
Análisis Inmediatos

## General

Las opciones agrupadas en esta página son de ámbito general y condicionan el comportamiento del antivirus en todos los casos. Son las siguientes:



### Contraseña de acceso a la configuración

- **Activar.** La primera vez que se marca esta casilla, se solicita la introducción de una contraseña. Esta permitirá proteger la configuración del antivirus (sólo será posible modificar la configuración si se conoce dicha contraseña). En el momento de introducir por primera vez la contraseña (o de modificarla) ésta se debe escribir dos veces (nueva contraseña y la confirmación de ésta). Cuando ya está asignada una contraseña, el botón **Cambiar contraseña** se habilita. A partir de ese momento, cada vez que se quiera modificar la configuración del antivirus, habrá que introducir dicha contraseña. Si ésta se conoce, además será posible modificarla (si se estima necesario).

### Reporte

- **Generar informe.** Si se marca esta casilla, todas las operaciones de análisis del antivirus registrarán las distintas incidencias en un fichero de resultados.

## Notificaciones en mensajes

- **Insertar avisos en mensajes modificados por el antivirus.** Si se marca esta casilla, cada vez que se encuentre un virus en un mensaje, se añadirá un texto a dicho mensaje a modo de advertencia. Dicho mensaje se añadirá independientemente de la acción que se haya decidido llevar a cabo al encontrar un virus.
- **No insertar avisos en mensajes salientes.** Si se marca esta casilla, no se incluirá ningún texto a modo de advertencia en los mensajes salientes (los enviados), cuando se encuentre algún virus en ellos.

## Estadísticas

Esta sección muestra los siguientes datos: el **Nº de mensajes analizados** por el antivirus, el **Nº de virus detectados** durante los análisis realizados y el número de **Virus neutralizados** por el antivirus.

Esta pestaña **General** de configuración, además contiene otra información de interés. Ésta es la siguiente: **Fecha fichero de virus** (fecha del *archivo de identificadores de virus* -fichero que permite la detección de los virus-, incorporado en el antivirus) y **Nº virus detectables** (indica el número de virus que el antivirus es capaz de detectar).

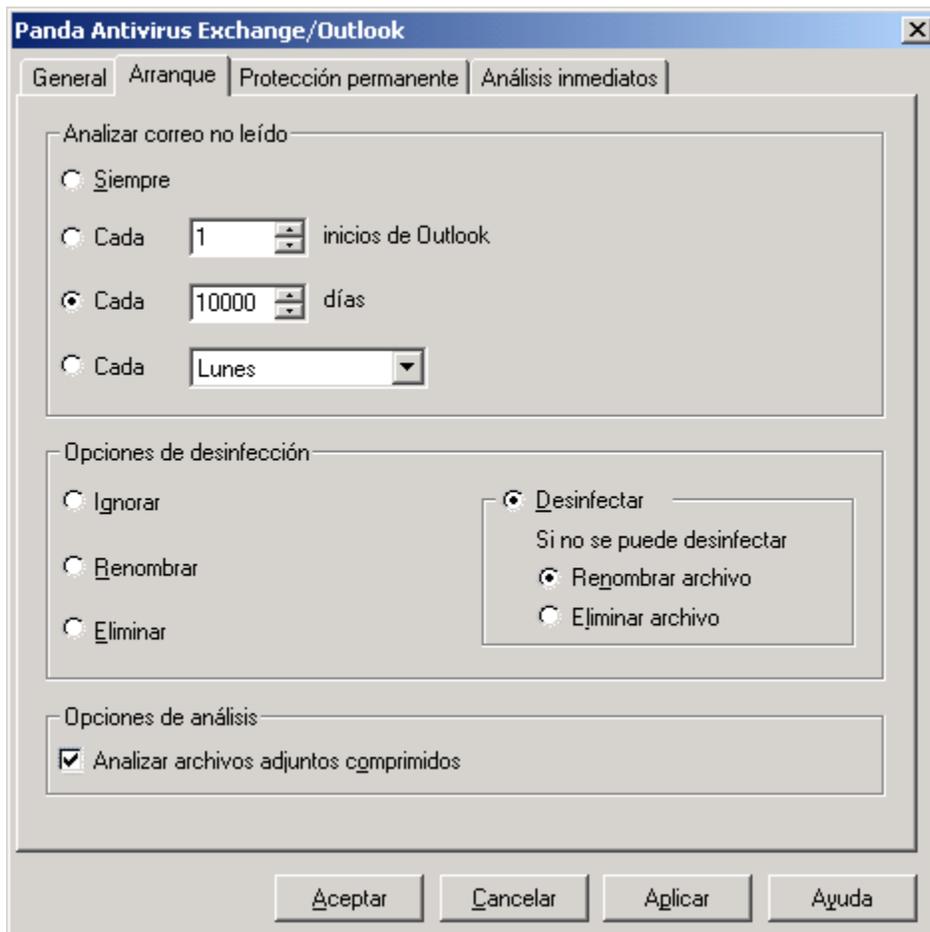
Adicionalmente, la ficha **General** incluye una barra de progreso en la parte inferior. Aquí se muestra, de forma gráfica, lo actualizado está tu antivirus. Ésta te indica el grado de actualización de tu antivirus. El virus está tan actualizado como espacio en verde aparece en dicha barra de progreso.

En la parte inferior de esta pestaña, se muestran los siguientes botones:

- Botón **Aceptar**: la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), se aplican y se guardan.
- Botón **Cancelar**: la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), no se aplican y tampoco se guardan.
- Botón **Aplicar**: la ventana no se cierra, pero los cambios que hayas realizado en esta ficha (y en las restantes), tienen efecto (se aplican en ese mismo momento).
- Botón **Ayuda**: accedes a una explicación sobre la ficha en la que te encuentras.

## Arranque

En esta página se puede configurar el comportamiento del antivirus en el momento en el que se arranca el programa de correo electrónico Exchange/Outlook. Las opciones disponibles son las siguientes:



### Analizar correo no leído

- **Siempre.** Si se marca dicha casilla, cada vez que se arranque o inicie Exchange/Outlook se analizarán todos los mensajes no leídos de la bandeja de entrada.
- **Cada cierto número de inicios de Outlook.** Si se marca dicha casilla, los mensajes no leídos de la bandeja de entrada se analizarán cada vez que se cumpla el número indicado de inicios del programa de correo.
- **Cada cierto número de días.** Si se marca dicha casilla, el análisis de los mensajes no leídos de la bandeja de entrada se llevará a cabo únicamente cada vez que pase el lapso de días que tú indiques en esta sección.
- **Cada ciertos días.** Si se marca dicha casilla, sólo se analizarán los mensajes no leídos de la bandeja de entrada el día de la semana que tú hayas elegido.

### Opciones de desinfección

- **Ignorar:** si se marca dicha casilla y se encuentra un virus, el antivirus no llevará a cabo ninguna acción aparte de mostrar una ventana avisando de que se ha encontrado un virus.
- **Renombrar:** si se marca dicha casilla y se encuentra un virus, el antivirus procederá a cambiar el nombre del fichero contaminado con virus.
- **Eliminar:** si se marca dicha casilla y se encuentra un virus, el antivirus procederá a borrar el fichero infectado.
- **Desinfectar:** si se marca dicha casilla y se encuentra un virus, el antivirus intentará desinfectar el fichero infectado.
- **Si no se puede desinfectar - Renombrar archivo:** si el antivirus no puede desinfectar un archivo contaminado, procederá a cambiar el nombre de dicho archivo.
- **Si no se puede desinfectar - Eliminar archivo:** si el antivirus no puede desinfectar un archivo infectado, procederá a borrar el mencionado archivo.

