Introducción

Panda Antivirus

Panda Antivirus es una solución completa y eficaz para mantener protegido su ordenador frente a cualquier tipo de virus. Se incluyen versiones Windows 95, Windows NT Workstation, Windows 3.1x, DOS y OS/2 para que Vd. esté protegido sea cual sea su sistema operativo. Esta ayuda es la correspondiente a **Panda Antivirus** para Windows NT Workstation.

Estrategias de protección

Panda Antivirus comprende varias estrategias de protección frente a los virus:

- **Protección permanente:** la protección permanente se encarga de proteger el ordenador frente a los virus en todo momento y sin requerir la intervención del usuario. La gran ventaja de esta estrategia de protección es que permite tener protegido el ordenador de una forma completamente automática.
- **Análisis bajo demanda:** el análisis bajo demanda permite analizar cualquier parte del ordenador a petición del usuario. Se debe elegir el área a analizar y en ese momento comenzará el análisis en busca de virus en el área señalada.
- **Desinfección:** una vez encontrado un virus, hay varias posibles acciones a llevar a cabo. Una de ellas es la desinfección que consiste en eliminar el virus del fichero dejando éste tal y como estaba antes de la infección.
- **Análisis heurístico:** el análisis heurístico es una técnica de análisis alternativa a las ya mencionadas. El análisis heurístico funciona bajo demanda. Es decir, el usuario debe indicar qué área del ordenador desea analizar con este método en un momento determinado. Esta técnica de análisis está preparada para encontrar virus desconocidos.
- **Búsqueda de cadenas:** al igual que el análisis heurístico, es una técnica de análisis alternativa y también funciona bajo demanda del usuario. Su utilidad es la búsqueda de nuevos virus a partir de datos ofrecidos por el soporte técnico de Panda Software.
- **Otras opciones:** bajo este apartado se engloban ciertas capacidades del antivirus destinadas a ofrecer información o a facilitar la gestión del mismo. Por ejemplo, se cuenta con un informe de resultados en el que se pueden ver las distintas incidencias y operaciones que se han llevado a cabo con el antivirus.

Soluciones antivirus Panda Software

Panda Software le ofrece las siguientes soluciones antivirus:

- **24h-365d® Seguro Antivirus® para PCs Individuales**. *Licencias.*
- **24h-365d® Seguro Antivirus® para PCs en red** (distribución automática desde servidores).
- **24h-365d® Seguro Antivirus® para Servidores de red** (Novell NetWare y Windows NT Server).
- **24h-365d® Seguro Antivirus® para Redes Locales**.
- **24h-365d® Seguro Antivirus® para clientes de e-mail y Groupware**.
- **24h-365d® Seguro Antivirus® para Servidores de e-mail y Groupware**.
- **24h-365d® Seguro Antivirus® para Servidores de Correo SMTP**.
- **24h-365d® Seguro Antivirus® para PCs conectados a Internet**.
- **24h-365d® Seguro Antivirus® para Servidores de Internet (SMTP, FTP y HTTP)**.

- **24h-365d® Seguro Antivirus® para Proxys**.

¿Qué es 24h-365d Seguro Antivirus Panda Software?

24h-365d® Seguro Antivirus® Panda Software, es un nuevo y revolucionario concepto de protección antivirus que aporta aún más seguridad. **24h-365d® Seguro Antivirus® Panda Software** es una extraordinaria combinación de productos y servicios que ofrece los más altos niveles de protección frente a los virus. **24h-365d® Seguro Antivirus® Panda Software** se puede contratar con diferentes tiempos de derecho a actualizaciones y con distintos periodos de actualización.

El producto lo aporta **Panda Antivirus**, un antivirus que ha logrado los certificados más exigentes en detección de virus como son:

- El **Certificado ICSA:** otorgado por la prestigiosa organización norteamericana ICSA a los productos antivirus que detectan periódicamente el 100% de los virus *In the Wild* (los virus más extendidos en cada momento) y más de un 90% de la *Zoo Collection* (colección de miles de virus menos extendidos).
- El **Certificado CheckMark:** otorgado por la revista inglesa especializada en Seguridad Informática *Secure Computing*.

Si usted no dispone de **24h-365d® Seguro Antivirus® Panda Software**, puede contratarlo utilizando la orden de pedido incluida en la tarjeta de registro. Los servicios ofrecidos por **24h-365d® Seguro Antivirus® Panda Software** son los siguientes:

- **Hot-Line:** durante UN año solucionaremos sus problemas técnicos por teléfono, fax, Internet o e-mail. Llame cuando llame, a cualquier hora del día o de la noche, Vd. encontrará técnicos al otro lado, personas altamente cualificadas que están a su disposición 24 horas al día, los 365 días del año. Este es un servicio exclusivo de **Panda Software**.
- **S.O.S. Virus:** si Vd. encuentra algún virus que **Panda Antivirus** no detecta o no elimina, enviaremos un mensajero a su domicilio (o recogeremos la muestra sospechosa de cualquier otro modo) y en menos de 24 horas desarrollaremos una nueva versión capaz de detectar y eliminar al nuevo virus. Le enviaremos esta nueva versión sin coste alguno.
- **Servicio de Actualizaciones con entrega a domicilio:** su antivirus estará totalmente actualizado. Vd. recibirá en su propio domicilio actualizaciones mensuales o trimestrales en CD o en disquetes si ha contratado nuestra solución **24h-365d® Seguro Antivirus® Panda Software**. También podrá actualizar el producto a través de nuestro WEB tantas veces como lo desee durante un año, garantizándole como mínimo una actualización nueva cada día.
- **Servicio WEB:** resolución de las dudas más frecuentes e información sobre virus.

Instalación

Requisitos

Para instalar **Panda Antivirus** para Windows NT Workstation se precisa de los siguientes elementos:

- Ordenador compatible con IBM con procesador 486 o superior.
- 16 Mb de RAM.
- 4 Mb de espacio en disco duro.
- Sistema operativo Windows NT 3.51 o superior.
- Unidad de CD-Rom.
- Ratón.

