Imprimir Esta Ayuda

Gracias a esta ayuda podrás consultar cualquier tema referente a Panda Antivirus Platinum. 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**. Sólo disponible para la ayuda en formato HLP.

  {button Imprimir TODA esta Ayuda,IF(InitMPrint(),`MPrintId(`10'):MPrintId(`15'):MPrintId(`20'):MPrintId(`25'):MPrintId(`30'):MPrintId(`35'):MPrintId(`40'):MPrintId(`45'):MPrintId(`50'):MPrintId(`55'):MPrintId(`60'):MPrintId(`65'):MPrintId(`70'):MPrintId(`75'):MPrintId(`85'):MPrintId(`80'):MPrintId(`90'):MPrintId(`95'):MPrintId(`100'):MPrintId(`105'):MPrintId(`110'):MPrintId(`115'):MPrintId(`120'):MPrintId(`125'):MPrintId(`130'):MPrintId(`135'):MPrintId(`140'):MPrintId(`145'):MPrintId(`150'):MPrintId(`160'):MPrintId(`175'):MPrintId(`310'):MPrintId(`165'):MPrintId(`180'):MPrintId(`215'):MPrintId(`185'):MPrintId(`195'):MPrintId(`190'):MPrintId(`171'):MPrintId(`172'):MPrintId(`155'):MPrintId(`220'):MPrintId(`345'):MPrintId(`350'):MPrintId(`535'):MPrintId(`221'):MPrintId(`222'):MPrintId(`223'):MPrintId(`224'):MPrintId(`226'):MPrintId(`210'):MPrintId(`225'):MPrintId(`525'):MPrintId(`530'):MPrintId(`531'):MPrintId(`540'):MPrintId(`200'):MPrintId(`235'):MPrintId(`230'):MPrintId(`241'):MPrintId(`245'):MPrintId(`250'):MPrintId(`255'):MPrintId(`241'):MPrintId(`260'):MPrintId(`265'):MPrintId(`196'):MPrintId(`275'):MPrintId(`270'):MPrintId(`300'):MPrintId(`85'):MPrintId(`305'):MPrintId(`255'):MPrintId(`315'):MPrintId(`320'):MPrintId(`325'):MPrintId(`330'):MPrintId(`331'):MPrintId(`335'):MPrintId(`310'):MPrintId(`340'):MPrintId(`540'):MPrintId(`545'):MPrintId(`550'):MPrintId(`555'):MPrintId(`560'):MPrintId(`565'):MPrintId(`570'):MPrintId(`575'):MPrintId(`580'):MPrintId(`585'):MPrintId(`590'):MPrintId(`595'):MPrintId(`600'):MPrintId(`605'):MPrintId(`610'):MPrintId(`615'):MPrintId(`620'):MPrintId(`175'):MPrintId(`320'):EndMPrint()')}

- Si deseas imprimir TODAS las FAQs (preguntas más frecuentes con sus respuestas), pulsa el botón **Imprimir TODAS las FAQs** (bajo estas líneas), o pulsa **aquí**. Sólo disponible para la ayuda en formato HLP.

  {button Imprimir TODAS las FAQs,IF(InitMPrint(),`MPrintId(`320'):MPrintId(`355'):MPrintId(`360'):MPrintId(`365'):MPrintId(`370'):MPrintId(`375'):MPrintId(`380'):MPrintId(`385'):MPrintId(`390'):MPrintId(`395'):MPrintId(`400'):MPrintId(`405'):MPrintId(`410'):MPrintId(`415'):MPrintId(`420'):MPrintId(`425'):MPrintId(`430'):MPrintId(`435'):MPrintId(`440'):MPrintId(`445'):MPrintId(`450'):MPrintId(`455'):MPrintId(`460'):MPrintId(`465'):MPrintId(`470'):MPrintId(`475'):MPrintId(`480'):MPrintId(`485'):MPrintId(`490'):MPrintId(`495'):MPrintId(`500'):MPrintId(`505'):MPrintId(`510'):MPrintId(`515'):MPrintId(`520'):MPrintId(`521'):MPrintId(`625'):EndMPrint()')}

NOTA: la impresión de la ayuda en su totalidad puede llevar bastante tiempo. Dependiendo de su impresora y las configuraciones que tenga establecidas, podrá ocupar mayor número de páginas.

Introducción a Panda Antivirus Platinum

Bienvenido/a a Panda Antivirus Platinum. Hemos diseñado Panda Antivirus Platinum para que sea fácil y cómodo de utilizar. En esta ayuda cuentas con explicaciones detalladas sobre todas las operaciones que se pueden llevar a cabo con Panda Antivirus Platinum. Consulta esta ayuda cuando tengas alguna dificultad o no sepas cómo llevar a cabo una determinada acción.

Panda Antivirus Platinum está preparado para trabajar bajo los siguientes sistemas operativos: Windows XP, Windows 2000 Pro, Windows NT, Windows Millennium, Windows 98 y Windows 95.

El principal objetivo de Panda Antivirus Platinum es acercar la más avanzada tecnología antivirus a todos los usuarios, aunando las altas capacidades para la detección y desinfección de virus, con la una gran facilidad de uso del antivirus. El creciente peligro de los virus informáticos y los avances tecnológicos que presentan, hacen necesario un antivirus de última generación con una tecnología de vanguardia.

Además, Panda Software pone a tu disposición un gran y efectivo abanico de servicios antivirus destinados a solucionar, en cualquier momento, los problemas que te puedan surgir con los virus. La combinación de un producto puntero y los mejores servicios personalizados para ti, convierten a Panda Antivirus Platinum en una de las mejores y más completas soluciones antivirus del mercado.

Nueva Tecnología y Nuevo Diseño

Panda Antivirus Platinum incorpora un nuevo motor antivirus extremadamente potente, capaz de actuar allí donde otros antivirus no pueden. Esto hace que Panda Antivirus Platinum sea un producto ideal para la detección y eliminación de virus. Todo ello sin interferir en los procesos que realiza el sistema, combinándose con él, llegando a formar parte de él, sin disminuir las capacidades y recursos de éste en medida alguna.

Por otra parte, su nuevo diseño se ajusta a los estilos que se están imponiendo en el mundo informático. Con ello se pretende conseguir un producto muy cómodo y fácil de utilizar, al mismo tiempo que nos ofrece toda la potencia necesaria para la protección antivirus.

Estrategias de Protección

Panda Antivirus Platinum ofrece un completo conjunto de estrategias de protección para las vías de entrada y salida del ordenador.

- **Análisis inmediatos y programados.** Permiten analizar de forma muy fácil y sencilla cualquier elemento del ordenador (Todo el Sistema, Discos Duros, Correo Electrónico, Memoria, Sistema Operativo,…etc.) en cualquier momento y de forma inmediata (Análisis inmediatos), o cuando el usuario así lo determine (Análisis programados).
- **Protección permanente.** Ofrece una protección total y automática en todo momento. Dicha protección se encuentra continuamente analizando los ficheros y mensajes con los que se trabaja. Por lo tanto, ésta permite proteger permanentemente el correo electrónico y los ficheros que utilizamos. Además, Panda Antivirus Platinum cuenta con un excelente firewall que te permitirá controlar todos los accesos (entradas y salidas de tu ordenador) a través de la red e Internet.

Hospital - Cuarentena

Panda Antivirus Platinum incorpora un nuevo sistema de protección adicional que aporta una mayor

seguridad y una estrecha relación con las acciones a realizar sobre los ficheros sospechosos o infectados. El Hospital está compuesto por una serie de funciones y herramientas nuevas que nos permiten controlar todos los ficheros y elementos que el antivirus considere sospechosos o infectados. De este modo, podrá mantener en Cuarentena a dichos ficheros, o enviarlos a Panda Software para su estudio y análisis.

Firewall

Se trata de un sistemas de seguridad adicional, incorporado en tu Panda Antivirus Platinum. Se conoce también con el nombre de *cortafuegos* y su utilización es conveniente para garantizar la seguridad de los ordenadores que se encuentran conectados a Internet o a una red. Consiste en un sistema de defensa mediante el cual se pretende establecer un muro (ficticio) de control entre tu ordenador y la red. A través de él sólo circularán los datos que tú indiques, siguiendo estrictamente las reglas de funcionamiento que tú definas.

Servicios

Junto con Panda Antivirus Platinum has adquirido un completo conjunto de servicios para ayudarte en todo lo relacionado con los virus. Sin duda, además de su gran poder de detección y desinfección, ésta es una de las ventajas más importantes que debería incorporar toda herramienta antivirus. En Panda Software lo sabemos muy bien y hacemos gala de unos excelentes servicios.

Actualización automática del antivirus: los antivirus utilizan un determinado fichero (denominado archivo de identificadores de virus, o fichero de firmas de virus) para reconocer y detectar cada uno de los virus. Éste contiene las características que identifican a un determinado virus, entre todos los existentes. A diario surgen nuevos virus. Esto significa que sus respectivos identificadores deberían incluirse en el fichero que comentamos, para que sean detectados por el antivirus. Esto es lo que hace Panda Software, poniendo a tu disposición cada día un nuevo fichero con los últimos identificadores. Panda Software prepara todos los días un nuevo archivo de identificadores, que detecta más virus que el anterior. Panda Antivirus Platinum permite ser actualizado a DIARIO. Por lo tanto, todos los días es posible la actualización del antivirus. También es posible indicarle al antivirus que debe actualizarse a sí mismo, de forma automática, a través de Internet. En tal caso, Panda Antivirus Platinum considerará si es necesario actualizarse y así lo hará si detecta una conexión abierta a Internet. Si eres usuario registrado, también podrás realizarla dichas actualizaciones manualmente, desde la Web de actualizaciones de Panda Software.

Envío a Panda de archivos sospechosos (S.O.S. Virus): gracias a Panda Antivirus Platinum, podrás enviar al Laboratorio de Investigación de Panda Software, todos los ficheros que consideres sospechosos de estar infectados. Éstos serán analizados y estudiados, enviándote en poco tiempo la solución correspondiente, o la certificación de que el fichero es correcto. Si encuentras algún nuevo virus, no tardaremos más de 24 horas en enviarte una solución antivirus que lo detecte y lo desinfecte.

FAQs (Preguntas más frecuentes con sus respuestas): es normal que en ocasiones te surjan dudas referentes al mundo de los virus y al propio programa antivirus. Además de recurrir a esta ayuda, con Panda Antivirus Platinum podrás acceder a las FAQs que éste incorpora. Se trata de una serie de preguntas con las respuestas correspondientes a cada una de ellas.

Envío de consultas técnicas vía correo electrónico: siempre puedes solucionar tus dudas mediante esta ayuda, el manual, o las FAQs. Además, Panda Antivirus Platinum permite, a través de un sencillísimo asistente, que envíes tus dudas o consultas de tipo técnico a Panda Software.

Buzón de sugerencias: ¿tienes algún comentario o sugerencia que hacernos para mejorar el antivirus o sus servicios?. Siempre que lo desees, puedes enviar tus comentarios o sugerencias a

Panda Software.

Por otra parte y de forma adicional, desde Panda Antivirus Platinum podrás consultar cualquiera de las características de otros productos antivirus, de seguridad, o de inventario de Panda Software, como Panda Antivirus Corporativo, Panda PerimeterScan, o Panda Invent.

Soporte técnico: 24 horas al día, 365 días al año, contamos con técnicos cualificados que te atenderán personalmente. Para que sea fácil y cómodo contactar con nosotros, te ofrecemos todos los medios: resolución de problemas a través de correo electrónico, fax, correo postal, y a través de nuestra Web (www.pandasoftware.es). Además, podrás contratar adicionalmente, el servicio personalizado de soporte técnico a través de teléfono (906). **El Soporte técnico en la web** te ayudará a contactar directamente y a encontrar más rápidamente la solución a tu problema, duda, consulta, etc.

Características de Panda Antivirus Platinum

Entre las distintas características de Panda Antivirus Platinum podemos mencionar las siguientes.

Información de estado en el inicio: cuando se abre la ventana de Panda Antivirus Platinum, -cuando se ejecuta Panda Antivirus Platinum-, éste informa sobre el estado actual del programa, así como las acciones que es recomendable realizar. De esta forma, siempre serás informado de lo actualizado que está tu antivirus, del número de virus que detecta, del estado de la protección permanente (archivos e Internet). Por otra parte, Panda Antivirus Platinum te sugiere -mediante sus avisos-, algunas acciones que deberías llevar a cabo (análisis del ordenador, actualizaciones, creación de discos de rescate,…).

Personalización de los Análisis. Podrás definir las características de los análisis (tanto de los inmediatos como de los programados), configurar, editar las propiedades de un análisis previamente creado, eliminar alguno de ellos,… etc. Esto quiere decir que tienes la capacidad de crear o establecer una serie de análisis predeterminados. De esta forma, al estar definidos por ti mismo, te permitirán posteriormente realizar ciertos análisis con un solo clic de ratón.

Información y configuración de la Protección permanente (Antivirus -análisis residentes- y Firewall). Es posible visualizar el estado actual de los análisis que se están llevando a cabo de forma continua, sin intervención del usuario (permanentes). Panda Antivirus Platinum, además permite realizar varias operaciones sobre estos análisis: activarlos si no lo estaban ya, desactivarlos en el caso de que estuviesen activos y configurarlos o determinar cómo debe ser su funcionamiento. Además, también puedes obtener información sobre el funcionamiento del firewall (**Ver actividad de red**) que Panda Antivirus Platinum incorpora y determinar cómo debe funcionar -configurarlo-.