### Opciones de análisis

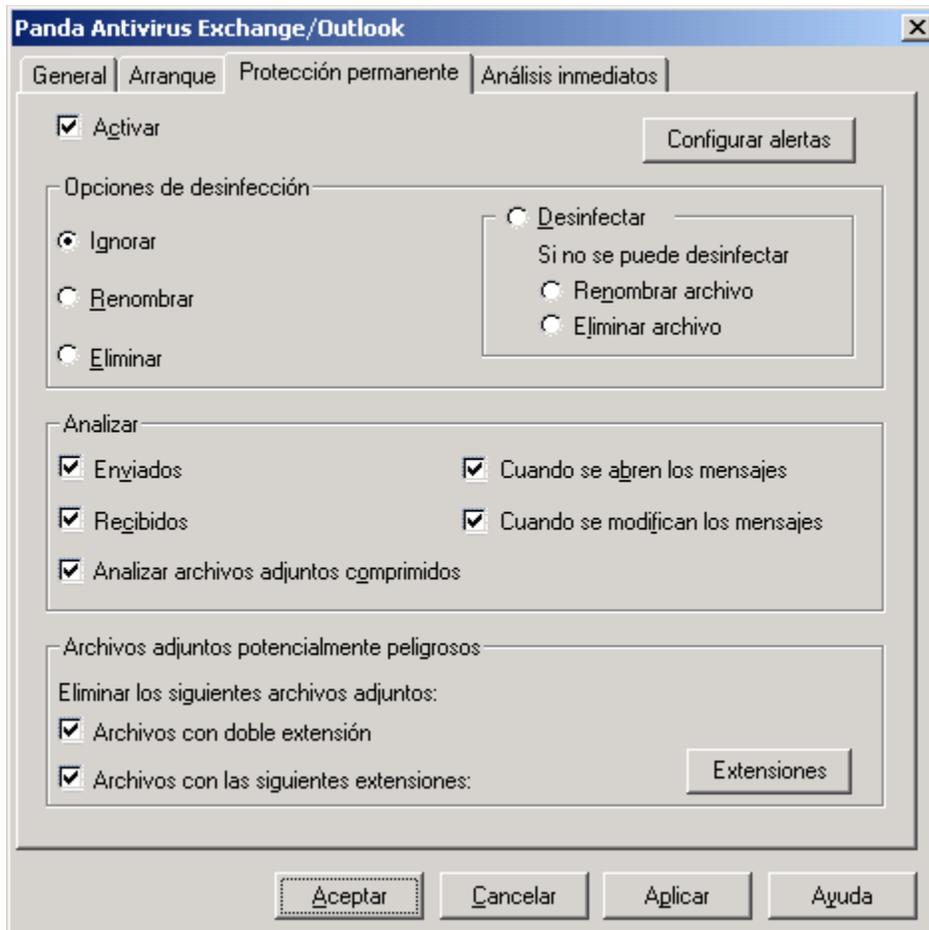
- **Analizar archivos adjuntos comprimidos:** si se marca esta casilla y se encuentra un fichero comprimido dentro de un mensaje, se procederá a su análisis como si se tratara de un archivo normal.

En la parte inferior de esta pestaña, se muestran los siguientes botones:

- Botón **Aceptar:** la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), se aplican y se guardan.
- Botón **Cancelar:** la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), no se aplican y tampoco se guardan.
- Botón **Aplicar:** la ventana no se cierra, pero los cambios que hayas realizado en esta ficha (y en las restantes), tienen efecto (se aplican en ese mismo momento).
- Botón **Ayuda:** accedes a una explicación sobre la ficha en la que te encuentras.

## Protección Permanente

La protección permanente consiste en un análisis que el antivirus realiza sin tu intervención y en todo momento. Esto lo hace de forma continua (siempre que dicha protección esté activada) sobre todos y cada uno de los mensajes de correo con los que se trabaja (enviados, recibidos, abiertos, cerrados, modificados, guardados, etc). En esta página se puede configurar la protección permanente que ofrece el antivirus. Las opciones disponibles son las siguientes:



**Activar:** si se marca esta casilla se activará la protección permanente. Esto quiere decir que se analizarán automáticamente todos los mensajes que lleguen así como todos los mensajes que se envíen, abran o guarden.

### Opciones de desinfección

- **Ignorar:** si se marca dicha casilla y se encuentra un virus, el antivirus no llevará a cabo ninguna acción aparte de mostrar una ventana avisando de que se ha encontrado un virus.
- **Renombrar:** si se marca dicha casilla y se encuentra un virus, el antivirus cambia del nombre del fichero contaminado con virus.
- **Eliminar:** si se marca dicha casilla y se encuentra un virus, el antivirus borra el fichero infectado.

- **Desinfectar:** si se marca dicha casilla y se encuentra un virus, el antivirus intentará desinfectar el fichero infectado.
- **Si no se puede desinfectar - Renombrar archivo:** si el antivirus no puede desinfectar un archivo contaminado, procederá a cambiar el nombre de dicho archivo.
- **Si no se puede desinfectar - Eliminar archivo:** si el antivirus no puede desinfectar un archivo infectado, procederá a borrar el mencionado archivo.

### Analizar

- **Enviados:** si se marca esta casilla, se analizarán los mensajes que se quieran enviar, antes de que se envíen. De esta manera, se evita el envío de ficheros contaminados.
- **Recibidos:** si se marca esta casilla, se analizarán todos los mensajes que se reciban en el mismo momento de su recepción, antes siquiera de que se abran.
- **Analizar archivos adjuntos comprimidos:** si se marca esta casilla y se encuentra un fichero comprimido dentro de un mensaje, se procederá a su análisis como si se tratara de un archivo normal.
- **Cuando se abren los mensajes:** si se marca esta casilla, se analizarán todos aquellos mensajes que se abran independientemente de cuándo se hayan recibido.
- **Cuando se modifican los mensajes:** si se marca esta casilla, se analizarán todos aquellos mensajes que se guarden (debido a que han sido modificados o simplemente al guardarlos).

**Archivos adjuntos potencialmente peligrosos.** Puedes indicar cuáles deben ser los ficheros, incluidos en los mensajes, que el antivirus debe eliminar.

- **Archivos con doble extensión:** si se marca dicha casilla, el antivirus borra todos los ficheros que tengan dos extensiones (*FICHERO.EXE.VBS*, por ejemplo) y que estén incluidos en los mensajes de correo (tanto enviados, como recibidos).
- **Archivos con las siguientes extensiones:** si se marca dicha casilla, el antivirus borra todos los ficheros que tengan una de las extensiones incluidas en la lista. Puedes consultar dicha lista de extensiones, incluir nuevas extensiones y eliminar extensiones de ella, pulsando el botón [Extensiones](#).

Botón **Configurar alertas**. Si se pulsa este botón, se accede a la ventana desde la cual es posible indicar cuáles son los destinatarios a los que el antivirus debe enviar mensajes de alerta correspondientes a los virus detectados. Esta ventana cuenta con las siguientes opciones:

- **Avisar al remitente:** si se marca esta casilla y se detecta un virus en un mensaje, la persona que lo envió recibirá un mensaje en el que se le alerta de esta situación de infección.
- **Avisar a los demás destinatarios:** si se marca esta casilla y se detecta un virus en un mensaje, todos los destinatarios de dicho mensaje, recibirán también un mensaje en el que se le alerta de esta situación de infección.
- **Enviar un mensaje al administrador:** si se marca esta casilla y se detecta un virus en un mensaje, el administrador de la red recibirá un mensaje alertándole de esta situación de infección. En la sección **Dirección e-mail del administrador**, se debe escribir la dirección de correo electrónico de la persona que administra y mantiene la red (el administrador), para que dicho mensaje llegue a su destino.