Procedimiento de instalación

Hay dos versiones de **Panda Antivirus** para Windows NT Workstation. Una de ellas corresponde a la versión 3.51 del mencionado sistema operativo y la otra a la versión 4.0. Se debe tener la precaución de instalar la versión correspondiente a cada sistema operativo.

Ambas versiones se pueden instalar únicamente desde el CD-Rom que acompaña al producto. Para instalar cualquiera de las dos versiones, hay que ejecutar el programa CDMENU.COM. Este programa presenta un sencillo menú de opciones. En primer lugar hay que elegir el idioma deseado y luego la versión que se quiere instalar. En este caso se debe elegir una de las dos versiones de **Panda Antivirus** para Windows NT, la 3.51 o la 4.0 en función del sistema operativo que se tenga instalado.

Para poder instalar la versión de **Panda Antivirus** para Windows NT Workstation es necesario que tenga derechos de administrador sobre su máquina. Esto es así debido a los derechos necesarios para instalar el driver que se encarga de la protección permanente.

El procedimiento de instalación consta de los siguientes pasos:

1. En primer lugar se presenta una pantalla de bienvenida.
2. Seguidamente se preguntan los datos del usuario.
3. Se pide el directorio en el que se desea instalar la aplicación.
4. Se solicita el grupo de programas en el que se crearán los iconos de acceso al antivirus.
5. Se da a elegir si se quiere instalar la protección permanente (driver **Sentinel**) o no.
6. Comienza la copia de ficheros al disco duro.
7. Una vez que haya acabado la copia de ficheros, se recomienda reinicar la máquina para que la protección permanente entre en funcionamiento.

Actualización del antivirus

Para actualizar una versión con una actualización recibida, basta con instalar la nueva versión sobre la antigua.

Desinstalación

Si se trata de la versión para Windows NT 3.51, la desinstalación de **Panda Antivirus** se realiza mediante el programa UNINST que se encuentra en el grupo de programas de la aplicación.

Si se trata de la versión para Windows NT 4.0, la desinstalación de **Panda Antivirus** se realiza mediante la opción *Agregar o quitar programas* del *Panel de Control*. Basta con elegir **Panda Antivirus Windows NT W/S 4.0** de la lista que se presenta en dicha opción y pulsar el botón *Agregar o Quitar*. Para completar la desinstalación, es necesario reiniciar la máquina.

No debe intentar desinstalar la versión borrando la carpeta donde haya instalado el antivirus. Desinstale siempre siguiendo el procedimiento descrito.

Qué es la protección permanente

La protección permanente es un programa que, desde el arranque de la máquina, intercepta todas aquellas operaciones que suponen riesgo de contagio para verificar que ningún virus entre en el sistema.

La protección permanente funciona de manera totalmente automática y sin requerir ninguna intervención por parte del usuario. A pesar de la vigilancia constante, el rendimiento del sistema no se ve afectado por lo que la instalación de la protección permanente es siempre aconsejable dado que aumenta considerablemente la protección del ordenador.

Cómo se usa la protección permanente

La protección permanente es una de las opciones de la instalación. Si se ha elegido instalar dicha protección, una vez que se arranque la máquina, la protección permanente (**Sentinel**) estará en funcionamiento.

Si el sistema operativo es Windows NT Workstation 3.51, **Sentinel** aparecerá como un icono minimizado en el escritorio de Windows. Si el sistema operativo es Windows NT Workstation 4.0, **Sentinel** aparecerá como un icono junto al reloj situado en la barra de tareas.

El funcionamiento de la protección permanente es totalmente automático. Si, en alguna operación, **Sentinel** detectara la presencia de un virus, avisaría de tal circunstancia y llevaría a cabo la acción pertinente.

Cómo se configura la protección permanente

La protección permanente se puede configurar para adaptarse a las necesidades de cada usuario. Haciendo doble clic sobre el icono de **Sentinel**, aparece una ventana con varias pestañas. Cada una de ellas hace referencia a la configuración de los distintos aspectos de **Sentinel**. Las opciones de configuración son las siguientes:

Estado

En esta pestaña se define el estado de la protección permanente.

- **Activado:** mediante esta opción, se activa o desactiva la protección permanente. Hay que tener en cuenta que, si se desactiva la protección permanente, el ordenador quedará desprotegido frente a los virus.
- **Entradas:** estando la protección permanente activada, esta opción indica que se deben analizar todas aquellas entradas de ficheros en la máquina. También se analizarán las creaciones de ficheros y las modificaciones de los mismos.
- **Salidas:** estando la protección permanente activada, esta opción indica que se deben analizar todas aquellas salidas de ficheros de la máquina. Se analizarán también todas las aperturas y ejecuciones de ficheros.
- **Renombrado:** estando la protección permanente activada, esta opción indica que se deben analizar en busca de virus todas las operaciones de renombrado de ficheros.
- **Red Microsoft:** si la protección permanente está activada, esta opción indica que se deben analizar en remoto todas las operaciones efectuadas sobre una unidad de red Microsoft.
- **Red Novell:** si está activa la protección permanente, esta opción indica que se analicen en remoto todas las operaciones efectuadas sobre una unidad de red Novell.

Información

En esta pestaña se muestran diversas informaciones referentes a la actividad de la protección permanente.

- **Revisados:** indica el número de ficheros que la protección permanente ha revisado en busca de virus desde el inicio del sistema.
- **Infectados:** esta información muestra el número de ficheros infectados que se han encontrado.
- **Desinfectados:** indica el número de ficheros desinfectados por la protección permanente.
- **Renombrados:** se muestra aquí el número de ficheros que la protección permanente ha renombrado.
- **Borrados:** en este punto se muestra el número de ficheros borrados por la protección permanente por estar contaminados con virus.
- **Movidos:** se informa aquí de cuántos ficheros ha movido la protección permanente por estar contaminados con virus.
- **Virus encontrados:** por último, se indica aquí cuántos virus se han encontrado.

Extensiones analizables

En este apartado se configuran las extensiones que la protección permanente debe analizar.