Análisis desde el *Explorador de Archivos* (análisis contextual): ofreciendo una alta integración con el sistema operativo, Panda Antivirus Platinum permite realizar análisis inmediatos desde el *Explorador de Archivos de Windows* con tan sólo pulsar un botón y sin tener que abrir previamente el antivirus. Desde el *Explorador de Archivos de Windows*, se pueden seleccionar ficheros y directorios o carpetas. Al pulsar con el botón derecho del ratón sobre ellos (menú contextual), aparecerá la opción **Analizar con antivirus Platinum**. Seleccionando esta opción, se analizarán por completo los ficheros y directorios seleccionados, en busca de virus.

Informe: todas las incidencias relacionadas con algún virus y con el funcionamiento del firewall, se pueden registrar en un informe para su posterior consulta. Toda la información se conserva entre distintas sesiones del antivirus para poder consultar los datos cuando sea necesario, siempre y cuando no se indique que se desea borrar esta información (borrar el informe -su contenido-).

Actualizaciones: el propio antivirus es capaz de actualizarse de forma inteligentemente por sí mismo, automáticamente a través de Internet, cuando lo considera necesario. Por otro lado, se podrán realizar las actualizaciones cuando el usuario lo desee y activar o desactivar la actualización automática.

Alertas: un completo sistema de alertas permite avisar de la presencia de un virus en el ordenador en el que se haya detectado, a través de la red (si se está conectado a una) o enviando un mensaje de correo electrónico.

Hospital: es posible aislar todos los ficheros infectados, o supuestamente infectados, para que no afecten al resto del sistema. Esta ventaja de Panda Antivirus Platinum hace posible mantener aislados o en cuarentena a ciertos ficheros con la intención de no infectar otros. Por otra parte, también existe

la posibilidad de enviar dichos ficheros a Panda Software. En este último caso, Panda Software enviará una solución antivirus para cada uno de ellos (en el caso de que se encuentren infectados).

Los mejores Servicios Panda Software: tu antivirus, Panda Antivirus Platinum, incluye una excelente gama de servicios con los que cuenta Panda Software. Siempre contarás con el respaldo de profesionales expertos en materias de antivirus y seguridad informática, que te asesorarán, te resolverán tus dudas y te solucionarán todos tus problemas. Algunos de los servicios adicionales que incluye Panda Antivirus Platinum son la Actualización, la consulta de FAQs (preguntas más frecuentes con sus respuestas), el Envío de ficheros sospechosos (S.O.S. Virus), Soporte técnico a través de la Web, Envío de consultas y el acceso a un Buzón de sugerencias. Para obtener más información sobre cada uno de los servicios que acompañan a Panda Antivirus Platinum, consulta el apartado Servicios de esta ayuda.

Nota: Panda Antivirus Platinum está preparado para trabajar bajo los siguientes sistemas operativos: Windows XP, Windows 2000 Pro, Windows NT, Windows Millennium, Windows 98 y Windows 95.-

Vías de Entrada de los Virus

Desde hace ya varios años, la tendencia entre los ordenadores personales es la conectividad. Cada vez más, el ordenador no es un elemento aislado con una única vía de entrada para los virus, como antiguamente. Esto, que es beneficioso para todos los usuarios y para los ordenadores personales en general, también ha multiplicado el número de vías de entrada disponibles para los virus.

Por todo lo anterior, es muy importante conocer cuáles son las vías de entrada que un virus puede usar para acceder a un ordenador y comprender cómo debe un antivirus proteger TODAS Y CADA UNA de esas vías de entrada.

Además de haberse multiplicado las posibles vías de entrada para los virus, también han aparecido nuevos tipos de virus y nuevas formas de transmitir dichos virus.

Por último, aunque no menos importante, hay que destacar la importancia de vigilar las salidas. Habitualmente esto no se tiene en cuenta porque se parte de un esquema "que no entre ningún virus". No hay que olvidar sin embargo, que la mayor parte de las infecciones son sin mala intención, es decir, una persona envía a otra un fichero, o DVD, CD-ROM, disquete, etc infectado sin ser consciente de que le está enviando un virus. Si todos cuidáramos nuestras "salidas" y no sólo nuestras entradas, se evitaría en gran medida la rápida difusión con la que cuentan hoy los virus. Además la persona que envía un virus puede verse perjudicada por dicha circunstancia.

DVDs, CD-ROMs, Disquetes y otras unidades de disco extraíbles

Antiguamente eran la única vía de entrada a un ordenador personal (siempre y cuando no estuviera conectado en red). Los virus pueden ir incluidos en los ficheros que se guarden en cualquiera de estos soportes, o estar en el sector de arranque (Boot) de una unidad de disco.

La respuesta de Panda Software a esta vía de entrada de virus es doble. Por un lado, se cuenta con un análisis continuo que ofrece protección permanente. De esta forma, todo acceso a cualquiera de los ficheros contenidos en el DVD, CD-ROM, disquete, o en otra unidad de disco haría que el fichero en cuestión fuera analizado por la protección permanente. Por otro lado, se ofrece la posibilidad de realizar un análisis inmediato (análisis bajo demanda) de cualquier DVD, CD-ROM, disquete u otro tipo de unidad de disco, que se introduzca para verificar si está libre de virus.

Por tanto, con una protección permanente adecuada, un antivirus puede resolver con eficacia el peligro que supone esta vía de entrada.

Redes de ordenadores

Esta vía de entrada para virus es antigua pero se ha generalizado enormemente en los últimos años. Actualmente, en casi todos los sitios en los que hay varios ordenadores hay una red que los conecta. El objetivo fundamental de una red es compartir información y por tanto la compartición de ficheros. Como en una red se comparten todo tipo de ficheros, ésta puede ser vía de transmisión de virus de archivos, y virus de macro, así como cualquier otro tipo de virus, gusanos o troyanos.

La respuesta de Panda Software a esta vía de entrada también es doble. Por un lado y como protección clave se sigue contando con un análisis continuo para ofrecer protección permanente. Este es el mismo que vigila el acceso a ficheros ya mencionado anteriormente. Cada vez que se intente enviar o recibir un fichero contaminado por un virus a través de la red, la protección permanente

analizará dicho fichero. Igual que en el caso anterior, también se cuenta con la posibilidad de llevar a cabo un análisis inmediato (análisis bajo demanda) para analizar cualquier unidad de red. Sin embargo, dado el carácter compartido de una red, constantemente se pueden estar añadiendo nuevos ficheros lo que dificulta el poder estar seguro de que una unidad de red esté libre de virus.

Igual que en el caso anterior, pero en este caso con más razón, el contar con una protección permanente adecuada es la mejor manera de asegurar esta vía de entrada frente a los virus.

Además, Panda Antivirus Platinum cuenta con un excelente firewall gracias al cual podrás restringir los permisos de ciertos programas para acceder a determinadas áreas o secciones de la red, direcciones IP (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes en una red), carpetas compartidas, etc.

Internet

Aunque Internet tiene ya varios años de existencia, hasta hace poco no era un medio masivo de comunicación, sin embargo hoy día es cada vez más frecuente su presencia en todos los ámbitos. La función primordial de Internet es facilitar, en muchos casos posibilitar, el intercambio de información. Por tanto, Internet también facilita el intercambio de ficheros que, como ya hemos dicho, son el "vehículo" de transmisión de los virus. Sin embargo, la situación es algo más compleja que en el caso de una red. Veamos por qué.

Internet cuenta con diferentes servicios. Estos servicios son, por ejemplo, las páginas Web, el correo electrónico, la transferencia de ficheros vía FTP, las comunicaciones a través de chat,…etc. Cada uno de estos servicios utiliza un protocolo (un lenguaje) determinado, por lo que es fundamental conocer estos lenguajes para poder analizar correctamente en busca de virus esta vía de entrada. Por ejemplo, un mensaje de correo electrónico puede traer asociado un fichero infectado con virus. Al no estar dicho fichero en su formato normal, un antivirus convencional, no podría detectarlo. También puede darse el caso de mensajes que no incluyendo ficheros infectados (como elementos adjuntos), se encuentren infectados (debido al código que éstos mismos incluyen, o el formato MIME de cada uno de ellos). Por eso es necesario un antivirus especialmente preparado que comprenda el formato en el que se reciben los mensajes de correo electrónico para poder descubrir el virus.

Las vías de entrada de un virus a través de Internet son las siguientes:

- **Correo electrónico:** los virus pueden estar incluidos en los ficheros adjuntos a un mensaje de correo electrónico, pero esto no es una condición necesaria. El virus también puede formar parte del propio mensaje (sin necesidad de estar incluido en un fichero adjunto). Es importante tener en cuenta que en Internet se usan dos protocolos (conjuntos de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) para el correo electrónico. Uno de ellos es **POP3** y se usa para el correo entrante (el correo recibido). El otro es **SMTP** y se usa para el correo saliente (el correo enviado). Como ya comentábamos, es muy importante que nuestro antivirus proteja tanto las posibles entradas, como las posibles salidas de virus. Además, los virus que han aparecido recientemente, aprovechan determinadas características y vulnerabilidades de ciertos programas de gestión de correo y de otros tipos de programas cuyo uso está muy extendido.
- **Noticias o News (NNTP):** mediante este servicio, se puede acceder a grupos de noticias que se debaten o que se colocan en determinados servidores para consultarlas y en su caso debatirlas. También se puede realizar una suscripción de tal modo que periódicamente se recibirán correos electrónicos con las nuevas noticias, susceptibles de estar infectados. Se podrán analizar las noticias gestionadas con Microsoft Outlook Express así como las gestionadas con Microsoft Exchange/Outlook.

- **Descarga de ficheros (FTP):** este servicio permite descargar ficheros de Internet y subir o colocar otros ficheros en determinadas direcciones de Internet. Estos ficheros pueden estar infectados por virus.
- **Páginas Web (HTTP):** en principio, las páginas Web (páginas HTML) son únicamente texto y gráficos por lo que no presentan peligro de virus. Sin embargo, cada vez más páginas Web tienen otro tipo de componentes como pueden ser Applets Java o controles ActiveX. Este tipo de objetos sí que pueden estar contaminados por virus y afectar a un ordenador únicamente por el hecho de acceder a una página Web.

Para solucionar un problema potencialmente tan grave, Panda Software plantea una serie de soluciones que Panda Antivirus Platinum incluye. Éstas son las siguientes:

- **Correo electrónico:** una protección permanente de carácter especial se encarga de analizar en busca de virus todos aquellos mensajes que se envían (protocolo SMTP) y todos los que se reciben (protocolo POP3). De esta forma, no se puede recibir ni enviar ningún mensaje de correo electrónico que contenga un fichero infectado con virus. Otros antivirus analizan únicamente el correo entrante. Esto es muy peligroso ya que posibilita el envío de virus con los perjuicios que esto puede suponer para el que envía el virus. La protección antivirus del correo electrónico que ofrece Panda Antivirus Platinum, funciona para los programas clientes de correo más extendidos y utilizados en la actualidad.

  Además hay un peligro adicional en el caso del correo electrónico. Todos los mensajes que se envían o reciben quedan almacenados en base de datos de mensajes. El formato de esta base de mensajes no es reconocido por los antivirus convencionales -si por Panda Antivirus Platinum- por lo que un antivirus normal no podrá analizar en busca de virus todos los mensajes enviados o recibidos antes de la instalación del antivirus o todos aquellos mensajes que no hayan sido analizados en el momento de su recepción por cualquier causa. Para solucionar esto, Panda Antivirus Platinum es capaz de entender el formato de la base de datos de mensajes de los programas Microsoft Outlook Express y Microsoft Outlook. De esta forma, Panda Antivirus Platinum permite analizar en el momento en el que se desee cualquiera de los mensajes de la base de datos de mensajes ofreciendo así la garantía de contar con un correo electrónico libre de virus.

- **Noticias o News (NNTP):** todos los contenidos con posibilidad de estar infectados por virus en un servidor en el que se presta un servicio de noticias (los documentos objeto de éstas) serán analizados por una protección permanente de carácter *especial* encargada de vigilar la conexión con ese servidor. De esta forma se garantiza una información consultada de forma segura, independientemente del programa de noticias con el que se trabaje.
- **Transferencia de ficheros (FTP):** todos los ficheros que se descarguen o suban a una dirección de Internet mediante FTP, serán analizados por una protección permanente. Dichos ficheros son analizados de forma local antes de enviarse, o cuando ya han llegado a nuestro ordenador. De esta forma no será posible transferir ningún fichero infectado. Todos aquellos ficheros que se hayan transferido anteriormente podrán ser analizados con un antivirus de ficheros no dándose aquí la problemática añadida mencionada para los mensajes de correo electrónico. La protección contra virus es independiente del programa de FTP que se esté usando.
- **Páginas Web (HTTP):** todos los contenidos con posibilidad de estar infectados por virus en una página Web o página HTML (Applets Java*,* controles ActiveX*,* etc.) serán analizados por una protección permanente. En ocasiones estos elementos son descargados al equipo que se conecta a dichas páginas. Cuando se hayan descargado estos elementos, serán analizados localmente por la protección permanente. De esta forma se garantiza una navegación segura independientemente del navegador con el que se visiten las páginas Web.