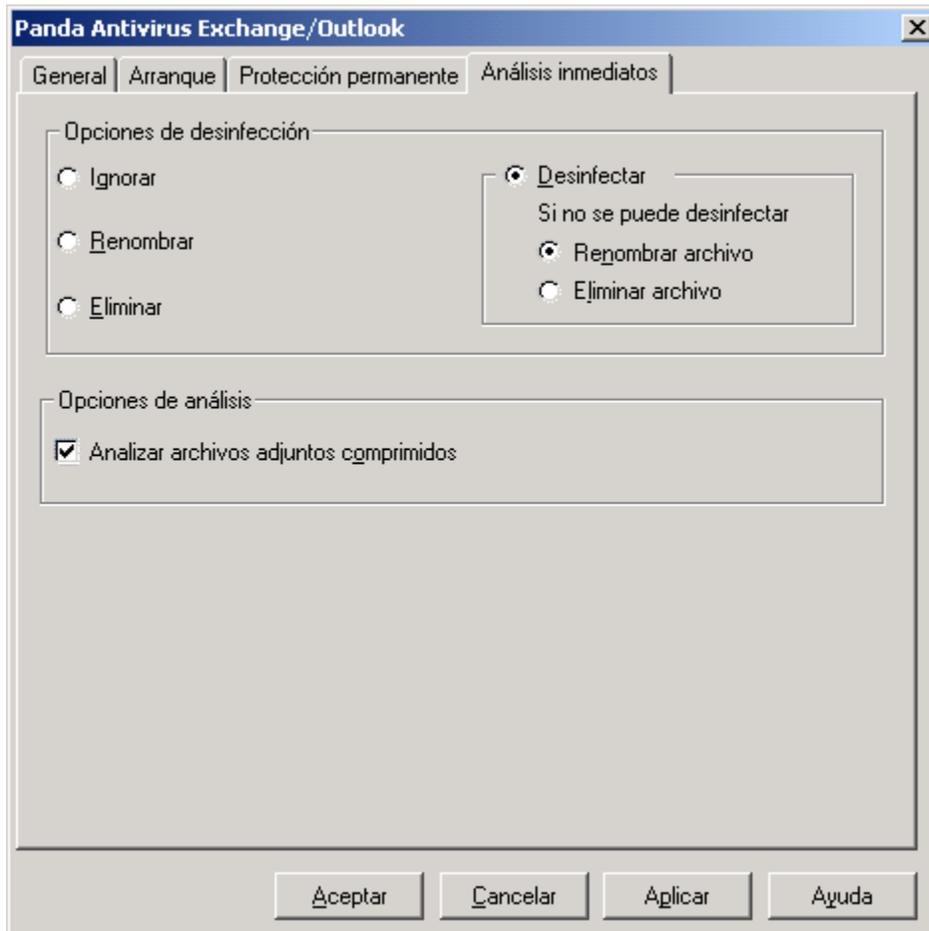
En la parte inferior de esta pestaña, se muestran los siguientes botones:

- Botón **Aceptar:** la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), se aplican y se guardan.

- Botón **Cancelar**: la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), no se aplican y tampoco se guardan.
- Botón **Aplicar**: la ventana no se cierra, pero los cambios que hayas realizado en esta ficha (y en las restantes), tienen efecto (se aplican en ese mismo momento).
- Botón **Ayuda**: accedes a una explicación sobre la ficha en la que te encuentras.

## Análisis Inmediatos

En esta página se pueden configurar las propiedades de los análisis bajo demanda -o análisis inmediatos- que ofrece el antivirus y que tú mismo puedes realizar en cualquier momento, cuando así lo indiques (analizar buzones de correo, carpetas, mensajes). Las opciones disponibles son las siguientes:



### Opciones de desinfección

**Ignorar:** si se marca dicha casilla y se encuentra un virus, el antivirus no llevará a cabo ninguna acción aparte de mostrar una ventana avisando de que se ha encontrado un virus.

**Renombrar:** si se marca dicha casilla y se encuentra un virus, el antivirus procederá a cambiar el nombre del fichero contaminado con virus.

**Eliminar:** si se marca dicha casilla y se encuentra un virus, el antivirus procederá a borrar el fichero infectado.

**Desinfectar:** si se marca dicha casilla y se encuentra un virus, el antivirus intentará desinfectar el

fichero infectado.

**Si no se puede desinfectar - Renombrar archivo:** si el antivirus no puede desinfectar un archivo contaminado, procederá a cambiar el nombre de dicho archivo.

**Si no se puede desinfectar - Eliminar archivo:** si el antivirus no puede desinfectar un archivo infectado, procederá a borrar el mencionado archivo.

### Opciones de análisis

**Analizar archivos adjuntos comprimidos:** si se marca esta casilla y se encuentra un fichero comprimido dentro de un mensaje, se procederá a su análisis como si se tratara de un archivo normal.

En la parte inferior de esta pestaña, se muestran los siguientes botones:

- Botón **Aceptar:** la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), se aplican y se guardan.
- Botón **Cancelar:** la ventana se cierra y los cambios que hayas realizado en esta ficha (y en las restantes), no se aplican y tampoco se guardan.
- Botón **Aplicar:** la ventana no se cierra, pero los cambios que hayas realizado en esta ficha (y en las restantes), tienen efecto (se aplican en ese mismo momento).
- Botón **Ayuda:** accedes a una explicación sobre la ficha en la que te encuentras.

## **Introducción a la Distribución a través de una Red**

La idea de distribuir el antivirus a través de una red surge para facilitar la labor de un administrador de red que quiere proteger un conjunto de puestos de una manera cómoda y rápida.

El funcionamiento es el siguiente:

1. El administrador de la red copia el antivirus a un directorio en el servidor o a un directorio compartido al que tengan acceso todos los usuarios. Esta copia se lleva a cabo a través de un programa instalador diseñado a tal efecto. Hay que tener en cuenta que NO se está instalando el antivirus en el servidor sino que únicamente se están copiando los ficheros necesarios para instalar el antivirus en los puestos.
2. Cada vez que un puesto se conecte a la red, se comprobará -de forma automática- si tiene el antivirus instalado y actualizado. Si éste se encuentra actualizado, no se hará nada pero si no tiene el antivirus instalado o no lo tiene actualizado, se procederá a la instalación o actualización del mismo de manera totalmente automática.

Como se ha visto, el servidor (o recurso compartido) únicamente sirve de medio para distribuir el antivirus a las estaciones.

Este procedimiento global sirve para prácticamente todo tipo de redes. Ahora bien, en cada una de ellas se lleva a cabo de una forma ligeramente diferente. En esta documentación se procederá a explicar dicho procedimiento para los tipos de redes más comunes hoy día.

## Cómo Distribuir el Antivirus a través de una Red

### Requisitos

Para la distribución de Panda Antivirus Exchange/Outlook a través de una red, se precisa:

- **Equipo y sistema operativo:** Ordenador compatible con IBM con alguno de los siguientes sistemas operativos: Windows XP, Windows 2000 Pro, Windows NT Workstation 4.0, Windows Millennium, Windows 98, o Windows 95.
- **Disco duro:**
  - Al menos, 6 MB de espacio libre en el disco duro del servidor que vaya a servir como medio de distribución.
  - Al menos, 6 MB de espacio libre en el disco duro de cada ordenador al que se le vaya a instalar (distribuir) el antivirus. del servidor que vaya a servir como medio de distribución.
- Tener instalado Exchange y/o Outlook en los ordenadores a los que se va a distribuir (o instalar) el antivirus.