- **Lista de extensiones:** en la lista de extensiones se pueden marcar todas aquellas extensiones que se desean analizar. La protección permanente intercepta siempre todos los ficheros a los que se accede pero sólo analizará aquellos ficheros que tengan una de las extensiones seleccionadas. Independientemente de la selección de extensiones que se haga, los ficheros EXE y COM se analizarán siempre.
- **Extensiones en lista:** este dato informa del número de extensiones que hay en la lista.
- **Extensiones activas:** este dato informa de las extensiones que se han marcado en la lista para analizar.
- **Añadir extensión:** para añadir una extensión a la lista, se debe escribir la extensión en la casilla a tal efecto y pulsar el botón *Añadir*.
- **Eliminar extensión:** para eliminar una extensión de la lista, se debe seleccionar en la lista la extensión a eliminar y pulsar el botón *Eliminar*.
- **Todos los ficheros:** si se marca esta opción, se analizarán todos los ficheros independientemente de las extensiones que se hayan seleccionado.
- **Analizar ficheros comprimidos:** si se marca esta opción, se analizarán los ficheros comprimidos a los que se acceda.

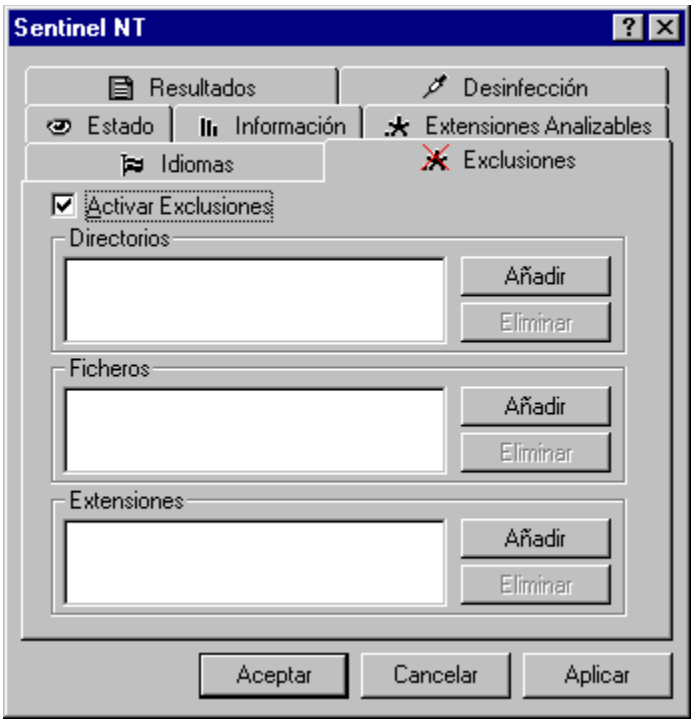
Idiomas

En esta pestaña se puede consultar el idioma en el que se encuentra la protección permanente y también se puede elegir otro idioma en la lista de idiomas disponibles.

- **Idiomas disponibles:** se muestra una lista con los distintos idiomas disponibles para la protección permanente. Para cambiar de idioma, basta con seleccionar el idioma deseado y pulsar el botón *Aceptar* o el botón *Aplicar*.
- **Idioma actual:** aquí se muestra el idioma en el que se encuentra en ese momento la protección permanente.

Exclusiones

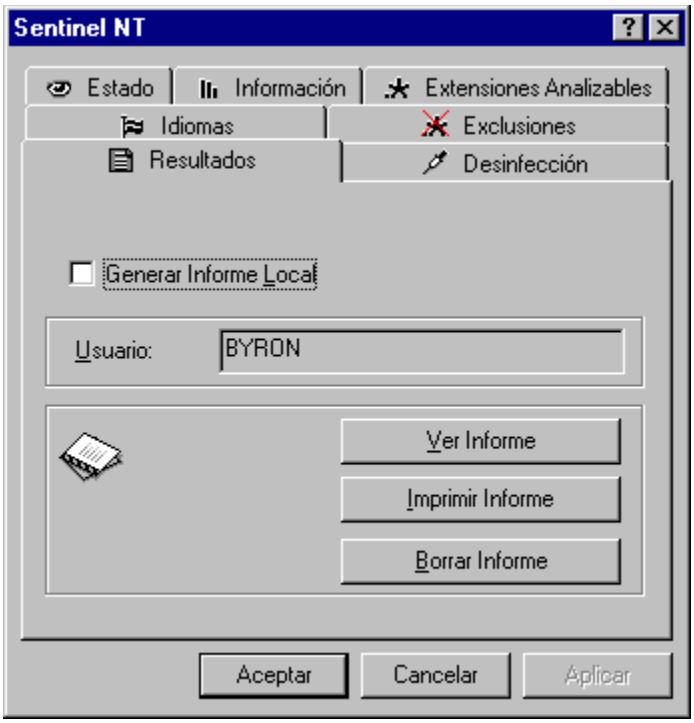
En esta pestaña se pueden indicar aquellas áreas, ficheros o extensiones que no se deseen analizar. Independientemente de lo que se haya indicado en *Extensiones*, todas aquellas áreas, ficheros o extensiones que se marquen aquí, **no se analizarán**.



- **Activar exclusiones:** si se marca esta opción, se activará la función de exclusión en función de los datos que se hayan indicado.
- **Directorio:** en este apartado se muestra una lista con todos aquellos directorios que no se deberán analizar.
- **Añadir directorio:** mediante esta opción, se pueden añadir directorios a la lista de directorios que no se analizarán.
- **Eliminar directorio:** mediante esta opción, se pueden eliminar directorios de la lista de directorios que no se analizarán.
- **Fichero:** en este apartado se muestra una lista con los ficheros que no se deben analizar.
- **Añadir fichero:** esta opción permite añadir un fichero a la lista de ficheros que no se analizan.
- **Eliminar fichero:** esta opción permite eliminar un fichero de la lista de ficheros que no se analizan.
- **Extensiones:** en este apartado se muestra una lista de las extensiones que no se deben analizar. Aunque alguna de estas extensiones esté en la lista de extensiones a analizar, no se analizará.
- **Añadir extensión:** gracias a esta opción, se puede añadir una extensión a la lista de extensiones no analizables.
- **Eliminar extensión:** gracias a esta opción, se puede eliminar una extensión de la lista de extensiones que no se analizan.