En resumen, se puede decir que Panda Antivirus Platinum ofrece una buena protección frente a los posibles virus que podrían ubicarse en nuestro ordenador a través de todos estos tipos de conexiones. Por un lado se analizan los datos cuando han entrado y también antes de que salgan del ordenador hacia el exterior, para verificar que no llegue o salga ningún virus. Por otro lado, es posible analizar todo el correo electrónico (Microsoft Outlook Express y Microsoft Exchange/Outlook) de que se disponga y se analizarán tanto los mensajes que se envíen como los que se reciban garantizando así una conexión a Internet libre de virus.

Es posible consultar más información sobre las vías de entrada utilizadas por los virus para sus infecciones, en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

¿Por Qué No Todos los Antivirus Son Iguales?

Es frecuente pensar que, al fin y al cabo, todos los antivirus son iguales. Quizá la idea más generalizada es que lo único que diferencia un antivirus de otro es el número de virus que ambos sean capaces de detectar.

Sin embargo, esto no es cierto. Lo que realmente diferencia a un antivirus de otro es la capacidad de protección que pueda ofrecer. Lo que un antivirus debe ofrecer es lo siguiente:

- **Protección de todas las vías de entrada:** es la característica fundamental de un antivirus, que proteja todos aquellos puntos por los que un virus puede infectar un ordenador.
- **Protección de todas las vías de salida:** tan importante como no infectarnos, es evitar la propagación de virus por nuestra parte. Es decir, evitar infectar a otros usuarios.
- **Actualización constante, inteligente y automática:** por su propia esencia, un antivirus necesita estar constantemente actualizado, ya que cada día surgen nuevos virus. Sin un servicio constante y DIARIO de actualizaciones, un antivirus se va quedando anticuado y va perdiendo utilidad. Adicionalmente, es de gran interés que el antivirus se actualice automáticamente, cuando así lo necesite. De esta forma, siempre tendremos el convencimiento de que nuestro antivirus detecta los últimos virus aparecidos y nos olvidaremos de realizar las actualizaciones de forma manual.
- **Soporte técnico:** por desgracia, las situaciones en las que se detecta un virus suelen ser conflictivas. A veces el virus se ha detectado tarde por no contar con un antivirus, o no mantenerlo actualizado. En otras ocasiones, el virus se detecta a tiempo pero el miedo al efecto del virus hace que se viva como una situación conflictiva. Como último punto para solucionar el problema de los virus, debe haber un eficaz soporte técnico capaz de dar respuesta a todos los problemas relacionados con virus. Siempre contarás con este soporte técnico. Siempre lo tendrás accesible, de una manera sencilla, para que te sea posible realizar tu trabajo con total normalidad. El objetivo del soporte técnico es ayudar a todos aquellos que, por desgracia, se han topado con un virus. Además, lo tendrás disponible las 24 horas del día, durante los 365 días del año.
- **Sencillez y potencia:** además de contar con un amplio poder de detección y desinfección de todos los virus conocidos, debe ser una herramienta fácil y cómoda de utilizar.

Lo que Panda Antivirus Platinum ofrece en este punto es lo siguiente:

- **Protección permanente** de todos los ficheros que intervienen en cualquier operación realizada. De esta forma, se evita de una manera automática y sencilla la entrada y salida de ficheros infectados en el ordenador. Además, también evita toda operación que se quiera realizar con ficheros infectados que, por una razón u otra, ya estén en el ordenador. La protección permanente de archivos también protege al ordenador de posibles virus que vengan a través de una red.
- **Análisis o Protección permanente** de todos los contenidos que llegan a través de correo electrónico (Microsoft Outlook Express y Microsoft Exchange/Outlook) y de aquellos que salen desde el ordenador hacia el exterior (mediante los protocolos SMTP, POP3, NNTP). Esto quiere decir que se analizarán automáticamente todos los mensajes de correo electrónico que se envíen o reciban independientemente del programa de correo electrónico que se utilice. También se analizarán todos los ficheros que se transfieran mediante los protocolos HTTP y FTP así como los Applets Java y controles ActiveX que puedan llegar por el protocolo HTTP. En este caso, la protección permanente se realizará sobre los ficheros una vez descargados o los que se van a enviar. También en estos casos el análisis será independiente del tipo de aplicación utilizada. Por último cabe destacar que también se analizarán en busca de virus todos los datos que se envíen o reciban hacia o desde los grupos de noticias.
- **Análisis o Protección permanente** para todos los mensajes de correo electrónico que se reciban

y envíen mediante en los programas Microsoft Outlook. Esta característica se presenta aparte de la Protección permanente (o análisis permanente) de correo electrónico llegado de Internet porque los dos programas mencionados pueden recibir correo electrónico de un servidor Exchange mediante otros protocolos (conjuntos de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) diferentes. Sin embargo, Panda Antivirus Platinum es capaz de analizar de manera permanente todos los mensajes que se reciban y envíen mediante en estos programas, independientemente del protocolo utilizado.

- **Protección permanente - Firewall** para permitir o restringir los accesos a Internet por parte de los programas instalados en el ordenador, las transferencias de ficheros a través de los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa), los accesos a determinadas direcciones IP (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes), la seguridad de las carpetas compartidas en red, bloqueos de intrusiones realizadas por otros programas o usuarios a tu ordenador, etc.
- **Análisis inmediato** (en el momento en que se desee) de cualquier área del ordenador. Mediante este tipo de análisis se puede chequear cualquiera de las áreas del ordenador en busca de virus. Puede parecer innecesario si se cuenta con una buena protección permanente pero no es así. Si, por cualquier razón, se tiene el ordenador infectado con virus, se debe contar con una manera sencilla de desinfectar completamente el ordenador. La protección permanente no permite esto ya que habría que intentar acceder a todos los ficheros infectados. El análisis inmediato permite analizar todo el sistema, los discos duros, los disquetes, la memoria, los discos locales de la red, mensajes,… de forma con junta o independiente.
- **Análisis bajo demanda** de cualquiera de las carpetas de correo (lugares donde se almacenan los mensajes) gestionadas mediante de los programas Microsoft Outlook Express y Microsoft Outlook. Esto permite analizar todos los mensajes que se hayan recibido o enviado aunque sean anteriores a la instalación del antivirus.

Actualización constante

Lo que Panda Antivirus Platinum ofrece en este aspecto es:

- **Actualización automática del antivirus:** cuando el antivirus detecta una conexión abierta a Internet, comprueba si está actualizado. Si no es así, él mismo se encarga de actualizarse, sin influir para nada en el correcto funcionamiento del sistema. Cuando la actualización automática ha finalizado, él mismo nos informa sobre resultado del proceso. ¡Olvídate!. Si la actualización automática se encuentra activa, olvídate de las actualizaciones del antivirus, ya que él las realizará por su cuenta.
- **Actualización diaria a través de Internet:** todos los días, los clientes registrados de Panda Software, disponen -a través de la página Web de actualizaciones de Panda Software (www.pandasoftware.es/es/actualizaciones.asp)- del último archivo de identificadores de virus (fichero que permite la detección de los virus). Este fichero se actualiza con nuevos virus TODOS LOS DÍAS.
- **Actualización del antivirus completo a través de Internet:** también se dispone en Internet de la última versión del antivirus que se actualiza mensualmente. Si eres cliente registrado de Panda Software, podrás actualizar tu antivirus completo, en la Web de actualizaciones de Panda Software.

Servicios adicionales accesibles desde el propio antivirus

Panda Antivirus Platinum incorpora un paquete con los servicios Panda Software más demandados, útiles y necesarios. Estos servicios sólo están disponibles para los usuarios que hayan realizado su **Registro**.

- **Actualizaciones:** este servicio permite la actualización manual o automática del archivo de identificadores de virus y del antivirus al completo. Para obtener más información, se puede consultar el apartado ¿Qué es una Actualización? de esta ayuda.
- **FAQs:** a través de las divisiones de Soporte Técnico y Atención al Cliente de Panda Software, se han recopilado las dudas y problemas más frecuentes que nos han planteado nuestros clientes. Se ha preparado para cada una de ellas una respuesta eficaz y comprensible que Panda Antivirus Platinum pone a tu disposición para que las puedas consultar en todo momento. A través de la ayuda y la consulta de las FAQs, podrás resolver tus dudas, evitando la necesidad de recurrir a llamadas telefónicas. Para obtener más información, consulta el apartado Servicios de esta ayuda.
- **Envío de consultas:** si mediante la consulta de la ayuda, las FAQs u otros medios, no has encontrado la respuesta a tu duda o problema, puedes recurrir a este servicio. Desde el propio Panda Antivirus Platinum, puedes enviarnos todas tus consultas. Para obtener más información, accede al apartado Servicios de esta ayuda.
- **Soporte técnico en la web:** te atenderemos y podrás resolver todos tus problemas accediendo directamente al soporte técnico que te ofrecemos en la Web de Panda Software. Desde el propio Panda Antivirus Platinum, puedes acceder a una sección de la Web en la que encontrarás ayuda específica para los usuarios de Panda Antivirus Platinum, soluciones a tus problemas, información y soluciones a las infecciones de los virus más peligrosos, acceso a las actualizaciones, recordatorio de claves de registro,… etc. Para obtener más información, accede al apartado Servicios de esta ayuda.
- **S.O.S. virus 24 horas:** mediante este servicio, Panda Software se compromete a entregar en un máximo de 24 horas una solución contra cualquier nuevo virus no detectado con nuestro archivo de identificadores de virus (fichero de firmas de virus -*pav.sig*-) más actualizado. Desde el propio programa, es posible enviar al *Laboratorio de Virus* de Panda Software todos los ficheros que estén causando problemas, con posibles infecciones de nuevos virus. Para obtener más información, se puede consultar el apartado Servicios de esta ayuda.
- **Consultar otros productos antivirus, de seguridad o inventario de Panda Software:** si necesitas conocer otro tipo de herramientas antivirus, de seguridad o inventario, Panda Antivirus Platinum te da información sobre cada una de las soluciones desarrolladas por Panda Software. Para obtener más información, puedes consultar el apartado Servicios de esta ayuda, así como las secciones correspondientes de la Web (Panda Seguro Antivirus Global, o Panda Invent).

Soporte técnico

Uno de los servicios fundamentales que Panda Software ofrece es el soporte técnico. Cuenta con las siguientes características:

- Está disponible las 24 horas del día los 365 días del año. En cualquier momento se puede acceder a él a través de correo electrónico y contar al otro lado con un técnico altamente cualificado dispuesto a solucionar cualquier problema relacionado con los virus.
- Se podrá contactar con el soporte técnico por teléfono (a través de un 906), fax, correo electrónico, correo ordinario o a través de nuestra página Web.

Si deseas consultar más información sobre el soporte técnico, accede a la Web de Soporte de Panda Software.

¿Dónde Puede Estar un Virus?

Es conveniente saber dónde puede "esconderse" un virus. La primera idea a tener clara es que un virus, para poder llevar a cabo su labor de contagiarse o de dañar total o parcialmente los datos del ordenador, debe ejecutarse. No obstante -cada vez más hoy en día-, también existen virus (generalmente se transmiten por correo electrónico), que pueden producir su infección sin llegarse a ejecutar. Por ejemplo, existen virus que pueden llegar en mensajes de correo electrónico. Éstos podrían realizan su infección simplemente con visualizarlos a través de la *Vista previa* (si el programa de correo la tiene activa). Por tanto, los virus se colocarán en lugares estratégicos que les permitan llevar a cabo sus infecciones:

- **Ficheros ejecutables:** los virus se introducen en ficheros ejecutables para poder así tomar el control del ordenador.
- **Documentos de algún programa con capacidad de manejar macros:** tradicionalmente, los ficheros no ejecutables no podían tener virus (o al menos no tenía sentido que los tuvieran) puesto que un virus en un fichero no ejecutable no puede actuar nunca. Sin embargo, el avance de ciertos programas como el paquete de productos Microsoft Office ha dotado a ficheros no ejecutables tales como documentos u hojas de cálculo, de macros. Una macro es un conjunto de instrucciones que pueden ser ejecutadas por un cierto programa. Dicho de otra forma, un documento de Microsoft Word puede contener un conjunto de instrucciones que el propio Word ejecutará. Esto ha abierto la posibilidad a los virus de infectar ficheros no ejecutables pero que puedan contener macros.
- **Ficheros anexos a mensajes de correo electrónico y los propios mensajes de correo electrónico, sin ficheros incluidos:** cualquier tipo de fichero (ejecutable o no ejecutable) se puede anexar o incluir en un mensaje de correo electrónico. Habitualmente, todos los mensajes de correo electrónico junto con sus correspondientes ficheros anexos se almacenan en un único fichero. Como la estructura de este fichero no es estándar ni tiene por qué ser conocida, un antivirus puede ver dicha base de mensajes como un fichero más y no encontrar virus en él. Del mismo modo, el mensaje podría no incluir ningún tipo de fichero y estar igualmente infectado. Esta característica es empleada, especialmente por algunos determinados virus. La infección se produce simplemente con la visualización del mensaje (el virus va incluido en su texto, no dentro de un fichero).
- **Sector boot:** el sector boot es un área dentro de un disquete o disco duro con información importante sobre el tipo de disco. Además, dicho sector almacena un programa que se ejecuta cuando se arranca desde el disco en cuestión. Por tanto y dado que dicho programa almacenado en el sector boot tiene la capacidad de ejecutarse, también es susceptible de ser infectado por un virus. Se debe tener en cuenta que un virus situado en un sector boot se ejecuta si se intenta arrancar desde un disquete aunque éste no sea de arranque.
- **Applets Java:** las páginas de Internet o páginas Web (páginas HTML) sólo podían contener texto y gráficos. Esto ha ido cambiando con la necesidad de poder hacer cada vez páginas más complejas. Ahora, las páginas Web también pueden contener pequeños programas llamados Applets Java. Cuando un navegador de Internet (browser) carga una página Web con alguno de estos pequeños programas, se encarga de ejecutarlos. El funcionamiento es similar al de un documento con una macro. Por tanto, los Applets Java también son susceptibles de ser infectados por virus. Cuando éstos se descargan a nuestro ordenador, son análizados por la protección permanente de archivos.
- **Controles ActiveX:** los controles ActiveX tienen la misma función que los Applets Java. Por tanto y dado que también se ejecutan, pueden verse infectados por virus. Cuando éstos se descargan a nuestro ordenador, son análizados por la protección permanente de archivos.