### Cómo distribuir el antivirus a todos los puestos de la red fácilmente

El proceso de distribución del antivirus a todos los puestos de la red consta de dos partes:

1. Copia del antivirus a un directorio al que puedan acceder todos los usuarios.
2. Distribución del antivirus a todos los puestos a medida que se van conectando a la red mediante el programa *RINSTALL*.

A continuación se explica en detalle cómo realizar los dos pasos mencionados. Algunos aspectos de este proceso de instalación requieren conocimientos del tipo de red mediante la cual se va a distribuir el antivirus. Todos estos conocimientos se explican con detalle para los principales tipos de red en los apartados correspondientes, consúltalos si tienes alguna duda.

### Copia del antivirus a un directorio al que puedan acceder todos los usuarios

El primer paso en la distribución del antivirus a través de la red, es la copia de ficheros a un directorio en uno de los discos duros del servidor. Es muy importante tener en cuenta que la copia de los ficheros al servidor debe realizarse en un entorno libre de virus. Si esto no fuera así, se podrían contaminar los ficheros del antivirus. Como dichos ficheros se van a distribuir a todas las estaciones que se conecten a la red, el virus se distribuiría junto con ellos. Para lograr una copia de ficheros segura y para cerciorarse de que éstos no se van a contaminar desde ninguna estación en el futuro, se debe llevar a cabo la copia de acuerdo a los siguientes pasos:

1. El administrador debe asegurarse de que su ordenador esté libre de virus. Sería conveniente que el administrador instalase el antivirus adecuado de Panda Software en su ordenador y activase la protección permanente correspondiente. No se debería continuar con la instalación mientras no se esté seguro de que el ordenador desde el que se esté instalando el antivirus está libre de virus.
2. Se debe elegir un directorio en el servidor correspondiente donde copiar los ficheros. Recomendamos la creación de un nuevo directorio llamado *PAVEXCLI* sobre el que tengan derechos de *lectura* todos los usuarios. Es importante que ningún usuario tenga derechos de

*escritura o borrado* sobre ese directorio ya que de lo contrario, cualquier usuario podría, accidental o voluntariamente, infectar o borrar los ficheros del antivirus con las graves consecuencias que ello conlleva.

3. Una vez que se ha creado el directorio de destino, basta con introducir el CD-ROM del antivirus, situarse en la unidad correspondiente y ejecutar el programa *SETUP.EXE*.

El proceso de instalación consta de una serie de ventanas en las que se van preguntando los distintos datos necesarios para llevar a cabo la instalación en tu equipo. Uno de los datos que se te pedirán será el directorio destino. Debes elegir el directorio creado a tal efecto para que se copien en él los ficheros del antivirus.

### **Distribución del antivirus**

Es en esta etapa donde se comprueba la ventaja de nuestro antivirus para PCs en red. En vez de tener que ir estación a estación instalando el antivirus, éste se instala automáticamente en cuanto una estación se conecta a la red.

Habitualmente, cuando una estación se conecta a una red, se ejecutan una serie de comandos o programas para preparar el trabajo en red de igual forma que se ejecutan una serie de comandos o programas cada vez que se arranca un ordenador. A esta serie de comandos y/o programas se la conoce como *Login Script* (o guión de entrada).

Nuestro antivirus con capacidad de distribución a través de una red, va acompañado de un programa llamado *RINSTALL* que se encarga de la distribución automática del antivirus. Por tanto, lograr la distribución automática del antivirus es tan fácil como colocar en el *Login Script* la ejecución de *RINSTALL*.

*RINSTALL* se ejecutará cada vez que una estación se conecte a la red. Lo primero que comprueba *RINSTALL* es que la estación conectada tenga instalado el antivirus. Si lo tiene instalado y actualizado, no hace nada, prosiguiendo la ejecución de los restantes comandos del *Login Script* normalmente. Si la estación no tiene instalado el antivirus o lo tiene desactualizado, *RINSTALL* instalará el antivirus. Una vez hecho esto, la ejecución de los restantes comandos del *Login Script* continúa normalmente.

Como el funcionamiento del *RINSTALL* es totalmente automático, el administrador de la red sólo tiene que copiar los ficheros y modificar el *Login Script* para instalar la protección antivirus que se irá propagando a las estaciones a medida que se vayan conectando.

### **Distribución del antivirus en una red Novell NetWare**

Para que el antivirus se distribuya automáticamente a todas las estaciones a medida que se vayan conectando en una red Novell NetWare, hay que introducir la siguiente línea en el *System Login Script*:

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

**Consulte el apartado [Novell NetWare](#) para obtener una explicación más detallada sobre estos aspectos.**

Como se puede ver en el ejemplo, hay que indicar el lugar del servidor en el que residen los ficheros del antivirus. Por eso, la mencionada línea deberá ir *después* del mapeo de unidades quedando esta

parte del *System Login Script* como sigue:

```
MAP ROOT F:=ALFA\SYS:  
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

**Nota:** estas líneas hacen referencia al supuesto caso en el que el servidor tena por nombre *Alfa* y que los ficheros residan en el volumen *SYS*.

### Distribución del antivirus en una red Windows NT

Para que el antivirus se distribuya automáticamente a las estaciones de la red a medida que éstas se vayan conectando, hay que añadir la siguiente línea al *Archivo de comandos de inicio de sesión* usando el programa Profile Manager:

Consulte el apartado [Windows NT](#) para obtener una explicación más detallada sobre estos aspectos.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se puede ver en el ejemplo, hay que indicar el lugar donde se copiaron los ficheros del antivirus. Por eso, la mencionada línea deberá ir *después* del mapeo de recursos compartidos quedando esta parte del *Archivo de comandos de inicio de sesión* como sigue:

```
NET USE F: \\ALFA\SYS  
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

**Nota:** estas líneas hacen referencia al supuesto caso en el que el servidor tena por nombre *Alfa* y que los ficheros residan en el volumen *SYS*.

### Distribución del antivirus en una red OS/2

Para que el antivirus se distribuya automáticamente a las estaciones de la red a medida que éstas se vayan conectando, hay que añadir la siguiente línea al fichero *PROFILE.BAT* (o *PROFILE.CMD*):