Resultados

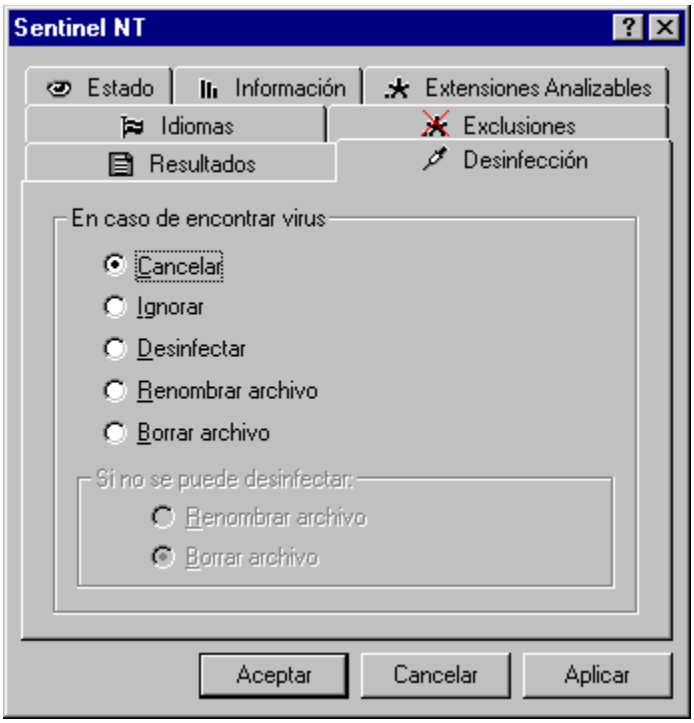
En esta pestaña se configura el comportamiento del sistema de informes de incidencias encontradas por la protección permanente.



- **Generar informe local:** si se activa esta opción, se generará un informe con las distintas incidencias que encuentre la protección permanente.
- **Usuario:** aquí se muestra el nombre del usuario de la máquina.
- **Ver informe:** este botón muestra el informe con las incidencias encontradas hasta el momento.
- **Imprimir informe:** gracias a este botón, se puede imprimir el informe de incidencias.
- **Borrar informe:** mediante este botón, se puede borrar el informe de incidencias.

Desinfección

En esta pestaña se configura el comportamiento de la desinfección de ficheros contaminados por virus y detectados por la protección permanente.



- **Cancelar:** si se marca esta opción, la operación en la que se haya detectado el virus será cancelada. Si, por ejemplo, el virus ha sido detectado en un fichero que se intentaba ejecutar, se cancelará la ejecución del mencionado fichero.
- **Ignorar:** con esta opción marcada, aunque se encuentre un virus se ignorará dicho suceso.
- **Desinfectar:** si se marca esta opción y la protección permanente detecta un virus, procederá a su desinfección dejando el fichero contaminado tal y como estaba antes de la infección.
- **Renombrar archivo:** con esta opción marcada, si se detecta un virus, **Sentinel** renombrará el fichero para que tenga extensión VIR.
- **Borrar archivo:** si se marca esta opción y **Sentinel** detecta un virus en un fichero, se procederá a borrar dicho fichero.
- **Si no se puede desinfectar, renombrar archivo:** si esta opción está activa, cuando **Sentinel** detecte un virus e intente desinfectarlo, en caso de no poder realizar dicha operación con éxito, el fichero se renombrará.
- **Si no se puede desinfectar, borrar archivo:** si esta opción está activa, cuando **Sentinel** detecte un virus e intente desinfectarlo, en caso de no poder realizar dicha operación con éxito, el fichero se borrará.

Qué es el análisis bajo demanda

El análisis bajo demanda le permite analizar cualquier área de su ordenador en el momento que Vd. elija. Cada análisis que se realiza se puede configurar mediante un conjunto de sencillas opciones.

Cómo se usa el análisis bajo demanda

Para realizar un análisis bajo demanda, hay que llevar a cabo los siguientes pasos:

1. **Ejecutar el antivirus:** para ejecutar el antivirus, vaya al grupo de programas donde se hayan creado los iconos que permiten su ejecución. Haga doble clic sobre el icono *Panda Antivirus*.
2. **Ir al apartado de análisis:** para ir a este apartado, pulse el botón *Analizar* en la barra de botones de la aplicación. Aparecerá una ventana para especificar qué se debe analizar y cómo se debe hacerlo.
3. **Escoger el área de análisis:** se debe elegir el área que se desea analizar. En una lista se muestran las distintas unidades reconocidas en el sistema. También se puede indicar un directorio o un fichero concreto mediante los botones a tal efecto.
4. **Configurar las extensiones:** este paso es opcional. El programa guarda la configuración de las extensiones que se quieren analizar. Por tanto, una vez configuradas, no hay por qué repetir la configuración en cada análisis.
5. **Configurar las opciones de análisis:** este paso también es opcional. El programa guarda la configuración de las opciones de análisis. Por tanto, una vez configurado el análisis, no hay por qué repetir la configuración en cada análisis. Sólo deberá variarse dicha configuración cuando se desee escoger un conjunto de opciones diferente. Cuenta con una explicación más detallada de las opciones de análisis en esta misma documentación en el apartado de configuración.
6. **Indicar si se quiere analizar únicamente el boot:** este paso es opcional. Si se marca esta opción, de las unidades seleccionadas sólo se analizará el boot y no los ficheros. Si no se marca esta opción, se analizarán tanto el boot como los ficheros en todas las unidades seleccionadas.
7. **Comenzar el análisis:** el botón *Analizar* da comienzo al análisis en busca de virus en las áreas seleccionadas y con las opciones escogidas.

Cómo se configura el análisis bajo demanda

Tal y como se ha mencionado, en un análisis se debe indicar:

- Qué área se quiere analizar.
- Qué extensiones se considerarán en el análisis.
- Cómo se va a llevar a cabo el análisis.