Panda Antivirus Platinum es capaz de realizar análisis en busca de virus en cualquiera de los lugares

mencionados ofreciendo así los mayores niveles de protección.

Si deseas obtener más información sobre los virus, puedes consultar la Enciclopedia de Virus, en la Web de Panda Software.

Los Virus Informáticos, Gusanos y Troyanos

Una de las mejores defensas contra los virus consiste en conocerlos. Sabiendo cómo funcionan los distintos tipos de virus, qué partes del ordenador afectan y cómo se comportan, podrá defenderse mejor contra ellos.

Básicamente podemos hablar de tres tipos de virus:

Virus de Boot

Virus de Archivo

Virus de Macro

Adicionalmente existen otras *especies* amenazantes -habitualmente consideradas también como virus-. Éstas son las siguientes:

Gusanos

Troyanos o Caballos de Troya

Todos ellos, pueden utilizar diferentes técnicas para realizar sus infecciones, propagarse y llevar a cabo determinadas acciones en los ordenadores infectados. Por este motivo, algunos de ellos pueden englobarse dentro de categorías específicas (en función de las técnicas que emplean -residentes, de sobrescritura, encriptados, multipartites, polimórficos, stealth, de tunneling,…-). Si quieres obtener más información sobre los tipos de virus y las técnicas que éstos utilizan, consulta la sección Técnicas utilizadas por los virus de esta ayuda. También puedes obtener información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Virus de Boot o de Sector de Arranque

Qué es el sector de arranque o boot

El sector de arranque (boot sector) es un área muy importante dentro de un disquete (boot) o un disco duro (MBR - Master Boot Record) dado que contiene información sobre el tipo de disco. Además, dentro de dicho sector hay un programa que se ejecuta al arrancar el ordenador y que se encarga de determinar si hay un sistema operativo en el disco y en caso de que lo haya de ejecutarlo.

Por tanto, cuando se arranca un ordenador, se intentará cargar el programa situado en el sector de arranque para que éste ejecute el sistema operativo. Una vez ejecutado el sistema operativo, se dice que el ordenador está arrancado y podemos comenzar a trabajar con él.

Qué infecta un virus de boot

Un virus de boot infecta el programa situado en el sector de arranque o boot sector. De esta forma, el virus se ejecutará cada vez que se arranque el equipo bien desde disquete, bien desde el disco duro.

Es importante tener en cuenta que hay virus que pertenecen a varios grupos y que por tanto pueden infectar tanto el boot como ficheros.

Cómo se puede contagiar un ordenador con un virus de boot

Para contagiarnos de un virus de boot, debemos arrancar o intentar arrancar el ordenador desde un disquete infectado. Es muy importante tener en cuenta que, aunque un disco NO sea de arranque, también nos puede contaminar con un virus de boot ya que el intento de arrancar es suficiente para que se dé el contagio.

Cómo "trabaja" un virus de boot

Cuando se arranca o intenta arrancar el ordenador desde un disco infectado, lo que sucede en realidad es que el virus se ejecuta. En ese momento, reserva un espacio en la memoria del ordenador y se "traslada" a dicho espacio reservado. Seguidamente, ejecuta el programa original del sector de arranque para ofrecer una apariencia de normalidad y que no se sospeche su presencia en el ordenador.

A partir de ese momento, todos los accesos que se hagan a un disco duro o a un disquete será interceptados por el virus. Éste mirará si el disco en cuestión está infectado y lo contaminará en caso negativo. Esto quiere decir que si se ha arrancado o intentado arrancar desde un disquete contaminado, en el primer acceso que se haga al disco duro éste será contaminado. Por tanto todos los sucesivos arranques que se realicen desde el disco duro estarán ejecutando el virus con lo que éste continuará contaminando más disquetes asegurando su propagación.

Cómo estar prevenido frente a un virus de boot

La mejor protección siempre es contar con un antivirus convenientemente actualizado. Si se tiene activada una protección permanente y se analizan todos los disquetes antes de acceder a ellos, será difícil que un virus de boot entre en el ordenador.

Hay una técnica muy sencilla que permite ofrecer una garantía adicional ya que evita que arranquemos accidentalmente con un disquete olvidado en la disquetera. Dicha técnica consiste en poner la secuencia de arranque en la BIOS de tal forma que siempre se intente arrancar primero

desde el disco duro y luego desde la disquetera.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Virus de Archivo o de Fichero

Qué infecta un virus de fichero

Como su propio nombre indica, un virus de archivo infecta los ficheros contenidos en cualquier medio de soporte físico que no esté protegido contra escritura. Por tanto un virus de archivo es capaz de infectar los ficheros de un disquete o de todo un disco duro.

Es importante tener en cuenta que hay virus que pertenecen a varios grupos y que por tanto pueden infectar tanto el boot como ficheros.

Cómo puede contagiar un virus de fichero

La forma de "contraer" un virus de archivo es ejecutando un fichero previamente infectado. Por eso mismo, los virus habitualmente sólo contagian ficheros ejecutables. La excepción a esto son los virus de macro que contagian ficheros no ejecutables tales como documentos.

Cómo "trabaja" un virus de fichero

Este tipo de virus se encarga de infectar programas o ficheros ejecutables (ficheros con extensiones *EXE* o *COM*). Al realizar la ejecución de uno de estos programas -de forma intencionada o no intencionada-, el virus se activa. Esto hace que se produzcan los efectos dañinos que caractericen al virus en cada caso. La mayoría de los virus existentes son de este tipo, pudiéndose clasificar cada uno de ellos en función de las acciones que realizan en cada caso.

Virus de fichero residentes: estos virus comprueban, en primer lugar, si se cumple la condición que hace que "ataquen". Si es así, el virus llevará a cabo su acción destructiva. Si no es así, el virus reservará un espacio en memoria y continuará con la ejecución del fichero normalmente para que no se note su presencia. Entonces, todas aquellas operaciones que se vayan a llevar a cabo con ficheros serán interceptadas por el virus que contaminará todos aquellos ficheros que no lo estuvieran previamente.

Virus de fichero de acción directa: estos virus también comprueban en primer lugar si se cumple la condición que hará que lleven a cabo su acción destructiva. Si es así, el virus contaminará en ese momento a nuevos ficheros. Generalmente suelen contaminar los ficheros del directorio actual o los ficheros de los directorios referenciados por la variable *PATH* del sistema. Finalmente, el virus continuará con la ejecución normal del fichero para que no se note su presencia. Como se ha visto, estos virus no se quedan en memoria sino que infectan en el mismo momento de su ejecución.

Virus de compañía: estos virus pueden ser residentes (permanentes) o de acción directa. Lo que los diferencia de los anteriormente comentados, es que sacan beneficio de un detalle del sistema operativo, concretamente del sistema operativo MS-DOS. En él, si existen dos ficheros con el mismo nombre pero con extensión *COM* y *EXE*, ejecutará primero el que tenga extensión *COM*. Por tanto, un virus de compañía no infecta un *EXE* sino que crea un *COM* (con el atributo de *oculto* para disimular su presencia) que contiene el virus. Cada vez que se intente ejecutar el fichero *EXE* se ejecutará en realidad el *COM* que llevará a cabo su labor y finalmente ejecutará el fichero *EXE* para que no se note su presencia.

Virus de sobreescritura: en todos los casos anteriores, el virus infectaba otros ficheros sin alterar el contenido original del fichero, tan sólo se limitaba a añadir cosas. Los virus de sobreescritura contaminan ficheros pero sobrescribiendo parcialmente la información contenida en ellos. Los efectos

de esta forma de actuar son dos: el fichero no vuelve a funcionar nunca más y no se puede desinfectar puesto que parte de la información original del fichero se ha perdido.

Cómo estar prevenido frente a un virus de fichero

En primer lugar, es muy importante tener siempre activada la protección permanente. La función de la protección permanente es vigilar todas aquellas operaciones del sistema operativo que suponen operaciones con ficheros.

Gracias a una buena protección permanente podemos estar protegidos frente a los virus de archivo. Adicionalmente hay una serie de medidas muy aconsejables. Son las siguientes:

- Analiza previamente todos aquellos ficheros que recibas, sea por el medio que sea: DVD, CD-ROM, disquetes, vía red, correo electrónico, Internet, etc.
- Utiliza sólo software original y de confianza.
- Realiza análisis periódicos de tu disco duro para verificar que no haya logrado entrar ningún virus.

Siempre es necesario contar con un buen antivirus convenientemente actualizado.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia). Si deseas consultar más consejos, puedes obtenerlos en el apartado Consejos para Mantenerse Alejado de los Virus, de esta ayuda.

Virus de Macro

Qué infecta un virus de macro

Dado que un virus no es más que un programa, para poder hacer algo debe ser cargado por el sistema operativo. Esta es la razón por la que los virus únicamente contagian ficheros ejecutables. Por mucho que un virus contamine un fichero de texto, éste -al no ser ejecutable-, nunca tomará el control del ordenador y por tanto nunca se podrá activar.

Todo esto cambia en el caso de los virus de macro. Las capacidades cada vez mayores de ciertos programas tales como procesadores de texto, hojas de cálculo, etc. han llevado a sus desarrolladores a incorporarles una interesante función: las macros. Una macro es una secuencia de instrucciones que el programa en cuestión (el procesador de texto o la hoja de cálculo por poner un ejemplo) es capaz de interpretar y ejecutar.

Por tanto, si se introduce código vírico en una de estas macros, dicho código será ejecutado por el programa accediendo así al control del ordenador.

Todo lo anterior quiere decir que los ficheros manejados por dichos programas (documentos, hojas de cálculo, etc.) tienen la capacidad de contener virus y contaminar otros ficheros de su mismo tipo.

Un peligro adicional de este tipo de virus es que, dado su carácter, se ejecutan "dentro" de un programa. Esto quiere decir que si el programa en cuestión es multiplataforma (es decir, si puede ejecutarse en diferentes sistemas operativos) el virus también lo será aumentando así el campo de posibles ficheros a infectar.

Cómo puede contagiar un virus de macro

Los virus de macro aprovechan una característica habitual en los programas que manejan macros. Se puede ver claramente en el caso del programa Word. Dicho programa maneja básicamente dos tipos de ficheros: documentos y plantillas. Las plantillas sirven para definir documentos genéricos y hacer así más fácil el trabajo no teniendo que empezar siempre desde cero.

En el caso de Word, son las plantillas las que pueden contener macros. El problema estriba en que, por defecto, todos los documentos se basan en una determinada plantilla denominada *NORMAL.DOT*. Dicha plantilla cuenta con una macro que se ejecuta automáticamente nada más abrir la plantilla.

Ésta es la característica de la que se aprovechan los creadores de virus. Contaminando la macro que se ejecuta automáticamente, se aseguran de activar el virus que a continuación contaminará todos aquellos documentos que se abran.

Cómo trabaja un virus de macro

Tal y como se ha explicado, las macros víricas se ejecutan y contaminan todos aquellos documentos que se abran. Éstos serán los encargados de transmitir la "infección".

Una de las características más peligrosas de los virus de macro es su alta velocidad de propagación. Por ejemplo, en una empresa un documento contaminado situado en la red y que consulten diferentes personas puede contaminar todos los documentos de la empresa en un espacio de tiempo muy breve.

El gran intercambio de este tipo de ficheros mediante correo electrónico hace que estos virus puedan propagarse a cualquier lugar del mundo en tiempos verdaderamente asombrosos.

Es importante señalar que, a pesar de que se crea lo contrario, el efecto que pueden llegar a tener estos virus es muy perjudicial igualando a los perjuicios que pueda llegar a causar cualquier virus de boot o de archivo.

Cómo estar protegido frente a un virus de macro

La protección más eficaz frente a los virus de macro es contar con un antivirus con protección permanente. De esta forma, cada vez que se intente abrir un documento infectado, la protección permanente nos avisará y cancelará la operación eliminando todo riesgo.

Dada la facilidad de expansión de este tipo de virus mediante el correo electrónico, también es recomendable contar con un antivirus con capacidad de analizar el correo electrónico en el mismo momento de su recepción y antes siquiera de que sea abierto.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Gusanos

Qué infecta un gusano

Los gusanos, aunque funcionan de forma similar a los virus, no lo son como tales. Los gusanos se diferencian de los virus en que no intentan infectar otros ficheros. Su objetivo es extenderse, empleando avanzadas técnicas de propagación. Es decir, crear copias de sí mismos y con ellas realizar infecciones en otros ordenadores. Las infecciones se realizan, en la mayoría de los casos, a través del correo electrónico, redes de ordenadores y canales de Chat IRC en Internet. También es posible que se reproduzcan en la propia memoria del equipo afectado.