Consulte el apartado [OS/2](#) para obtener una explicación más detallada sobre estos aspectos.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se puede ver en el ejemplo, hay que indicar el lugar donde se copiaron los ficheros del antivirus. Por eso, la mencionada línea deberá ir *después* del mapeo de recursos compartidos quedando esta parte del archivo *PROFILE.BAT* como sigue:

```
NET USE F: \\ALFA\SYS  
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

**Nota:** estas líneas hacen referencia al supuesto caso en el que el servidor tena por nombre *Alfa* y que los ficheros residan en el volumen *SYS*.

### Distribución del antivirus en una red Pathworks

Para que el antivirus se distribuya automáticamente a las estaciones de la red a medida que éstas se

vayan conectando, hay que añadir la siguiente línea en la secuencia de conexión de un grupo en el que se encuentre todos los usuarios a los que se quiera instalar el antivirus:

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se puede ver en el ejemplo, hay que indicar el lugar donde se copiaron los ficheros del antivirus. Por eso, es conveniente tener definido el mapa de unidades antes de que se ejecute *RINSTALL*.

### **Distribución del antivirus en una red Banyan-Vines**

Para que el antivirus se distribuya automáticamente a las estaciones de la red a medida que éstas se vayan conectando, hay que añadir la siguiente línea en el perfil de cada usuario cuya máquina se quiera proteger. El perfil de un usuario es la secuencia de órdenes que se ejecutan cada vez que dicho usuario se conecta a la red.

Basta con editar el mencionado perfil con el comando *MUSER* y añadir la línea:

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

**Nota:** esta línea hacen referencia al supuesto caso de que la unidad del servidor esté mapeada como *F* y que los ficheros se hayan copiado en el directorio *PAVEXCLI*.

Es muy conveniente tener definido el mapa de unidades antes de que se ejecute *RINSTALL* para asegurarse de que el disco duro del servidor se referencia de igual manera desde todas las estaciones.

La modificación uno a uno de todos los perfiles de usuario puede llegar a ser una tarea muy laboriosa si hay muchos usuarios. Habitualmente suele haber un perfil común utilizado por todos los usuarios. A dicho perfil se le llama desde los distintos perfiles de los usuarios. El comando que hay que usar para llamar a un perfil desde otro es:

```
USE Sample_Profile@grupo@organización
```

donde *Sample\_Profile* es un usuario ficticio. Además, *grupo* y *organización* son los correspondientes en la estructura de cada empresa.

De esta manera basta con hacer las oportunas modificaciones sobre el perfil *Sample\_Profile* para que afecten a todos los usuarios que llamen a dicho perfil desde el suyo propio.

### **Instalación del antivirus en un puesto no conectado a la red**

Si se quiere instalar Panda Antivirus Exchange/Outlook en un puesto no conectado a la red, hay que llevar a cabo el siguiente procedimiento:

1. Introducir el CD-ROM de Panda Antivirus Exchange/Outlook, situarse en la unidad correspondiente y ejecutar el programa *SETUP.EXE*. El proceso de instalación consta de una serie de ventanas en las que se te van preguntando los distintos datos necesarios para llevar a cabo la instalación en tu equipo. Uno de los datos que se te pedirá será el directorio destino. Debes elegir un directorio en el equipo donde está instalando y no un directorio del servidor tal y como se ha descrito anteriormente.

2. Una vez terminado el proceso de instalación, ejecuta el siguiente comando:

```
C:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(si has instalado el antivirus en otra unidad o directorio, indica el adecuado).

3. Cuando termine el proceso de distribución, Panda Antivirus para Exchange/Outlook estará instalado en tu equipo.
4. Elimina el directorio donde hayas instalado el antivirus en el paso 1 ya que no se precisará más.

#### **Solución de problemas de distribución**

Si el antivirus no se distribuye adecuadamente en uno o más equipos, ve a dicho equipo o equipos y compruebe lo siguiente:

1. Que desde ese equipo se puede realizar una conexión con el servidor en el que se ha copiado el antivirus.
2. Prueba a ejecutar el programa *RINSTALL* directamente. Sitúate en el directorio del servidor en el que hayas copiado el antivirus y ejecuta el siguiente comando: *RINSTALL PAVEX.SCR*

Si las dos comprobaciones anteriores han sido correctas, revisa el guión de entrada cerciorándote de que ha modificado el guión adecuado y de que la línea corresponda con la que se ha visto en este manual.

## Características Avanzadas

### Cómo evitar que los usuarios modifiquen la configuración de Panda Antivirus Exchange/Outlook

Si se desea evitar que los usuarios a los que se va a instalar automáticamente Panda Antivirus Exchange/Outlook puedan variar la configuración del mismo, se debe seguir el procedimiento que se describe a continuación:

1. Instalar Panda Antivirus Exchange/Outlook en el ordenador del administrador de la red.
2. Abrir el programa de correo Exchange/Outlook y configurar el antivirus de la manera deseada.
3. Proteger la configuración con contraseña. Esto se hace en la ventana de configuración del antivirus.
4. Copiar el fichero `PAVEXCLI.CFG` situado en el directorio `WINDOWS\SYSTEM` en el ordenador del administrador al directorio de la red desde el que se va a distribuir el antivirus.
5. Proceder a la modificación del *login script* para que comience la distribución del antivirus a todos los puestos de la red.

Es importante tener en cuenta que el procedimiento descrito debe llevarse a cabo antes de que comience la distribución del antivirus a través de la red.

## Conocimientos Necesarios sobre Novell NetWare

La distribución del antivirus a través de una red Novell NetWare precisa de unos conocimientos mínimos sobre dicho sistema. A continuación se describirán los conceptos que se precisa conocer ilustrándolos con ejemplos de cómo preparar el sistema de manera adecuada.

### Comandos que se ejecutan cuando se inicia una sesión de red

Habitualmente, cuando un ordenador arranca se ejecutan una serie de comandos definidos en un fichero. En el caso de MS-DOS o Windows, dicho fichero es el *AUTOEXEC.BAT*.

De igual manera, también es habitual que, cuando un ordenador se conecta a una red, se ejecuten una serie de comandos. A esta serie de comandos y/o programas se la conoce como *login script* o guión de entrada.

El *login script* puede ser general (el mismo para todos los usuarios) o particular (uno distinto para cada usuario). También se puede dar una solución mixta con un login script general común a todos los usuarios y un login script particular de cada usuario.

Dado que el *login script* se ejecuta cada vez que un usuario se conecta a la red, es el lugar adecuado para lograr la distribución del antivirus a los puestos. Bastará con ejecutar en el *login script* el programa de distribución de antivirus de Panda Software para que el mencionado antivirus se vaya distribuyendo a todos los puestos a medida que se vayan conectando a la red.

### System Login Script

En el caso de Novell NetWare, el login script general común a todos los usuarios se conoce como *System Login Script*. Se debe editar dicho fichero para añadir en él la ejecución del programa de distribución de antivirus de Panda Software. Para editar el *System Login Script* hay que llevar a cabo los siguientes pasos:

1. Si se tiene una versión Novell NetWare 3.x hay que usar el programa *SYSCON*. Si se tiene una versión Novell NetWare 4.x hay que usar el programa *NETADMIN*. Todos los servidores Novell NetWare tienen un volumen llamado *SYS* y dentro de este volumen siempre hay un directorio *PUBLIC*. Los dos programas mencionados (*SYSCON* y *NETADMIN*) se encuentran en dicho directorio.
2. Para editar el *System Login Script* con el programa *SYSCON*, hay que ejecutar el programa, seleccionar la opción **Supervisor Options** y luego la opción **System Login Script**.
3. Para editar el *System Login Script* con el programa *NETADMIN*, hay que ejecutar el programa e ir seleccionando los dos puntos ( . . ) en el cuadro de la izquierda hasta que ya no aparezca dicha opción. En ese momento, se verá una única opción (a la derecha estará descrita como una *organización*). Hecho esto, hay que seleccionar esa única opción y pulsar la tecla *F10*. En el menú que aparece hay que seleccionar la opción **Ver o editar propiedades del objeto** y en el siguiente menú que aparece hay que seleccionar la opción **Guión de entrada**. Hecho esto, ya se puede modificar el *System Login Script*.

En el *System Login Script* se deben introducir dos líneas: la línea referente al *mapeo* (se explica este concepto en el siguiente apartado) y la línea referente a la distribución automática del antivirus.

### **Asociación de una letra de unidad**

En este apartado se procederá a explicar el concepto de *mapeo*. En un ordenador, el disco duro se suele identificar con la letra *C*, la disquetera con la letra *A* o *B* y el CD-ROM con la *D*, la *E*, etc. dependiendo de los discos duros instalados.