La configuración de un análisis comprende indicar qué extensiones se van a considerar y las opciones de análisis.

Extensiones

Pulsando el botón *Extensiones* aparece una ventana que permite indicar qué extensiones se desean analizar.

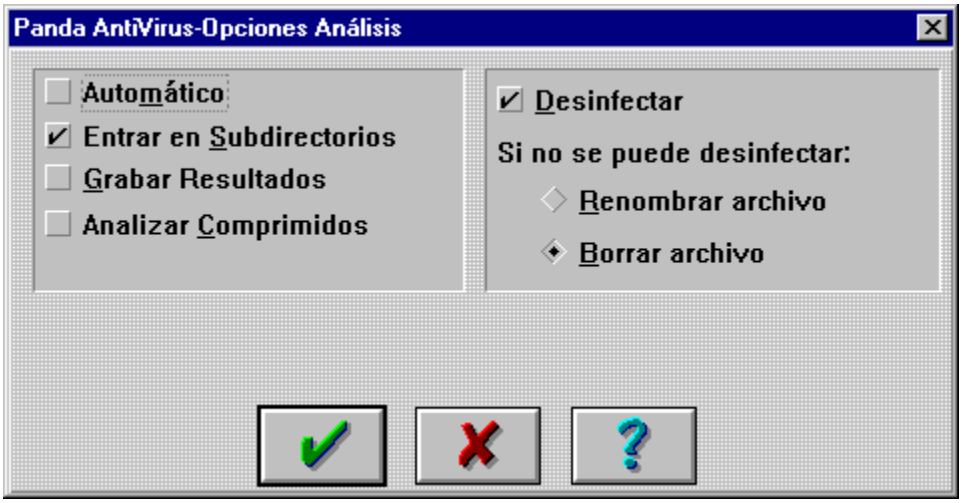
La opción *Todas* sobre la lista de extensiones indica que se analizarán todos los ficheros con independencia de su extensión. Si esta opción no está marcada, sólo se analizarán los ficheros cuya extensión coincida con alguna de las de la lista.

Dos botones permiten añadir y eliminar extensiones a la lista. Por defecto, se proporciona una lista con las extensiones más comunes y una selección de aquellas extensiones susceptibles de albergar virus.

Independientemente de la selección de extensiones que se haga, los ficheros EXE y COM se analizarán siempre.

Opciones de análisis

Pulsando el botón *Opciones* aparece una ventana que permite elegir las opciones de análisis que son las siguientes:



- **Automático:** si se marca esta opción, el proceso de análisis será completamente automático. Si se encuentran virus, el proceso informará de ello pero continuará y no se verá interrumpido. Esto es especialmente útil cuando el ordenador tiene muchos ficheros infectados y se están desinfectando.
- **Entrar en subdirectorios:** si se marca esta opción, se analizarán los subdirectorios encontrados en las áreas que se estén analizando. Si no se marca dicha opción, no se analizarán los subdirectorios encontrados con lo que si se escoge analizar una unidad pero no se marca esta opción, únicamente se analizará el directorio raíz de la misma.
- **Grabar resultados:** si se marca esta opción, los datos relativos al análisis en cuestión se registrarán en el fichero de resultados.
- **Analizar comprimidos:** si se marca esta opción, se analizarán los ficheros comprimidos que se encuentren.
- **Desinfectar:** si se marca esta opción y se encuentra un virus, el antivirus tratará de desinfectarlo.
- **Si no se puede desinfectar, renombrar:** si se marca esta opción y se encuentra un virus que el antivirus no puede desinfectar, se procederá a renombrar el archivo en cuestión.
- **Si no se puede desinfectar, borrar:** si se marca esta opción y se encuentra un virus que el antivirus no puede desinfectar, se procederá a borrar el archivo en cuestión.

Qué es el análisis heurístico

El análisis heurístico es una técnica de análisis adicional especialmente pensada para detectar virus desconocidos.

Al igual que el análisis bajo demanda, el análisis heurístico es inmediato y a demanda del usuario. El método de análisis en que se basa el análisis heurístico es completamente diferente del método de análisis bajo demanda. Éste último se basa en intentar encontrar uno de los virus que el antivirus conoce mientras que el heurístico intenta determinar si existe un virus basándose en características generales comunes en la mayoría de los virus.

Dado que el análisis heurístico sólo puede determinar que un fichero es sospechoso de estar infectado por un virus y que no se cuenta con información suficiente sobre el supuesto virus, no se pueden desinfectar aquellos supuestos virus detectados por el análisis heurístico.

Es importante tener en cuenta que el análisis heurístico es un complemento del análisis bajo demanda.

El funcionamiento del análisis heurístico es similar al del análisis bajo demanda.

Cómo se usa el análisis heurístico

Para realizar un análisis heurístico, hay que llevar a cabo los siguientes pasos:

1. **Ejecutar el antivirus:** para ejecutar el antivirus, vaya al grupo de programas donde se hayan creado los iconos que permiten su ejecución. Haga doble clic sobre el icono *Panda Antivirus*.
2. **Ir al apartado de análisis heurístico:** para ir a este apartado, pulse el botón *Investigar* en la barra de botones de la aplicación. Aparecerá una ventana para especificar qué se debe analizar mediante el método heurístico y cómo se debe hacer.
3. **Escoger el área de análisis:** se debe elegir el área que se desea analizar. En una lista se muestran las distintas unidades reconocidas en el sistema. También se puede indicar un directorio o un fichero concreto mediante los botones a tal efecto.
4. **Configurar las opciones del análisis heurístico:** este paso es opcional. El programa guarda la configuración de las opciones del análisis heurístico. Por tanto, una vez configurado el análisis heurístico, no hay por qué repetir la configuración en cada análisis de este tipo que se realice. Sólo deberá variarse dicha configuración cuando se desee escoger un conjunto de opciones diferente. Se ofrece una explicación más detallada sobre las opciones de análisis heurístico en el apartado de configuración en esta misma documentación.
5. **Comenzar el análisis:** el botón *Analizar* da comienzo al análisis heurístico en busca de virus en las áreas seleccionadas y con las opciones escogidas.