Cómo puede contagiar o extenderse un gusano

Los gusanos que centran sus infecciones en otros ordenadores, copian el programa que utilizan para realizar la infección en un determinado directorio de dicho equipo. Esto lo consiguen propagándose a través de cualquiera de las posibles vías de entrada o acceso a otros ordenadores. Un gusano también puede estar compuesto por varios programas. Entonces, cada uno de ellos actúa de forma subordinada a uno de éstos que se considerará principal. Esta variación, suele ser denominado como gusano de red.

Cómo trabaja un gusano

Podemos resumir los pasos que generalmente lleva a cabo un gusano, para producir sus infecciones, en los siguientes:

1. El gusano aprovecha los fallos de seguridad en el sistema, o en una determinada herramienta software, para introducirse en el ordenador, o en una red de ordenadores.
2. El gusano entra en los equipos a los que pueda acceder a través de un hueco de seguridad, o una vulnerabilidad.
3. Una vez allí, el gusano crea una copia de sí mismo.
4. Después, intenta introducirse en todos los ordenadores a los que pueda tener acceso desde éste (ya sea a través de una red, o a través de Internet).

Cuando un gusano es ejecutado, se instala y permanece generalmente inactivo hasta que se apaga o se reinicia el ordenador. No obstante cada uno de ellos utiliza técnicas diferentes para asegurar su ejecución siempre que se arranca el ordenador y se entra en Windows. Por ejemplo la modificación del *Registro de Windows*.

Cómo estar protegido frente a un gusano

La mejor forma es proteger todas las posibles vías de entrada, por las cuales se pueden introducir en el sistema. Entre ellas, hay que tener en cuenta el correo electrónico y las conexiones mediante chat IRC. Además de éstas -las más utilizadas por los gusanos en los últimos tiempos-, hay que proteger todas las restantes.

Por otra parte, los gusanos aprovechan vulnerabilidades existentes en determinadas herramientas de software. Para proteger estas posibles entradas, es necesario contar con las últimas versiones de dicho software, convenientemente actualizadas con los últimos parches a tal efecto.

Tipos de gusanos

Dependiendo del lenguaje en el que se encuentren escritos los gusanos, y los métodos que utilicen

para extenderse, podemos diferenciar varios tipos. Algunos podrían ser los siguientes:

- *Gusanos de correo electrónico.* Se propagan a través de mensajes de correo electrónico, utilizando programas clientes de correo como Outlook Express, Outlook, etc.
- *Gusanos de IRC (gusanos de mIRC y de Pirch).* Se propagan a través de los canales de Chat, utilizando programas como mIRC y Pirch.
- *Gusanos de VBS (Visual Basic Script).* Están escritos o creados en el lenguaje de priogramación Visual Basic Script.
- *Gusanos de Windows32.* Se propagan a través de las API de Windows.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Troyanos o Caballos de Troya

Qué infecta un troyano

Los troyanos, aunque funcionan de forma similar a los virus, no lo son como tales. Los troyanos simulan ser programas inofensivos que llegan a nuestro ordenador por cualquier medio posible. El usuario, creyendo que se trata de una aplicación de gran utilidad o un fichero de interés para él, lo ejecuta o lo abre. En ese momento el troyano se instala en su ordenador otro programa que producirá efectos nocivos.

Cómo puede contagiar o extenderse un troyano

Los troyanos incluyen o ‘‘cuelan’’ determinados programas en nuestro ordenador, a través de cualquiera de los conocidos medios de contagio. Éstos se encargan de realizar las acciones necesarias para entorpecer nuestro trabajo, causar daños en mayor o menor medida y robar información.

Cómo trabaja un troyano

Un troyano puede haberse introducido en nuestro ordenador y, sin embargo, no haber realizado ninguna acción o efecto. Éste se mantendrá a la espera de que se cumpla una determinada condición -condición de activación-, para actuar. Cuando esto ocurra podrán activarse huecos de seguridad (backdoor) en nuestro ordenador que permitan la eliminación de ficheros, o la pérdida de información del disco duro. A través de estos huecos de seguridad, nuestro equipo podría ser atacado.

Su principal objetivo es el acceso a determinados puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) para dejarlos abiertos y accesibles desde el exterior (de ahí el nombre de troyanos -adoptando el nombre del *Caballo de Troya* de la mitología-). Esto implica que mediante una conexión (desde otro equipo de la red local, o conectado a Internet) se podría acceder a toda la información contenida en el equipo afectado por el troyano y realizar en él todo tipo de acciones.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Técnicas Utilizadas por los Virus

Para evitar su detección por parte de los antivirus, los virus han ido desarrollando una serie de técnicas especializadas y complejas. Los antivirus han tenido que ir adaptándose a estas nuevas técnicas para poder detectar los cada vez más complejos y perfeccionados virus.

Estas son algunas de las técnicas que, más habitualmente, utilizan los virus:

Sobreescritura / Virus de Sobreescritura: esta técnica se aplica sobre los ficheros que han sido infectados por el virus. El virus se encarga de escribir información dentro del contenido del fichero, o en parte de él, de tal forma que dicho fichero pierde información definitivamente (no se puede recuperar).Un virus de sobreescritura, puede aplicar a demás cualquier otro tipo de las técnicas aquí comentadas.

Ocultamiento (Stealth): es una técnica propia de los virus residentes. La infección de un fichero hace necesario modificar el fichero contaminado. Esto hace que se pueda saber que un virus ha manipulado dicho fichero. Para evitarlo, el virus residente puede llegar a vigilar todas aquellas operaciones destinadas a obtener información sobre el fichero infectado e interceptarlas ofreciendo la información anterior a la infección perpetrando así el engaño.

Sobrepasamiento (Tunneling): los virus y los antivirus usan técnicas parecidas. Los virus interceptan todas las operaciones del sistema operativo sobre ficheros para poder contaminar todos aquellos ficheros a los que acceda. Por otro lado, las protecciones permanentes de los antivirus interceptan también las operaciones sobre ficheros para vigilar que los ficheros a los que se pretende acceder no estén contaminados. Mediante la técnica de sobrepasamiento o tunneling, un virus logra encontrar los servicios interceptados por la protección permanente y usarlos directamente sin que la protección permanente lo sepa. No obstante, existen técnicas antivirus alternativas, que permiten la detección de los virus que realizan este tipo de operaciones.

Autoencriptación / Virus Encriptados o Cifrados: los virus tienen como principal misión replicarse a sí mismos. Los antivirus los detectan buscando una cierta cadena (también llamada firma) que sea igual en todas las copias de un mismo virus. Para evitar este mecanismo de búsqueda de virus (que es el más común) algunos virus son capaces de encriptarse cambiándose cada vez que infectan un fichero. De esta forma, el virus nunca se replica exactamente igual con lo que el método tradicional falla. Sin embargo, la rutina que sirve para hacer la encriptación es siempre la misma y en esto se pueden basar los antivirus para localizar a este tipo de virus.

Polimorfismo / Virus Polimórficos: en este caso, los virus no sólo se encriptan de manera distinta cada vez sino que cada vez varía la propia rutina de encriptación. De esta manera, no hay dos copias de un mismo virus que sean iguales, todas sus partes varían. Para detectar este tipo de virus se usan técnicas de simulación de desencriptación que obligan al virus a "mostrarse".

Virus Multipartites: este tipo de virus pueden realizar varias o múltiples infecciones. En cada una de estas infecciones, pueden utilizar técnicas diferentes. La combinación de varias técnicas de infección les hace bastante peligrosos.

Puedes consultar más información sobre virus en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

¿Cómo Prevenir las Infecciones?

A continuación te ofrecemos una serie de consejos para prevenir las peligrosas infecciones debidas a los virus, gusanos o troyanos. Recuerda que la prevención es una de las herramientas más eficaces para luchar contra los virus informáticos.

Copias de seguridad: acostúmbrate a realizar copias de seguridad de tus datos más importantes periódicamente. Es uno de los consejos más escuchados y menos atendidos del mundo informático. Unas copias de seguridad periódicas no sólo son una solución frente a los virus sino frente a cualquier posible problema que se pueda dar en el ordenador. Si sólo se hacen copias de seguridad de los datos importantes, se lograrán copias de seguridad pequeñas y rápidas de hacer. Es conveniente hacer al menos una copia de seguridad mensual.

Analiza todo lo que recibas: esta es una de las bases más importantes en la prevención. Analiza todos aquellos programas o ficheros que vayas o hayas introducido en tu ordenador, antes de ejecutarlos o abrirlos. De esta forma podrás detectar los posibles virus antes de que tengan tiempo de infectar ninguno de tus ficheros.

Analiza todo lo que envíes: ten la completa seguridad de que todo lo que envías a otros usuarios o compartes en una red de ordenadores, está completamente libre de virus. Si bien es cierto que debemos proteger las entradas de virus a nuestro ordenador, también es cierto que es importante impedir que nosotros mismos demos lugar a otras infecciones.

Cuenta con una protección permanente activa: las protecciones permanentes vigilan constantemente todas aquellas operaciones realizadas en el ordenador que sean susceptibles de permitir una infección por un virus. Si se tienes activada una buena protección permanente como la incluida en Panda Antivirus Platinum, el riesgo de contagio es mínimo y se facilita enormemente el trabajo con el ordenador ya que no hay que estar pendiente de analizar todo lo que se recibe. La protección permanente se encarga de ello automáticamente.

Análisis periódicos: analiza todo tu ordenador periódicamente. Gracias a los análisis programados de Panda Antivirus Platinum es fácil realizar análisis periódicos en los momentos en los que no se esté trabajando con el ordenador. Este tipo de análisis periódicos impedirá que, si un virus ha entrado en tu ordenador, se extienda demasiado. Es conveniente realizar un análisis de todo el sistema al menos una vez a la semana, aunque esto depende del uso que se haga del ordenador.

Permanece actualizado: dada la cantidad de virus nuevos que se detectan mes a mes, del orden de los 300, es imprescindible contar con un servicio de actualizaciones que mantengan el antivirus al día. De otro modo, cada mes nuevos y peligrosos virus serán capaces de infectar tu ordenador con impunidad.

Disco de arranque limpio (Discos de Rescate): por lo que pueda pasar, guarda a mano un disquete de arranque limpio de virus. Esto facilitará la limpieza del ordenador en caso de que esté contaminado por un virus. Aunque dicho disco lo puedes crear tu mismo, Panda Antivirus Platinum te permitirá crear varios discos. Con ellos podrás arrancar el ordenador desde un entorno libre de virus y además, analizar el ordenador mediante el antivirus en línea de comandos. Por lo tanto, es conveniente crearlos y contar así con un disco de arranque y discos de desinfección (discos de rescate). Éstos constituyen una herramienta imprescindible para limpiar un ordenador infectado por un virus.

En definitiva, sería conveniente que tuvieses en cuenta y llevases a la práctica una serie de consejos. Si deseas consejos sobre la prevención de infecciones y la protección antivirus, consulta la sección **Consejos para Mantenerse Alejado de los Virus** (en esta ayuda), o accede a la Enciclopedia de Virus, en la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Consejos para Mantenerse Alejado de los Virus

Si deseas mantenerte alejado de los virus, o evitarlos, es recomendable que sigas los siguientes consejos que te sugiere Panda Software:

1. **Utiliza un buen antivirus y actualízalo frecuentemente.** La mejor manera de estar protegido contra los virus es instalar un buen antivirus en tu ordenador.

   Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Porque los conoce, sabe cómo actúan y también sabe cómo eliminarlos.

Sin embargo, cada día aparecen más de 20 nuevos virus que los antivirus no son capaces de reconocer. Para la detección y eliminación de estos virus es necesario actualizar frecuentemente nuestro antivirus. Por lo tanto, la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización, preferentemente diaria

2. **Comprueba que tu antivirus incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta.** Si bien un antivirus perfectamente actualizado es la mejor arma para luchar contra los virus, es aconsejable contar con servicios adicionales.

   El servicio de soporte técnico, bien a través de correo electrónico o por teléfono, es de gran ayuda ante cualquier problema o duda que pueda surgir relacionado con virus o con el funcionamiento del antivirus.

En el supuesto de verse afectado por algún virus de reciente creación, se debe contar con un servicio de resolución urgente de nuevos virus capaz de eliminarlos en el menor tiempo posible.

Otro servicio fundamental son las alertas sobre nuevos virus peligrosos, por ejemplo, a través de listas de correo.

3. **Asegúrate de que tu antivirus esté siempre activo.** Un antivirus está activo cuando dispone de una protección permanente capaz de vigilar constantemente todas las operaciones realizadas en

el ordenador.

Existen dos maneras para comprobar que la protección permanente está activa; a través de un icono fijo en la *Barra de tareas de Windows*, junto a la información horaria, o en la propia configuración del programa antivirus.

Estar protegido contra los virus requiere una protección permanente, tanto de fciheros como de correo electrónico

4. **Verifica, antes de abrirlo, cada nuevo mensaje de correo electrónico recibido.** El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.

   Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip"). Además, no es necesario ejecutar el fichero adjunto de un mensaje de correo para ser infectado; en algunos sistemas basta únicamente con abrir el mensaje, o visualizarlo mediante la *Vista previa*'

Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente al utilizado normalmente por el remitente.