Los volúmenes (*discos duros*) del servidor Novell NetWare deben también identificarse con una letra de unidad para así poder referirse a directorios y ficheros en estos volúmenes desde las estaciones sin problemas. A la operación de asociar una letra de unidad a un volumen se la conoce como *mapeo*.

Es muy interesante que todas las estaciones tengan los mismos *mapeos* para así asegurarse de que, para todas ellas, los distintos volúmenes del servidor se referencian igual. Para ello, basta con colocar la orden de mapeo en el *System Login Script*. Generalmente, los volúmenes comienzan a nombrarse a partir de la letra *F*, pero se puede usar cualquier otra letra de unidad que no esté siendo usada. La orden de mapeo, teniendo esto en cuenta, sería:

```
MAP ROOT F:=NOMBRE_SERVIDOR\NOMBRE_VOLUMEN
```

Si el nombre del servidor es *ALFA* y el nombre del volumen es *SYS*, la orden sería:

```
MAP ROOT F:=ALFA\SYS:
```

## Conocimientos Necesarios sobre Windows NT

La distribución del antivirus a través de una red Windows NT precisa de unos conocimientos mínimos sobre dicho sistema. A continuación se describirán los conceptos que se precisa conocer ilustrándolos con ejemplos de cómo preparar el sistema de manera adecuada.

### Comandos que se ejecutan cuando se inicia una sesión de red

Habitualmente, cuando un ordenador arranca, se ejecutan una serie de comandos definidos en un fichero. En el caso de MS-DOS o Windows, dicho fichero es el *AUTOEXEC.BAT*.

De igual manera, también es habitual que, cuando un ordenador se conecta a una red, se ejecuten una serie de comandos. A esta serie de comandos y/o programas se la conoce como *login script* o guión de entrada. En el caso de Windows NT se usa el nombre de *Archivo de comandos de inicio de sesión*.

En el caso de Windows NT, cada usuario tiene su propio archivo de comandos de inicio de sesión. Esto hace que, en principio, haya que modificar los archivos de comandos de inicio de sesión de todos los usuarios a los que se quiera distribuir el antivirus. Para evitar esta pesada tarea, Panda Software ha desarrollado una utilidad llamada Profile Manager cuyo funcionamiento se explica a continuación.

Dado que el archivo de comandos de inicio de sesión se ejecuta cada vez que un usuario se conecta a la red, es el lugar adecuado para lograr la distribución del antivirus a los puestos. Bastará con ejecutar en el archivo de comandos de inicio de sesión el programa de distribución de antivirus de Panda Software para que el mencionado antivirus se vaya distribuyendo a todos los puestos a medida que se vayan conectando a la red.

### Archivos de comandos de inicio de sesión - Profile Manager

Para instalar el programa Profile Manager que permite modificar de forma conjunta todos los archivos de comandos de inicio de sesión, hay que insertar disco etiquetado como *Editor de comandos de inicio para Windows NT* o situarse en el directorio correspondiente del CD-ROM y ejecutar el programa *SETUP.EXE*. Por ejemplo:

```
A:\SETUP
```

Una vez instalado, realice los siguientes pasos:

1. Ejecuta el programa.
2. Selecciona el modo simplificado.
3. Selecciona la opción **Editar comandos de inicio de dominio** dentro del menú **Archivo**.
4. En la parte inferior de la ventana se verá un editor de texto. Es en dicho editor donde se hacen las modificaciones pertinentes que afectarán a todos los archivos de comandos de inicio de sesión.
5. Salir del programa, salvando las modificaciones.

En el *Archivo de comandos de inicio de sesión* se deben introducir dos líneas: la línea referente al *mapeo* (se explica este concepto en el siguiente apartado) y la línea referente a la distribución automática del antivirus.

### **Asociación de una letra de unidad**

En este apartado se procederá a explicar el concepto de *mapeo*. En un ordenador, el disco duro se suele identificar con la letra *C*, la disquete con la letra *A* o *B* y el CD-ROM con la *D*, la *E*, etc. dependiendo de los discos duros instalados.

En el caso de una red Windows NT, el concepto de *mapeo* va relacionado con el concepto de *recurso compartido*. La totalidad o cualquier parte del disco duro del servidor (o de los discos si tiene varios) puede compartirse y convertirse así en un *recurso compartido*. Estos recursos compartidos son los que deben mapearse para luego poder referirse a ellos desde las estaciones.

Es muy interesante que todas las estaciones tengan el mismo *mapeo* para así asegurarse de que, para todas ellas, los distintos recursos compartidos del servidor se referencian igual. Para ello, basta con colocar la orden de mapeo en el *Archivo de comandos de inicio de sesión*. Generalmente los recursos compartidos comienzan a nombrarse a partir de la letra *F*, pero se puede usar cualquier otra letra de unidad que no esté siendo usada. La orden de mapeo, teniendo esto en cuenta, sería:

```
NET USE F: \\NOMBRE_SERV\NOMBRE_RECURSO
```

Si el nombre del servidor es *ALFA* y el nombre del recurso compartido es *SYS*, la orden sería:

```
NET USE F: \\ALFA\SYS
```

## Conocimientos Necesarios sobre OS/2

La distribución del antivirus a través de una red OS/2 precisa de unos conocimientos mínimos sobre dicho sistema. A continuación se describirán los conceptos que se precisa conocer ilustrándolos con ejemplos de cómo preparar el sistema de manera adecuada.

### Comandos que se ejecutan cuando se inicia una sesión de red

Habitualmente, cuando un ordenador arranca, se ejecutan una serie de comandos definidos en un fichero. En el caso de MS-DOS o Windows, dicho fichero es el *AUTOEXEC.BAT*.

De igual manera, también es habitual que, cuando un ordenador se conecta a una red, se ejecuten una serie de comandos. A esta serie de comandos y/o programas se la conoce como *login script* o guión de entrada. En el caso de OS/2, cada usuario tiene un fichero llamado *PROFILE.BAT* (o *PROFILE.COMD*) que se ejecuta cada vez que el usuario se conecta a la red.

Como cada usuario tiene su propio archivo de comandos de inicio de sesión, hay que modificar el archivo *PROFILE.BAT* de cada uno de los usuarios a los que se quiera distribuir. El inconveniente es que las futuras modificaciones también suponen la edición de todos los ficheros *PROFILE.BAT*. Esto se puede evitar creando un fichero *BAT* que contenga las líneas necesarias para la distribución del antivirus y llamando a dicho fichero desde los correspondientes ficheros *PROFILE.BAT*. De esta forma, cualquier modificación futura bastará con hacerla sobre el fichero *BAT* creado afectando así a todos los usuarios.

Dado que el login script se ejecuta cada vez que un usuario se conecta a la red, es el lugar adecuado para lograr la distribución del antivirus a los puestos. Bastará con ejecutar en el login script el programa de distribución de antivirus de Panda Software para que el mencionado antivirus se vaya distribuyendo a todos los puestos a medida que se vayan conectando a la red.

### Asociación de una letra de unidad

En este apartado se procederá a explicar el concepto de *mapeo*. En un ordenador, el disco duro se suele identificar con la letra *C*, la disquetera con la letra *A* o *B* y el CD-ROM con la *D*, la *E*, etc. dependiendo de los discos duros instalados.