Cómo se configura el análisis heurístico

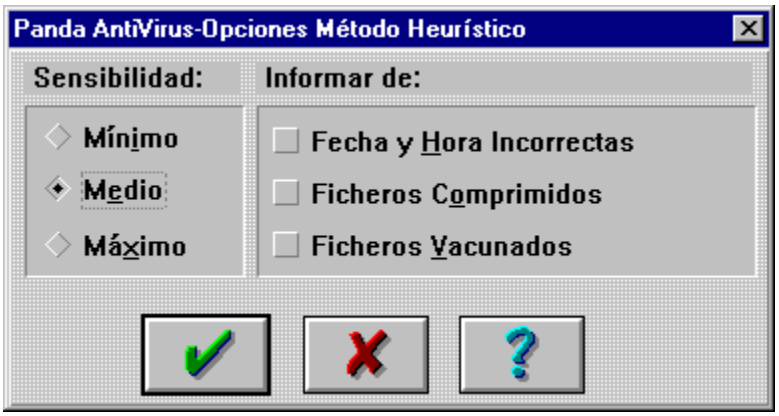
Tal y como se ha mencionado, en un análisis heurístico se debe indicar:

- Qué área se quiere analizar mediante este método.
- Cómo se va a llevar a cabo el mencionado análisis.

La configuración de un análisis heurístico consiste en las opciones de dicho tipo de análisis.

Opciones de análisis

Pulsando el botón *Opciones* aparece una ventana que permite elegir las opciones de análisis heurístico que son las siguientes:



- **Sensibilidad mínima:** si se marca esta opción, la sensibilidad del análisis heurístico será baja logrando así que sólo se indiquen como posibles ficheros contaminados aquellos muy sospechosos de contener un virus.
- **Sensibilidad media:** si se marca esta opción, el análisis heurístico se llevará a cabo con una sensibilidad media. De esta forma, sólo se indicarán como sospechosos aquellos ficheros con bastante probabilidad de estar contaminados.
- **Sensibilidad máxima:** si se marca esta opción, la sensibilidad del análisis heurístico será máxima indicando como sospechosos de infección todos aquellos ficheros en los que se detecte alguna posibilidad de encontrarse infectado. A pesar de lo dicho, la posibilidad de que un fichero no infectado se muestre como sospechoso incluso con este nivel de sensibilidad, es mínima.
- **Informar de fecha y hora incorrectas:** si se marca esta opción, se avisará cada vez que se encuentre un fichero con fecha u hora incorrectas.
- **Informar de ficheros comprimidos:** si se marca esta opción se avisará cada vez que se encuentre un fichero comprimido.
- **Informar de ficheros vacunados:** si se marca esta opción se avisará de todos aquellos ficheros vacunados que se encuentren.

Qué es la búsqueda de cadenas

El análisis bajo demanda se basa en buscar en los ficheros partes de los virus que el antivirus conoce. Dado que cada día surgen nuevos virus, el análisis bajo demanda se va quedando anticuado poco a poco.

La búsqueda de cadenas usa el mismo método que el análisis bajo demanda pero se puede indicar una cadena (parte de un virus) para que la busque. De esta manera, el servicio de atención al cliente de **Panda Software** puede indicarle a Vd. una cadena correspondiente a un nuevo virus para que el antivirus la detecte a pesar de no tener información referente a dicho virus en su interior.

Al igual que el análisis bajo demanda, la búsqueda de cadenas es inmediata y a demanda del usuario.

Cómo se usa la búsqueda de cadenas

Para realizar una búsqueda de cadenas, hay que llevar a cabo los siguientes pasos:

1. **Ejecutar el antivirus:** para ejecutar el antivirus, vaya al grupo de programas donde se hayan creado los iconos que permiten su ejecución. Haga doble clic sobre el icono *Panda Antivirus*.
2. **Ir al apartado de búsqueda de cadenas:** para ir a este apartado, pulse el botón *Buscar* en la barra de botones de la aplicación. Aparecerá una ventana para especificar qué se debe analizar mediante la búsqueda de cadenas y cómo se debe hacer.
3. **Escoger el área en el que se va a realizar la búsqueda:** se debe elegir el área en el que se desea buscar. En una lista se muestran las distintas unidades reconocidas en el sistema. También se puede indicar un directorio o un fichero concreto mediante los botones a tal efecto.
4. **Indicar las cadenas que se deben buscar:** hay que escribir las cadenas que el antivirus debe buscar o elegir cadenas ya introducidas de una lista. Dado que el programa guarda las cadenas que se hayan introducido en otras ocasiones, si no se desea añadir ninguna cadena nueva no hay por qué realizar este paso.
5. **Comenzar la búsqueda:** el botón *Buscar* da comienzo a la búsqueda de las cadenas indicadas en las áreas escogidas.

Cómo se configura la búsqueda de cadenas

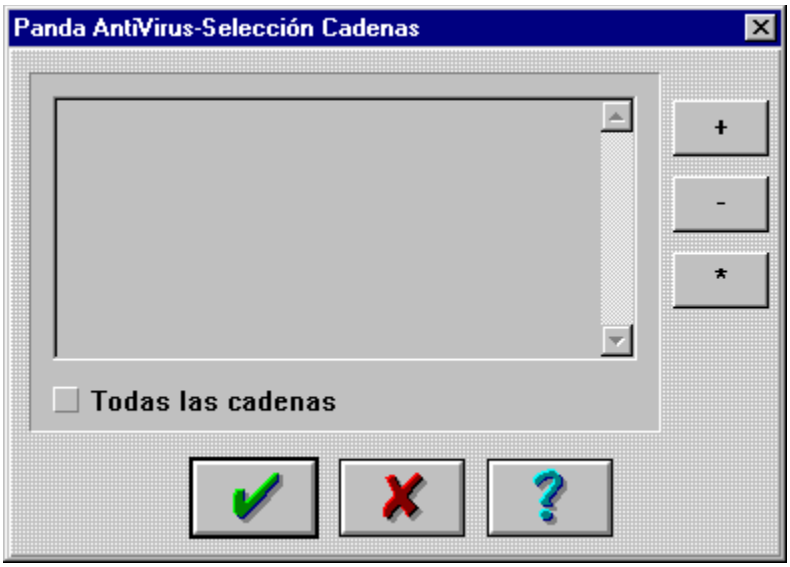
Tal y como se ha mencionado, en una búsqueda de cadenas se debe indicar:

- Qué área se quiere analizar mediante este método.
- Qué cadenas se deben buscar.