5. **Evita la descarga de programas de lugares no seguros en Internet.** Muchas páginas de Internet permiten la descarga de programas y ficheros a los ordenadores de los internautas. Cabe la posibilidad de que estos ficheros estén infectados con virus.

Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de

programas desde sitios Web que no nos ofrezcan garantías. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.

6. **Rechaza archivos que no hayas solicitado, cuando estés en chats o grupos de noticias (news).** Gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los grupos de noticias y los chats, respectivamente.

   Los grupos de noticias o "news", como no son listas de correo y usan su propio sistema de transmisión por Internet (NNTP), también necesitan de una protección eficaz y constante.

Ambos sistemas, además de permitir la comunicación con otras personas, también facilitan la transferencia de ficheros. Aquí es donde hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.

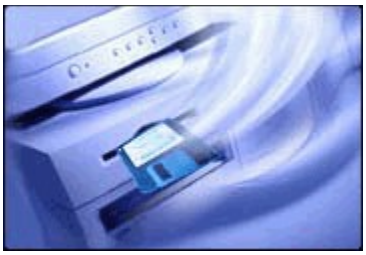
7. **Analiza siempre con un buen antivirus los disquetes que vayas a usar en tu ordenador.** Además de Internet, otra de las vías de infección de virus más frecuente son los disquetes.

   Es una buena norma analizar, mediante un buen antivirus, todos aquellos disquetes que entren y salgan de nuestro ordenador.

Al utilizar nuestros disquetes en otros ordenadores es aconsejable protegerlos contra escritura, bajando la pestaña de la parte inferior derecha del disquete, en su parte trasera.

8. **Retira los disquetes de las disqueteras al apagar o reiniciar tu ordenador.** A pesar de que Internet es uno de los medios de propagación de virus más habituales, cabe resaltar que los disquetes siguen siendo una vía de infección de gran magnitud.

   Además de analizar con un antivirus todos los disquetes utilizados, una forma de evitar que se activen los ya clásicos virus de boot o de arranque consiste en retirar los disquetes de las disqueteras al apagar o reiniciar el ordenador.



Por si se nos olvida hacerlo, es conveniente contar con un antivirus capaz de comprobar en tales circunstancias la existencia de disquetes infectados.

9. **Analiza el contenido de los archivos comprimidos.** Los ficheros comprimidos, muy útiles por contener en su interior múltiples ficheros y ocupar menos espacio, son un caldo de cultivo para los virus.

   En primer lugar, hay que demandar a nuestro antivirus que detecte el mayor número de formatos comprimidos posible

Antes de abrir directamente uno de estos ficheros, como los de formato ZIP, es aconsejable guardarlos en carpetas temporales -creadas por los usuarios y cuyos ficheros pueden ser posteriormente borrados- en lugar de abrirlos sobre directorios de trabajo, por ejemplo, la carpeta *Windows*, *Mis Documentos*, el *Escritorio*, etc.

10. **Mantente alerta ante acciones sospechosas de posibles virus.** Mediante el simple uso del ordenador, hay numerosos síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los ficheros, avisos de macros en documentos Word o Excel que en principio no deberían contenerlas, recepción por parte de otras personas de mensajes nuestros de correo que no hemos enviado.

Como solución más completa a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de nuestra compañía antivirus.

11. **Adopta las medidas y opciones de seguridad correspondientes a las aplicaciones que usas normalmente, en tu política de protección antivirus.** Los programas informáticos más utilizados se convierten, precisamente por esa razón, en blanco de los autores de virus. Sus fabricantes suelen incluir en ellos opciones de seguridad contra virus.

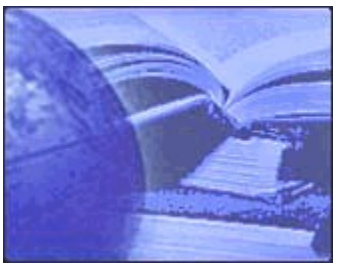
    Tal es el caso de los navegadores de Internet, procesadores de texto, programas de correo, etc., que disponen de características para asegurar un poco más la información. Si no estamos familiarizados con ellas, podemos acudir a la ayuda del propio programa y realizar una búsqueda del término *seguridad* para saber cómo utilizarlas.

Es conveniente aprovechar estas opciones específicas de seguridad, además de contar con un antivirus constantemente actualizado.

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

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

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



Sin embargo, ante la gran cantidad de información recibida por diferentes medios, es aconsejable

contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos: compañías antivirus, empresas consultoras de seguridad, organismos que informan de alertas tempranas, organismos gubernamentales, universidades, etc.

14. **Utiliza siempre software legal.** A la hora de instalar nuevos programas en el ordenador, el riesgo de infección es menor si se trata de software legal.

    Sin embargo, si el software nos ha llegado en un CD-ROM pirata, o se trata de software legal manipulado posteriormente para saltarse la protección de los propios fabricantes, nadie nos puede asegurar que esté libre de virus.

Además, si se trata de software antivirus, su legalidad nos permite disfrutar de todos los servicios adicionales que garantizan su eficacia y seguridad.

15. **Exige a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus.** En la lucha contra los virus se precisa la participación de todos los agentes implicados en el sector informático: empresas, usuarios finales, compañías antivirus, medios de comunicación, etc.

    Como Internet es el medio más utilizado por los virus para su propagación, la colaboración de los proveedores de acceso a Internet es muy importante.

Así mismo, es aconsejable que los fabricantes de software y las publicaciones que ofrecen CD-ROM adopten medidas para no difundir virus.

La contribución de todos ellos ayudará a minimizar el problema de las infecciones provocadas por virus.

Nota: puedes consultar estos consejos y otras informaciones de interés respecto a los virus informáticos en la Enciclopedia de Virus, dentro de la Web de Panda Software (www.pandasoftware.es/enciclopedia).

Discos de Rescate

En ocasiones, cuando nos encontramos bajo la amenaza de ciertos virus, puede ocurrir que sea imposible arrancar el ordenador, o hacerlo desde un entorno libre de virus. En tal caso es necesario poder arrancar el ordenador desde un disquete de arranque o sistema (libre de virus) y poder realizar un análisis, detección y desinfección desde la disquetera (con ese u otros discos).

Panda Antivirus Platinum permite crear varios discos que harán posible iniciar, analizar y desinfectar un ordenador desde un entorno libre de virus: los denominados *Discos de Rescate*. Teniendo en cuenta que un entorno seguro es todo ordenador en el que no haya virus residentes en memoria que puedan interferir con el análisis o con la desinfección.

Panda Antivirus Platinum cuenta con una utilidad para la creación de estos discos: **Discos de Rescate**. Su misión es la de crear unos discos que permitan el arranque y el análisis de un ordenador. Con estos discos será posible arrancar el ordenador e impedir que los virus se puedan cargar en memoria, cuando el ordenador se inicie (siempre que estos discos se encuentren siempre libres de virus -cuando los hayas creado, es aconsejable protegerlos contra escritura, mediante la pestaña correspondiente-).

Una vez arrancado el ordenador, será posible analizarlo y desinfectarlo desde los discos de rescate, ya que estos contienen el antivirus en línea de comandos.

Como nota adicional, cabe destacar que es muy importante que los *Discos de Rescate* se creen en un ordenador limpio de virus. Esto nos garantiza que los disquetes generados también se encuentran libres de virus. En caso contrario, estos discos no servirán de nada ya que no permitirán un arranque del ordenador libre de virus.

Los discos de rescate pueden crearse de dos formas:

Desde en botón Inicio de Windows

1. Pulsa el botón **Inicio** de Windows.
2. Selecciona **Programas**.
3. Accede el grupo de programas **Panda Antivirus Platinum**.
4. Selecciona la opción **Discos de Rescate**.
5. Se muestra una explicación sobre el cometido de los *Discos de Rescate*. Ten a mano tres disquetes de 3 ½ de alta densidad vacíos, donde se generarán los *Discos de Rescate*. Pulse el botón **Siguiente**.
6. Se pide la introducción de un disquete en la disquetera (*Disco de Rescate 1*). Hazlo y pulsa el botón **Aceptar** (se perderá el contenido de este disco y se copiarán en él ciertos ficheros).
7. Se pide la introducción de otro disquete (*Disco de Rescate 2*). Extrae el primero, rotúlalo como *Disco de Rescate 1* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado). Entonces, introduce el siguiente disco y pulsa el botón **Aceptar** (se perderá el contenido de este disco y se copiarán en él ciertos ficheros).
8. Se pide la introducción de otro disquete (*Disco de Rescate 3*). Extrae el segundo, rotúlalo como *Disco de Rescate 2* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado). Entonces, introduce el siguiente disco y pulsa el botón **Aceptar** (se

perderá el contenido de este disco y se copiarán en él ciertos ficheros).

9. Se muestra un mensaje indicando el final del proceso de creación de los Discos de Rescate. Pulsa el botón **Cerrar**. Extrae el tercero, rotúlalo como *Disco de Rescate 3* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado).

Desde la ventana del antivirus

1. En la ventana del antivirus, selecciona la opción **Inicio**, dentro del **Panel de control**.
2. Si aun no has creado los discos de rescate, se te indicará en la sección **Avisos**, a través de un texto como el siguiente: ***Todavía no has creado los discos de rescate. ¡Hazlo ahora!***. Cuando ya hayas creado los discos de rescate, dicho aviso desaparecerá de esta sección.
3. Si pulsas sobre dicho aviso o sugerencia, se ejecutará el asistente para la creación de los discos de rescate.
4. Se muestra una explicación sobre el cometido de los *Discos de Rescate*. Ten a mano tres disquetes de 3 ½ de alta densidad vacíos, donde se generarán los *Discos de Rescate*. Pulse el botón **Siguiente**.
5. Se pide la introducción de un disquete en la disquetera (*Disco de Rescate 1*). Hazlo y pulsa el botón **Aceptar** (se perderá el contenido de este disco y se copiarán en él ciertos ficheros).
6. Se pide la introducción de otro disquete (*Disco de Rescate 2*). Extrae el primero, rotúlalo como *Disco de Rescate 1* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado). Entonces, introduce el siguiente disco y pulsa el botón **Aceptar** (se perderá el contenido de este disco y se copiarán en él ciertos ficheros).
7. Se pide la introducción de otro disquete (*Disco de Rescate 3*). Extrae el segundo, rotúlalo como *Disco de Rescate 2* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado). Entonces, introduce el siguiente disco y pulsa el botón **Aceptar** (se perderá el contenido de este disco y se copiarán en él ciertos ficheros).
8. Se muestra un mensaje indicando el final del proceso de creación de los Discos de Rescate. Pulsa el botón **Cerrar**. Extrae el tercero, rotúlalo como *Disco de Rescate 3* y protégelo contra escritura, moviendo la pestaña del disco (así evitarás borrados accidentales del mismo, o que sean pueda contaminar por algún virus si se introducen en un ordenador infectado).

¿Cómo se utilizan los Discos de Rescate?

Si en algún momento es necesario utilizar los *Discos de Rescate*, para arrancar el ordenador desde un entorno libre de virus y/o analizarlo, hazlo del siguiente modo:

1. Con el ordenador apagado, introduce el *Disco de Rescate 1* en la disquetera.
2. Enciende, reinicia, o arranca el ordenador. Éste detectará un sistema operativo en el disquete que se encuentra en la disquetera y arrancará o se iniciará desde él.
3. Sigue las instrucciones que aparecerán en pantalla.

Registro OnLine

Un antivirus, además de ser una herramienta capaz de detectar y eliminar todos los virus, debe estar acompañado de unos servicios que incrementen las prestaciones de éste (actualizaciones, servicio de asistencia técnica ante incidencias víricas, posibilidad de realizar consultas técnicas, soporte continuo, … etc.).

La versión comercial de tu Panda Antivirus Platinum incluye una serie de servicios que lo acompañan, haciéndolo mucho más completo y útil.

Para poder acceder a dichos servicios y utilizarlos de forma correcta, es necesario registrarse como usuario de Panda Antivirus Platinum. Sólo en tal caso, podrán ser utilizados los servicios.

¿Cómo se realiza el registro?. Muy sencillo, éste se puede realizar durante el proceso de instalación del antivirus, o posteriormente cuando ya se encuentre instalado. En cualquier caso, éste será un registro online. Esto quiere decir que se realizará mediante el acceso a la sección de Registro (service.pandasoftware.es/rol), en la Web de Panda Software. Si tu antivirus incluye una tarjeta de registro, también podrás registrarse como usuario, rellenándola y enviándola por correo electrónico, postal, o fax a Panda Software.

Si decides realizar tu registro online, tras la instalación del antivirus, debes hacerlo desde la sección **Servicios**, en la ventana de Panda Antivirus Platinum, del siguiente modo:

1. En la ventana del antivirus, pincha sobre la opción **Servicios**, dentro del **Panel de control**.
2. En la sección inferior se te indica la necesidad de realizar un registro, para poder acceder y utilizar cada uno de los servicios incluidos en Panda Antivirus Platinum. Pulsa sobre la dirección Web que se te indica y accederás directamente a la página de registro online de Panda Software.
3. Una vez allí, indica tu **País** y tu **Idioma**.
4. Indica también si utilizarás tu Panda Antivirus Platinum en una empresa, o no.
5. Finalmente indica alguna vez anteriormente te has registrado como cliente de Panda Software, o no.
6. Sea cual sea la respuesta a la pregunta anterior, rellena los datos que se te indican y pulsa el botón **Enviar**.