En el caso de una red OS/2, el concepto de *mapeo* va relacionado con el concepto de *recurso compartido*. La totalidad o cualquier parte del disco duro del servidor (o de los discos si tiene varios) puede compartirse y convertirse así en un *recurso compartido*. Estos recursos compartidos son los que deben mapearse para luego poder referirse a ellos desde las estaciones.

Es muy interesante que todas las estaciones tengan el mismo *mapeo* para así asegurarse de que, para todas ellas, los distintos recursos compartidos del servidor se referencian igual. Para ello, basta con colocar la orden de mapeo en el archivo *PROFILE* de cada usuario. Generalmente los recursos compartidos comienzan a nombrarse a partir de la letra *F*, pero se puede usar cualquier otra letra de unidad que no esté siendo usada. La orden de mapeo, teniendo esto en cuenta, sería:

```
NET USE F: \\NOMBRE_SERV\NOMBRE_RECURSO
```

Si el nombre del servidor es *ALFA* y el nombre del recurso compartido es *SYS*, la orden sería:

```
NET USE F: \\ALFA\SYS
```



## Sintaxis de los Comandos de los Scripts (.SRC)

A lo largo de esta documentación, se habrá observado que siempre se pasa un parámetro al programa *RINSTALL*. Este parámetro es el nombre de un fichero de extensión *SCR* (ficheros de script). Un fichero de script es un fichero de texto dividido en secciones donde se indica un comando por cada línea. El fichero de script es el que determina el comportamiento del programa *RINSTALL*.

Los ficheros *SCR* adecuados para *RINSTALL* pueden tener 6 secciones diferentes:

Sección común [*COMMON*]: estos mandatos se ejecutan siempre.

Sección DOS [*DOS*]: los mandatos de esta sección se ejecutan bajo MS-DOS, Windows 95 y Windows 3.1x.

Sección Windows 3.1x [*WIN*]: los mandatos de esta sección se ejecutan bajo MS-DOS, Windows 95 y Windows 3.1x pero sólo si se localiza el directorio de Windows 3.1x en el disco duro de la estación de trabajo.

Sección Windows 95 [*WIN95*]: los mandatos de esta sección se ejecutan bajo MS-DOS, Windows 95 y Windows 3.1x pero sólo si se localiza el directorio de Windows 95 en el disco duro de la estación de trabajo.

Sección Windows NT [*WINNT*]: los mandatos de esta sección se ejecutan únicamente bajo Windows NT.

Sección OS/2 [*OS/2*]: los mandatos de esta sección se ejecutan únicamente bajo OS/2.

Hay tres tipos de mandatos:

- Ficheros a copiar:** todas las líneas que NO comiencen con el carácter #, indican un fichero que deberá estar presente en el directorio de origen y que se deberá copiar al directorio destino. Por defecto, los ficheros sólo se copiarán si no existen en el directorio destino o si el fichero presente en el directorio de destino es más antiguo que el que se encuentra en el directorio de origen.
- Asignaciones:** estos mandatos comienzan por el carácter # y tienen la siguiente estructura: *#Variable = valor*. Sirven para asignar un cierto valor a una variable. A continuación se detallan las distintas variables disponibles en los ficheros script (*SCR*).

Nombre de variable	Descripción
<i>Win3xDir</i>	Directorio de Windows 3.1x
<i>Win95Dir</i>	Directorio de Windows 95
<i>WinNTDir</i>	Directorio de Windows NT
<i>BaseSourcePath</i>	Directorio de origen base

*BaseTargetPath* Directorio de destino base  
*RelSourcePath* Directorio de origen relativo  
*RelTargetPath* Directorio de destino relativo

*SourcePath* BaseSourcePath + RelSourcePath  
*TargetPath* BaseTargetPath + RelTargetPath

*CopyMode* Indica las condiciones de copia de los ficheros. Puede tomar tres valores. *COPY* indica que se copiarán los ficheros sólo si no existen en el directorio destino. *UPDATE* indica que se copiarán los ficheros sólo si la versión a copiar es más reciente que la existente en el directorio destino. *OVERWRITE* indica que los ficheros se copiarán siempre. *ONCHANGE* indica que se realizará la copia sólo si el fichero origen es distinto que el fichero destino, no teniendo en cuenta si éste es más antiguo o no.

*ErrorMode* Indica si deben mostrarse o no los mensajes de error. Se le puede asignar un valor 0 (no se mostrarán los mensajes) o un valor 1 (sí se mostrarán los mensajes).

**3. Funciones:** estos mandatos también comienzan con el carácter #, y sirven para llevar a cabo determinadas operaciones. Su sintaxis es la siguiente: *#Función parámetro1, parámetro2, ...*. Las distintas funciones disponibles son:

#### *AddProfileEntry*

Esta función añade una entrada en una sección de un archivo tipo *INI*. Recibe 4 parámetros:

Parámetro 1: indica la sección en la que crear la entrada.  
Parámetro 2: indica el campo (la 1ª parte de la entrada).  
Parámetro 3: indica el valor (la 2ª parte de la entrada).  
Parámetro 4: indica la ruta al archivo INI.

Ejemplo:

```
#AddProfileEntry Windows, Load,  
f:\pavfn\winkir.exe, c:\windows\win.ini
```

#### *AppendLine*

Esta función añade una línea a un fichero de texto. Recibe 3 parámetros:

Parámetro 1: indica la ruta al fichero de texto.  
Parámetro 2: indica la línea de texto a añadir.  
Parámetro 3: *LITERAL* (es opcional). Indicando este parámetro, nos aseguramos de que la línea de texto figure tal y como se ha escrito eliminando cualquier modificación que se haya podido introducir.

Ejemplo:

```
#AppendLine c:\autoexec.bat,  
c:\pavfn\sentinel.com
```

### ***AppendLineBefore***

Esta función añade una línea a un fichero de texto pero siempre antes otra línea especificada. Recibe 4 parámetros:

- Parámetro 1: indica la ruta al fichero de texto.
- Parámetro 2: indica la línea de texto a añadir.
- Parámetro 3: indica la línea de texto posterior a la que se inserta.
- Parámetro 4: *LITERAL* (es opcional). Indicando este parámetro, nos aseguramos de que la línea de texto figure tal y como se ha escrito eliminando cualquier modificación que se haya podido introducir.

Ejemplo:

```
#AppendLineBefore c:\autoexec.bat,  
c:\pavfn\sentinel.com, win, LITERAL
```

### ***DeleteLine***

Esta función sirve para borrar una línea de un fichero de texto. Recibe 2 parámetros:

- Parámetro 1: indica la ruta al fichero de texto.
- Parámetro 2: indica la línea de texto a borrar.

Ejemplo:

```
#DeleteLine c:\autoexec.bat,  
c:\pavfn\sentinel.com
```

### ***InsertLine***

Esta función sirve para insertar una línea al principio de un fichero de texto. Recibe 3 parámetros:

- Parámetro 1: indica la ruta al fichero de texto.
- Parámetro 2: indica la línea de texto a insertar.
- Parámetro 3: *LITERAL* (es opcional). Indicando este parámetro, nos aseguramos de que la línea de texto figure tal y como se ha escrito eliminando cualquier modificación que se haya podido introducir.

Ejemplo:

```
#InsertLine c:\autoexec.bat,  
c:\pavfn\sentinel.com
```

### ***MakeDir***

Esta función crea un directorio. Recibe un parámetro:

- Parámetro 1: indica la ruta al directorio a crear.