La configuración de una búsqueda de cadenas consiste en las cadenas que se deben buscar.

Cadenas

Pulsando el botón *Cadenas* aparece una ventana que permite elegir las cadenas que se buscarán.



En dicha ventana se ve una lista de cadenas introducidas. Mediante unos botones a tal efecto, se puede añadir una cadena a dicha lista, modificar una de las cadenas ya introducidas o eliminar una cadena de la lista.

No se buscarán todas las cadenas indicadas en la lista a no ser que se marque la opción *Todas las cadenas*. Si dicha opción no está marcada, sólo se buscarán las cadenas seleccionadas en la lista.

Cómo desinfectar con Panda Antivirus

No existe un apartado específico de desinfección en **Panda Antivirus**. La desinfección va asociada al análisis bajo demanda o a la protección permanente. Si el análisis bajo demanda o la protección permanente encuentran un virus, intentarán desinfectarlo (si se ha configurado así en las opciones de estos dos apartados).

La configuración de la desinfección permite indicar que se borren o renombren todos aquellos ficheros contaminados que no se puedan desinfectar.

Un virus se puede encontrar en el boot de un disco o en ficheros. En cada caso, hay que proceder de una manera ligeramente diferente. Consulte los apartados correspondientes para obtener un procedimiento de desinfección detallado.

Desinfección de un virus de boot

Partición FAT

Para desinfectar un virus de boot de la unidad C, debe realizar los siguientes pasos:

1. Apague su ordenador. Introduzca un disquete de arranque limpio de virus (si va a realizar la desinfección desde CD-Rom, el disquete deberá cargar los drivers del CD) y reinicie su máquina.
2. Una vez que haya arrancado, ejecute nuestro antivirus en línea de comandos (PAVCL) de acuerdo a las siguientes indicaciones:

   - Si desea ejecutar **Pavcl** desde un disquete, introduzca el disco 1 de **Panda Antivirus** para DOS/Windows 3.1x y teclee lo siguiente:

     ```
     PAVCL C: /CLV
     ```

   - Si desea ejecutar **Pavcl** desde nuestro CD-Rom, introdúzcalo en la unidad lectora, sitúese en el directorio DOSWIN3X y en el idioma deseado y teclee lo siguiente:

     ```
     PAVCL C: /CLV
     ```

     Si en cualquiera de las dos situaciones le aparece un mensaje indicando que la unidad escogida no es válida, teclee lo siguiente:

     ```
     PAVCL /HD0 /CLV
     ```

Partición NTFS

Para desinfectar un virus de boot contando con una partición NTFS, es importante saber si el virus afecta al master boot, al boot o a ambos. En caso de que el virus afecte únicamente al master boot, el procedimiento indicado para particiones FAT es igualmente válido en este caso.

Si el virus afecta al boot, la manera de eliminar el virus es reemplazar el boot por un boot genérico mediante cualquiera de las herramientas que Windows NT provee a tal efecto.

Desinfección de un virus presente en ficheros

Si ha encontrado virus en ficheros, proceda a limpiar su sistema configurando el antivirus de la siguiente manera:

- En *Opciones de análisis* active *Todas las extensiones*, *Desinfectar* y *Análisis automático*.
- Vaya al apartado de análisis y elija la opción correspondiente a analizar todo el sistema (todas las unidades). Según se vaya realizando el análisis, se irán limpiando los ficheros infectados.

Desinfección mediante la protección permanente

Sentinel es capaz de desinfectar los virus que encuentra. Si **Sentinel** detecta un virus y está configurado para desinfectarlo, lo desinfectará antes de que se realice la operación en curso y, una vez desinfectado, continuará con la operación en la que se ha detectado el virus. **Sentinel** siempre muestra una ventana indicando la detección del virus.

Análisis en línea de comandos

Panda Antivirus cuenta con un programa llamado **Pavcl** que se ejecuta desde la línea de comandos de MS-DOS. Nuestro analizador desde la línea de comandos detecta y desinfecta los mismos virus que cualquier otra versión de **Panda Antivirus**.

Pavcl es un analizador rápido y que ocupa poca memoria pero, para manejarlo, es necesario tener un cierto conocimiento de los parámetros que admite. **Pavcl** está disponible en el disquete número 1 de la versión DOS/Windows 3.1x o en el directorio del idioma correspondiente dentro del directorio DOSWIN3X en el CD-Rom.

Parámetros de Pavcl

Tareas

`/NOM` No analizar la memoria.

`/NOB` No analizar el sistema de arranque BOOT.

`/NOF` No analizar ficheros.

`/ALL` Analizar todas las unidades del sistema.

`/INVx` Investigar en la unidad "x" en busca de virus desconocidos.
Ejemplo: `/INVA` investiga en la unidad A:.

`/CLV` Eliminar los virus que se hayan detectado.

`/LIS` Listar los virus contemplados en esta versión.

`/HEU` Activar método de detección Heurístico.

`/CMP` Analizar comprimidos.

`/CDR` Muestra los códigos de retorno de **Pavcl**.

`/SAV` Guardar los parámetros en un fichero. En las siguientes ejecuciones añadirá estos parámetros a los introducidos en cada sesión.

`/IB+` Añadir vacuna Interna al BOOT.
`/IB-` Quitar vacuna Interna al BOOT.
`/IB*` Verificar vacuna Interna del BOOT.

`/EB+` Añadir vacuna Externa al BOOT.

`/EB-` Quitar vacuna Externa al BOOT.
`/EB*` Verificar vacuna Externa del BOOT.