Si decides realizar tu registro online, durante la instalación del antivirus, selecciona la casilla correspondiente. Esto te llevará a la página de registro online de Panda Software. Una vez allí, indica tu **País** y tu **Idioma**, indica si utilizarás el antivirus en una empresa o no, e indica también si te has registrado en alguna ocasión anterior como cliente de Panda Software. En cualquier caso, rellena los datos que se te soliciten y pulsa el botón **Enviar**.

Requisitos de Instalación

Para que sea posible la instalación y correcto funcionamiento de Panda Antivirus Platinum, deben cumplirse previamente una serie de requisitos de hardware y software. Éstos son los siguientes:

Requisitos para la instalación del antivirus

- **Procesador:** Pentium 300 Mhz.
- **Memoria RAM:** 128 MB.
- **Disco Duro:** 50 MB de espacio libre mínimo en disco duro.
- **CD-ROM:** se debe contar con una unidad de CD-ROM, para la instalación de Panda Antivirus Platinum, ya que solamente se distribuye en este tipo de soporte físico. Si has descargado tu Panda Antivirus Platinum desde Internet, no necesitarás contar con unidad de CD-ROM, para instalar el antivirus.
- **Sistema Operativo:** tener instalado alguno de los siguientes sistemas operativos: Windows XP, Windows 2000 Pro, Windows NT WS 4.0, Windows Me, Windows 98, o Windows 95.
- En la configuración de las propiedades -colores- de la pantalla, es necesario establecer que ésta debe trabajar con, al menos, 16 Bits -Colores: Color de alta densidad (16 Bits)-.

Requisitos para la instalación del firewall

- Si tienes instalado Windows NT WS 4.0, debes contar con el Service Pack 5, o superior e Internet Explorer 5.01 o superior.
- Si tienes instalado Windows 95, debes contar con Dun 1.3 (Dial-Up Networking) y Winsock 2 (*WS2_32.DLL*)
- Si tienes instalado el firewall Sygate, debes desinstalarlo.

Instalación de Panda Antivirus Platinum

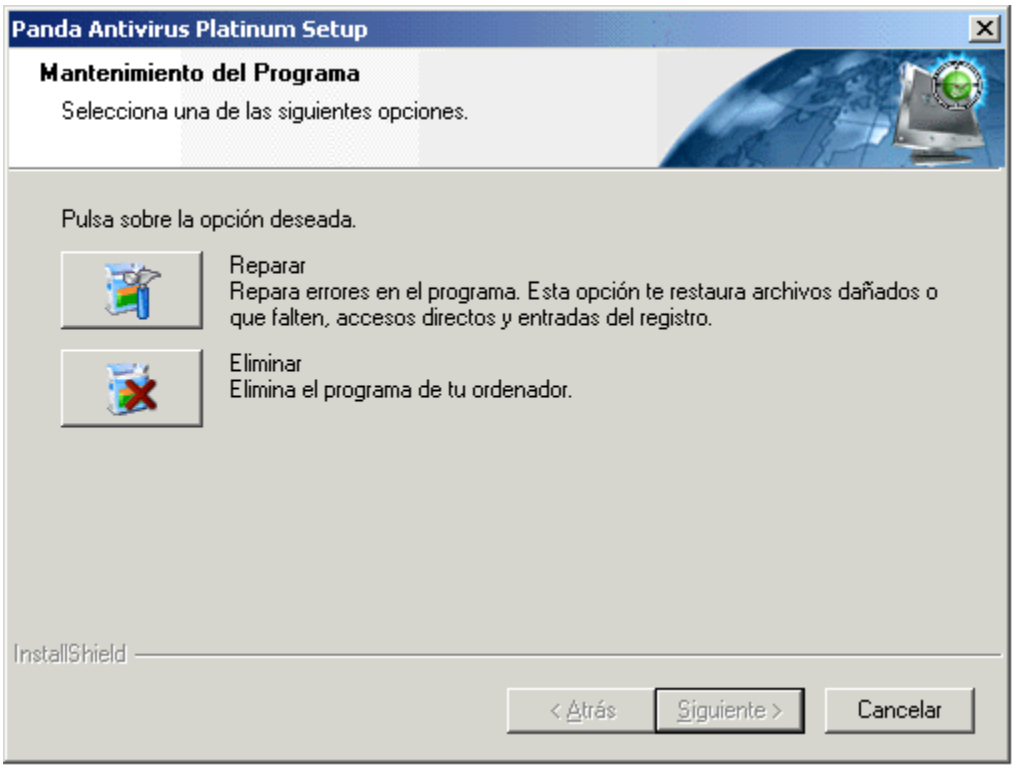
Antes de comenzar con la instalación de Panda Antivirus Platinum, asegúrate de que se cumplen los requisitos previos necesario para instalar el antivirus y que éste funcione correctamente. Puedes consultarlos en la sección Requisitos de Instalación, de esta ayuda.

Puedes haber adquirido u obtenido tu Panda Antivirus Platinum mediante una descarga desde Internet (página Web de Panda Software, u otras), o a través de CD-ROM. Aunque el proceso de instalación es el mismo o similar en ambos casos, vamos a diferenciar las dos posibilidades en cuanto a la instalación se refiere.

Si todos los requisitos previos se cumplen, procede a la instalación del antivirus, del siguiente modo:

Si instalas desde el CD-ROM de Panda Antivirus Platinum

1. Introduce el CD-ROM de Panda Antivirus Platinum en la unidad lectora de CD-ROM del ordenador donde deseas instalarlo.
2. Automáticamente se ejecutará una aplicación que permitirá instalar el antivirus. Si tienes desactivada la opción de ejecución automática en tu ordenador, ejecuta el programa *CDMENU.EXE* que se encuentra en el CD-ROM.
3. Esto mostrará un menú con diferentes opciones. Selecciona la opción **Instalar Panda Antivirus Platinum**.
4. Si se detecta que Panda Antivirus Platinum ya está instalado, se mostrará un cuadro de diálogo, con las siguientes posibilidades:



Reparar. Esta opción permite restaurar la versión de Panda Antivirus Platinum que se encuentra

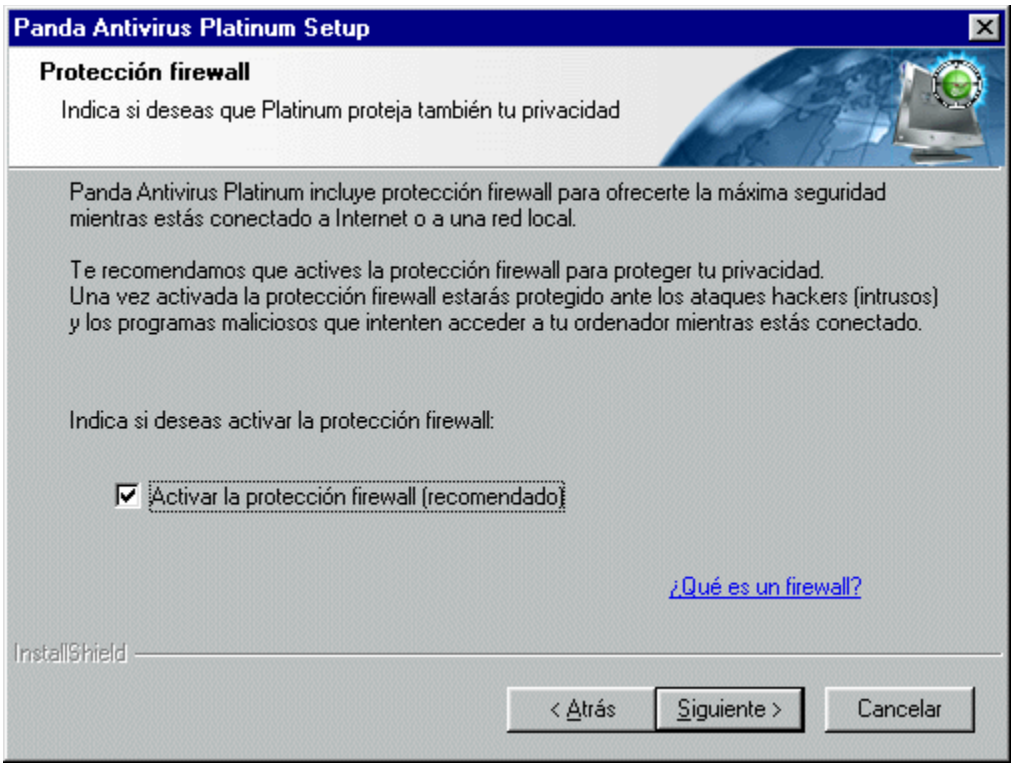
actualmente instalada. Al pulsar este botón, se realizarán las siguientes operaciones:

- Copia de los ficheros necesarios.
- Se pide confirmación para reiniciar el ordenador al finalizar la reparación. Selecciona una de las dos posibilidades (**Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**) y pulsa el botón **Finalizar**.

Eliminar. Esta opción desinstala o elimina Panda Antivirus Platinum. Al seleccionar esta posibilidad, se realizarán las siguientes operaciones:

- Se pide confirmación para eliminar la aplicación y todos sus componentes. El botón **Cancelar** permite detener el proceso, y el botón **Aceptar**, elimina el antivirus.
- Tras la desinstalación, se pide confirmación para reiniciar el ordenador. Selecciona una de las dos posibilidades (**Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**) y pulsa el botón **Finalizar**.

5. Si Panda Antivirus Platinum no está instalado, aparece una pantalla de bienvenida al proceso de instalación. En ella se recomienda cerrar todos los programas abiertos y desinstalar cualquier otro antivirus, antes de continuar. Hazlo y pulsa el botón **Siguiente**.
6. Se muestra el acuerdo de licencia. Acéptalo, pulsando el botón **Sí**, para continuar.
7. Puedes **Analizar la memoria durante la instalación** y/o **Analizar el disco duro durante la instalación**. Realiza la selección deseada y pulsa el botón **Siguiente**.
8. Sólo si en el paso anterior se indicó la realización de algún análisis, éste se llevará a cabo. Cuando finalice, pulsa el botón **Aceptar**.
9. Introduce tu **Nombre de usuario** y el **Nombre de organización** y pulsa el botón **Siguiente**.
10. El antivirus se instala, por defecto en un determinado directorio o carpeta. Para instalarlo en otro directorio, pulsa el botón **Examinar…** Después de indicar el directorio o carpeta de instalación alternativo, pulsa el botón **Siguiente** para continuar.
11. Puedes indicar si deseas activar el firewall incluido en Panda Antivirus Platinum. Para hacerlo, marca la casilla **Activar la protección firewall (recomendado)** y pulsa el botón **Siguiente**. Puedes obtener información sobre lo que es un firewall, pinchando sobre la opción **¿Qué es un firewall?**.



Puedes activar el firewall ahora (durante el proceso de instalación de tu Panda Antivirus Platinum), pero también lo puedes hacer después. En el segundo caso, podrás activarlo al acceder a la configuración de la protección permanente de firewall en la ventana del antivirus (seleccionando el menú **Protección permanente** en el Panel de control de la ventana del antivirus y después la opción **Configurar**, en el panel **Firewall**).

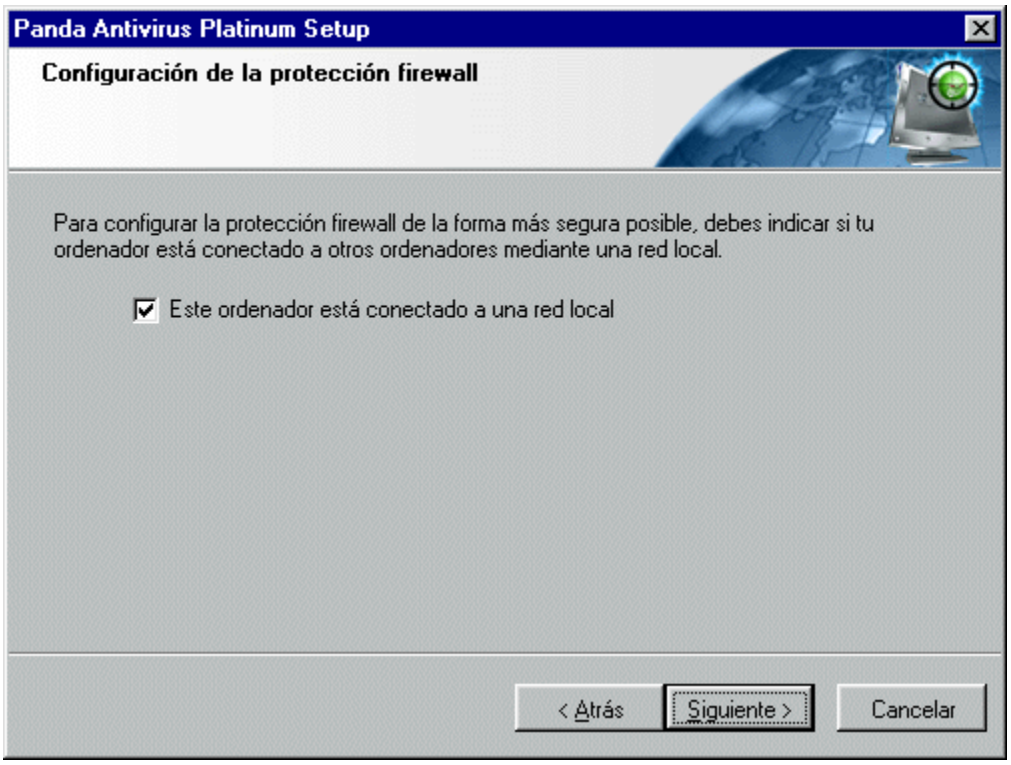
Si deseas ampliar información sobre la activación del firewall y su configuración, puedes consultar el apartado ¿Cómo Configurar el Firewall de Panda Antivirus Platinum?.