Ejemplo:

```
#MakeDir c:\pavfn
```

#### **NoWinLoad**

Dentro del fichero *WIN.INI* hay una sección [*Windows*] que tiene una entrada llamada *Load*. Este comando hace que se carguen una serie de programas al entrar en Windows. Puede haber más de un programa en el mismo comando *Load*. El mandato *NoWinLoad* elimina el programa que se desee del comando *Load*. Recibe un parámetro:

Parámetro 1: indica el programa que se quiere no cargar.

Ejemplo:

```
#NoWinLoad c:\pavfn\winkir.exe
```

#### **ReplaceLine**

Esta función reemplaza una línea de un fichero de texto. Recibe 3 parámetros:

Parámetro 1: indica la ruta al fichero de texto.

Parámetro 2: indica la línea de texto a sustituir.

Parámetro 3: indica la nueva línea de texto.

Ejemplo:

```
#ReplaceLine c:\autoexec.bat,  
«TargetPath»SENTINEL.COM,  
«TargetPath»SENTINEL.COM /OE
```

#### **SetProfileEntry**

Esta función asigna un valor a una entrada en una cierta sección de un archivo *INI*. La función intenta encontrar la mencionada sección. Si la encuentra, le asigna el valor. Si no, crea la entrada y le asigna el valor. En caso de no existir la sección, también se crearía. Recibe 4 parámetros:

Parámetro 1: indica la sección del fichero INI

Parámetro 2: indica el campo (la 1ª parte de la entrada)

Parámetro 3: indica el valor (la 2ª parte de la entrada)

Parámetro 4: indica la ruta al archivo INI.

Ejemplo:

```
#SetProfileEntry Windows, Load,  
c:\pavfn\winkir.exe, c:\windows\win.ini
```

#### **WinLoad**

Dentro del fichero *WIN.INI* hay una sección [*Windows*] que tiene una entrada llamada *Load*. Este comando hace que se carguen una serie de programas al entrar en Windows. Puede haber más de

un programa en el mismo comando *Load*. El mandato *WinLoad* añade el programa que se desee al comando *Load*. Recibe un parámetro:

Parámetro 1: indica el programa que se quiere cargar.

Ejemplo:

```
#WinLoad c:\pavfn\winkir.exe
```

#### ***AdminRequired***

Mediante esta función se indica que desde ese momento y hasta que no aparezca una línea con la función *EndAdminRequired*, es necesario ser administrador para poder ejecutar todo el bloque de comandos (los que se encuentren entre *#AdminRequired* y *#EndAdminRequired*). La función sólo tiene efecto cuando el *RInstall* se ejecuta con el parámetro */Local*. Esta función no admite parámetros.

Ejemplo:

```
#adminRequired
```

#### ***EndAdminRequired***

Cuando aparece esta función se indica que todos los comandos siguientes se podrán ejecutar sin necesidad de ser administrador. Solamente tiene efecto cuando *RInstall* se ejecuta con el parámetro */Local*. Esta función no admite parámetros.

Ejemplo:

```
#EndAdminRequired
```

#### ***ResetMode***

Indica si se el equipo se debe reiniciar en ese momento o, en caso de ser necesario, si no se reiniciará. El valor 0 significa que no se produce el reinicio, mientras que el 1 significa que éste se debe producir en ese mismo instante. En cualquiera de los dos casos se presentará un aviso.

#### ***CheckSpace***

Mediante este comando se comprueba la existencia de espacio (en Mb) existente en el destino. En caso de no encontrarlo, presenta un aviso y no se realiza la copia de ficheros.

Parámetro 1: indica el tamaño necesario en Mb.

Ejemplo:

```
#CheckSpace 8
```

#### ***CopyFileAs***

Realiza la copia de un fichero desde un origen hasta su destino indicando el modo de copia y hace posible que el fichero cambie de nombre es dicho destino. Admite tres parámetros:

Parámetro 1: indica la ruta original del fichero.

Parámetro 2: indica destino el fichero destino.

Parámetro 3: indica el modo de copia, mediante las siguientes posibilidades: *COPY* (el fichero sólo se copiará si no existe ya en el destino), *UPDATE* (el fichero sólo se copiará si la versión a copiar es más reciente que la ya existente en el destino), *OVERWRITE* (el fichero siempre se copiará, aunque origen y destino sean iguales) y *ONCHANGE* (se copiará siempre que los ficheros origen y destino sean distintos).

#### *DeleteDirDelayed*

Cuando finaliza la ejecución de *RInstall* (después de los comandos *#Run*), este comando borra un directorio completo, incluyendo los subdirectorios.

Parámetro 1: indica el directorio a borrar.

Ejemplo:

```
#DeleteDirDelayed c:\pavfn
```

#### *ExchangeRequired*

Mediante dicho comando se indica la necesidad de tener instalado un cliente de Exchange/Outlook para seguir procesando la sección en la que se encuentra. No admite ningún parámetro.

Ejemplo:

```
#ExchangeRequired
```

#### *EndExchangeRequired*

Mediante dicho comando se indica que ya no es necesario tener instalado un cliente de Exchange/Outlook para seguir procesando la sección en la que se encuentra. No admite ningún parámetro.

Ejemplo:

```
#EndExchangeRequired
```

## Imprimir esta Ayuda

Gracias a esta ayuda podrás consultar cualquier tema referente a Panda Antivirus Platinum para Exchange/Outlook. Sin embargo también puedes imprimir secciones concretas de la misma, o ésta en su totalidad.

- Si deseas imprimir un tema concreto, colócate en él y pulsa el botón **Imprimir** en la barra de botones.
- Si deseas imprimir un capítulo completo (libro con sus hojas), pulsa el botón **Temas de Ayuda** y selecciona dicho libro en la ficha principal de la ayuda (**Contenido**). Entonces, pulsa el botón **Imprimir...**
- Si deseas imprimir TODA la ayuda al completo, pulsa el botón **Imprimir Ayuda Completa**, en la barra de botones. También puedes utilizar el botón que aparece bajo estas líneas (**Imprimir TODA esta Ayuda**) o pulsar [aquí](#).

```
{button Imprimir TODA esta
Ayuda,IF(InitMPrint(),`MPrintId(`50'):MPrintId(`999'):MPrintId(`30'):MPrintId(`20'):MPrintId(`40'):MPrint
Id(`41'):MPrintId(`42'):MPrintId(`1005'):MPrintId(`43'):MPrintId(`44'):EndMPrint())}
```

**NOTA:** la impresión de la ayuda en su totalidad puede llevar bastante tiempo. Dependiendo de tu impresora y las configuraciones que tengas establecidas, podrá ocupar 31 páginas, aproximadamente.

## Lista de Extensiones

La lista de extensiones engloba todos los tipos de ficheros (todas las extensiones) que el antivirus debe eliminar si los encuentra incluidos en los mensajes. Para ver y modificar esta lista es necesario acceder a la pestaña **Protección Permanente** (correspondiente a la configuración) y pulsar el botón **Extensiones**. En cualquier momento, puedes agregar a esta lista otros tipos de extensiones, o eliminar de ella cualquiera de los tipos ya incluidos.

Para agregar una nueva extensión a la lista, escríbela en la sección **Nueva extensión** y pulsa el botón **Añadir**.

Para borrar alguna de las extensiones de la lista, selecciónala en ella y pulsa el botón **Eliminar**.

Si lo que deseas es borrar todas las extensiones de la lista, pulsa el botón **Limpiar lista**. Siempre podrás reestablecer la lista original (la que viene preparada de fábrica, o por defecto), pulsando el botón **Restaurar**.

Cuando hayas realizado cambios que estimes oportunos en la lista, pulsa el botón **Aceptar** para salir guardando y aplicándolos, o el botón **Cancelar** para que éstos no tengan efecto.