`/IF+` Añadir vacuna Interna a un Fichero.
`/IF-` Quitar vacuna Interna a un Fichero.
`/IF*` Verificar vacuna Interna de un Fichero.

`/EF+` Añadir vacuna Externa a un Fichero.
`/EF-` Quitar vacuna Externa a un Fichero.
`/EF*` Verificar vacuna Externa de un Fichero.

`/B+` Añadir vacuna Interna y Externa al BOOT.
`/B-` Quitar vacuna Interna y Externa al BOOT.
`/B*` Verificar vacuna Interna y Externa del BOOT.

`/F+` Añadir vacuna Interna y Externa a un Fichero.
`/F-` Quitar vacuna Interna y Externa de un Fichero.
`/F*` Verificar vacuna Interna y Externa de un Fichero.

Modificadores

`/NSB` No analizar los subdirectorios de nivel inferior.

`/PTH` Analizar los directorios contenidos en la variable PATH del DOS.

`/ISO` Activar el método de aislamiento.

`/NOS` Desactivar el sonido.

`/AEX` Analizar todos los ficheros, independientemente de su extensión.

`/AUT` Exploración sin la intervención del usuario.

`/OVR` Sobrescribir antes de borrar.

`/NOR` No generar fichero de resultados.

`/DEL` Borra los ficheros infectados aunque se puedan desinfectar.

`/LOC` Analiza todas las unidades locales.

`/NBR` No permite cancelar el proceso de análisis.

`/ITW` **Pavcl** sólo analizará en busca de los virus *In The Wild*. Este parámetro sólo debe usarse en

condiciones especiales.

Adicionalmente dispone del switch "/?" estandarizado en el DOS, para tener acceso a una lista de los switches disponibles. En esta también se incluyen aquellos correspondientes a los idiomas soportados por la versión de **Pavcl**.

Las tareas por defecto son:

- Analizar Memoria.
- Analizar Boot.
- Analizar Ficheros.

y los modificadores por defecto son:

- Analizar subdirectorios.
- No desinfectar.
- Efectos de sonido activados.
- Analizar sólo extensiones ejecutables.
- Generar fichero de resultados.

Las tareas /?, /LIS, /INVx son exclusivas, es decir, cuando son seleccionadas ninguna de las otras tareas se realiza. Después de finalizadas se regresa al DOS. El camino o caminos que quieren analizarse se especifica como es habitual en el DOS:

[Unidad:][Camino][NombreFichero]

Informe de resultados

El informe de resultados va guardando las distintas operaciones que se van realizando con el antivirus así como las distintas incidencias que se produzcan.

La información contenida en el informe de resultados se conserva de sesión en sesión. Por tanto, es útil para consultar, en cualquier momento, la actividad que se ha llevado a cabo con el antivirus.

Por cada operación realizada, se guardan los siguientes datos:

- Fecha y hora.
- Tipo de operación.
- Área sobre la que se ha llevado a cabo la operación.
- Número de ficheros revisados.
- Todas las incidencias habidas relacionadas con los virus.

Para que se vayan almacenando los datos en el informe de resultados, es necesario activar la opción *Grabar resultados* dentro de la ventana de *Opciones de Análisis*.

El contenido del informe de resultados se puede imprimir para facilitar su consulta. También se puede borrar el contenido del informe de resultados en cualquier momento para evitar que adquiera un tamaño demasiado grande.

Lista de virus

La lista de virus presenta una lista con los virus que **Panda Antivirus** es capaz de detectar. En la lista de virus se indica el nombre y el tamaño de cada virus.

Junto a la lista, se indica el número de virus reconocidos en esa versión de **Panda Antivirus**. También se indica la fecha del fichero de virus para saber, de esa manera, lo actualizado o desactualizado que se encuentra el antivirus.

Se puede indicar el nombre de un virus en el hueco destinado a tal efecto para encontrar así un virus concreto con mayor facilidad. Con ese mismo fin, la lista de virus se presenta ordenada alfabéticamente.

Una vez elegido un virus, si se pulsa el botón *Info*, aparece una ventana con una serie de datos de interés como son:

- Nombre.
- Origen.
- Tamaño.
- Alias.
- Fecha en la que se detectó por primera vez.
- Si se puede desinfectar o no.
- Áreas de la máquina que pueden verse afectadas por el virus.
- Características de comportamiento del virus.

A continuación, se detalla una explicación sobre las distintas características con que puede contar un virus:

- **Residente:** cuando se ejecuta, el virus reserva una pequeña parte de la memoria y se instala en ella para ir contagiándose desde ahí.
- **Stealth:** es una técnica que usan algunos de los virus residentes. Esta técnica consiste en camuflar los cambios que el virus hace sobre los ficheros que infecta. Cuando alguien intenta mirar una de las características del fichero que el virus ha modificado, el virus, que está residente en memoria, intercepta la consulta y ofrece los datos anteriores a la modificación.
- **Encriptado:** los virus que poseen esta característica son capaces de encriptarse de manera diferente cada vez que infectan un fichero. De esta forma, no se puede intentar buscar el virus mediante una cadena.
- **Sobreescritura:** los virus de sobreescritura, que pueden ser residentes o no, sobreescriben el fichero que infectan. Dicho fichero queda, por tanto, inservible. El tamaño del fichero no varía a no ser que el tamaño del virus sea mayor que el del fichero. La única manera de eliminar estos virus es borrando el fichero infectado y poniendo en su lugar una copia sin infectar.
- **Polimórfico:** los virus polimórficos son versiones avanzadas de los virus encriptados. Los polimórficos son capaces de cambiar el método de encriptación de generación en generación. De esta forma, no hay ninguna parte del virus que permanezca inalterada.

Funcionamiento general

Panda Antivirus para Windows NT presenta un cómodo interface fácil de usar. En la ventana principal del programa, las opciones más comunes están disponibles a través de unos botones de gran tamaño.

Pulsando sobre esos botones se accede a las distintas partes del programa. Refiérase al apartado correspondiente para obtener una explicación de funcionamiento detallada.