12. Sólo si en el paso anterior marcaste la casilla **Activar protección firewall (recomendado)** y si tu ordenador cuenta con una única conexión de red o con un único acceso telefónico, debes indicar si tu ordenador está conectado a una red de ordenadores. Si es así, marca la casilla **Este ordenador está contectado a una red local**.

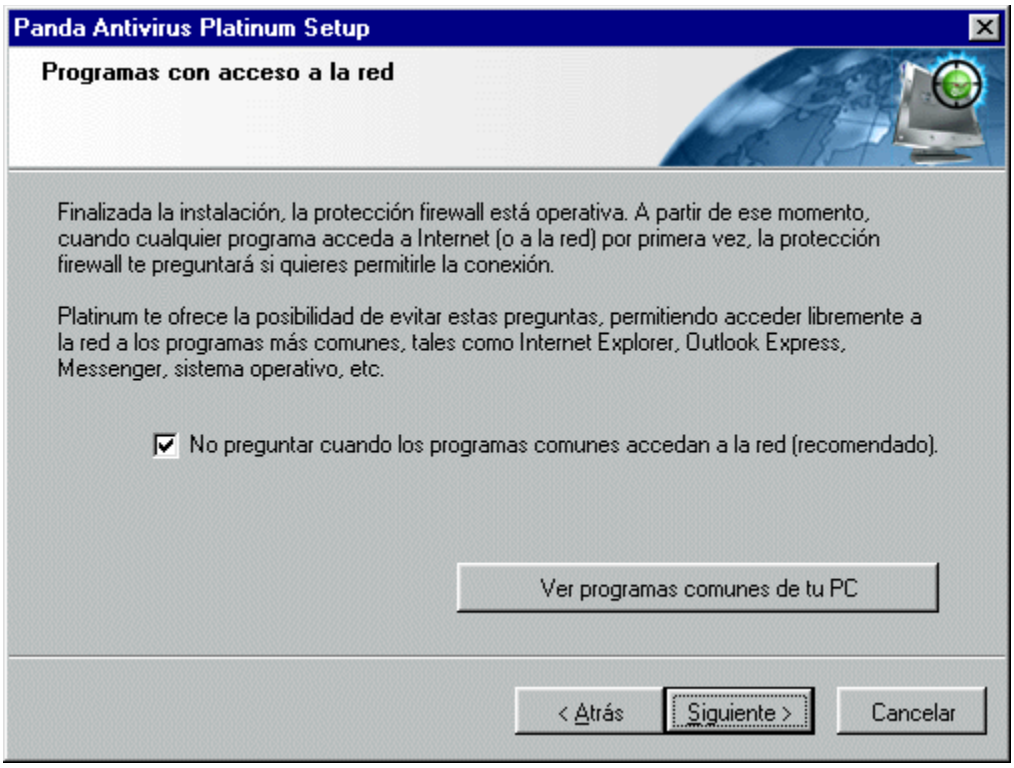
    Sólo en el caso de que tu ordenador tenga establecidas varias conexiones de red y/o varios accesos telefónicos, podrás seleccionar aquellos que se deben utilizar para compartir ficheros e impresoras en la red. Én tal caso, aparecerá una lista con todas las conexiones de red y/o los accesos telefónicas de tu ordenador. Selecciona los que estimes oportuno (no es recomendable marcar aquellos que permiten la conexión directa a Internet -MODEM, xDSL, etc-) marcando la casilla correspondiente.

    Nota: si el sistema operativo de tu ordenador es Windows NT 4.0, no aparecerá la lista de adaptadores de red. Las reglas avanzadas de seguridad no se aplicarán sobre un único adaptador, sino sobre todos los existentes. Por otra parte, las opciones de configuración de las carpetas compartidas (ficha **Seguridad**, en la configuración del firewall), no estarán activas.

    En cualquier caso, pulsa el botón **Siguiente**.



13. Si en los pasos anteriores activaste el firewall, podrás indicarle a Panda Antivirus Platinum que te avise siempre que un programa común acceda a la red. Si no deseas ser informado, marca la casilla **No preguntar cuando los programas comunes accedan a la red (recomendado)**. También puedes consultar la lista de los programas que son considerados como comunes en tu ordenador, pulsando el botón **Ver programas comunes de tu PC**. En cualquier caso, pulsa el botón **Siguiente**.



14. Comienza la copia de los ficheros del antivirus, al disco duro.
15. Al finalizar la copia de todos los ficheros, se podrá realizar el registro online (a través de Internet) como usuario de Panda Antivirus Platinum. Marca la opción que desees: **Sí, quiero registrarme ahora**, o **No, lo haré más tarde** y pulsa el botón **Siguiente**.
16. Sólo si en el paso anterior se seleccionó la opción **Sí, quiero registrarme ahora**, se accederá a la Web de Registro online de Panda Software. Introduce los datos que se solicitan en ella. También puedes realizarlo después de instalar el antivirus.
17. Sólo si en el paso correspondiente de esta instalación indicaste que se debía instalar o activar el firewall -si marcaste la casilla Activar protección firewall (recomendado)-, puedes seleccionar una de las siguientes opciones: **Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**. En cualquier caso, pulsa el botón **Finalizar**. Si marcaste la primera opción, el ordenador se reiniciará y actualizará el sistema para el correcto funcionamiento del antivirus.

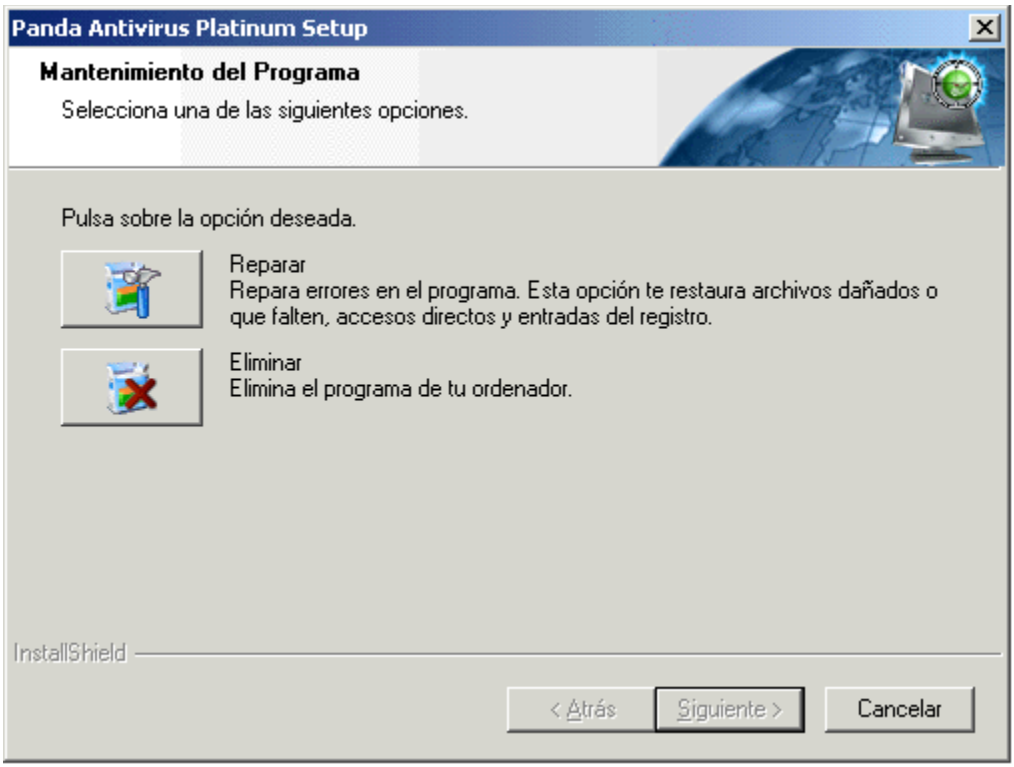
    Nota: recuerda que la protección permanente del firewall solamente entrará en funcionamiento si reinicias tu ordenador. Sin embargo, el antivirus y sus protecciones permanentes de archivos y de correo, funcionarán correctamente. La protección permanente del firewall, permanecerá inactiva hasta que reinicies tu ordenador.

18. Finalmente, podrás indicar si deseas **Abrir ahora Panda Antivirus Platinum**, o **Leer ahora los consejos sobre Panda Antivirus Platinum**. Si la primera casilla se encuentra marcada, la ventana del antivirus se abrirá cuando pulses el botón **Finalizar**. Si has marcado la segunda casilla, se mostrará una ventana con los consejos para mantenerte alejado de los virus, cuando pulses el botón **Finalizar**.

Si instalas mediante un fichero descargado de Internet

1. Ejecuta el fichero que has descargado de Internet, haciendo doble clic sobre él.

2. Si se detecta que Panda Antivirus Platinum ya está instalado, se mostrará un cuadro de diálogo, con las siguientes posibilidades:



Reparar. Esta opción permite actualizar y volver a configurar la versión de Panda Antivirus Platinum que se encuentra actualmente instalada. Si pulsas este botón, se realizarán las siguientes operaciones:

- Copia de los ficheros necesarios.
- Se pide confirmación para reiniciar el ordenador al finalizar la reparación. Selecciona una de las dos posibilidades (**Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**) y pulsa el botón **Finalizar**.

Eliminar. Esta opción desinstala o elimina Panda Antivirus Platinum. Si se elige esta posibilidad, se realizarán las siguientes operaciones:

- Se pide confirmación para eliminar la aplicación y todos sus componentes. Pulsa el botón **Cancelar** para detener el proceso, o el botón **Aceptar**, para eliminar el antivirus.
- Tras la desinstalación, se pide confirmación para reiniciar el ordenador. Selecciona una de las dos posibilidades (**Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**) y pulsa el botón **Finalizar**.

3. Si Panda Antivirus Platinum no está ya instalado, aparece una bienvenida al proceso de instalación. En ella se recomienda cerrar todos los programas abiertos y desinstalar cualquier otro antivirus, antes de continuar. Hazlo y pulsa el botón **Siguiente**.
4. Se muestra el acuerdo de licencia. Acéptalo, pulsando el botón **Sí**, para continuar.
5. Puedes **Analizar la memoria durante la instalación** y/o **Analizar el disco duro durante la instalación**. Realiza la selección deseada y pulsa el botón **Siguiente**.

6. Sólo si en el paso anterior se indicó la realización de algún análisis, éste se llevará a cabo. Cuando finalice, pulsa el botón **Aceptar**.
7. Introduce tu **Nombre de usuario** y el **Nombre de organización** y pulsa el botón **Siguiente**.
8. El antivirus se instala, por defecto en un determinado directorio o carpeta. Para instalarlo en otro directorio, pulsa el botón **Examinar…** Después de indicar el directorio o carpeta de instalación alternativo, pulsa el botón **Siguiente** para continuar.
9. Puedes indicar si deseas activar el firewall incluido en Panda Antivirus Platinum. Para hacerlo, marca la casilla **Activar la protección firewall (recomendado)** y pulsa el botón **Siguiente**. Puedes obtener información sobre lo que es un firewall, pinchando sobre la opción **¿Qué es un firewall?**.
10. Si en el paso anterior marcaste la casilla **Activar protección firewall (recomendado)**, y si tu ordenador cuenta con una única conexión de red o un único acceso telefónico, debes indicar si tu ordenador está conectado a una red de ordenadores. Si es así, marca la casilla **Este ordenador está contectado a una red local**. En cualquier caso, pulsa el botón **Siguiente**.

    Sólo en el caso de que tu ordenador tenga configuradas varias conexiones de red y/o varios accesos telefónicos, podrás seleccionar aquellas que se deben utiliza para compartir ficheros e impresoras en la red. En tal caso, aparecerá una lista con todas las conexiones de red y/o accesos telefónicos de tu ordenador. Selecciona los que estimes oportuno (no es recomendable marcar aquellos que permiten la conexión directa a Internet -MODEM, xDSL, etc-) marcando la casilla correspondiente.

    Nota: si el sistema operativo de tu ordenador es Windows NT 4.0, no aparecerá la lista de adaptadores de red. Las reglas avanzadas de seguridad no se aplicarán sobre un único adaptador, sino sobre todos los existentes. Por otra parte, las opciones de configuración de las carpetas compartidas (ficha **Seguridad**, en la configuración del firewall), no estarán activas.

11. Si en los pasos anteriores activaste el firewall, podrás indicar a Panda Antivirus Platinum que te avise siempre que un programa común acceda a la red. Si no deseas ser informado, marca la casilla **No preguntar cuando los programas comunes accedan a la red (recomendado)**. También puedes consultar la lista de los programas que son considerados como comunes en tu ordenador, pulsando el botón **Ver programas comunes de tu PC**. En cualquier caso, pulsa el botón **Siguiente**.
12. Comienza la copia de los ficheros del antivirus, al disco duro.
13. Al finalizar la copia de todos los ficheros, se podrá realizar el registro online (a través de Internet) como usuario de Panda Antivirus Platinum. Marca la opción que desees: **Sí, quiero registrarme ahora**, o **No, lo haré más tarde** y pulsa el botón **Siguiente**.
14. Sólo si en el paso anterior se seleccionó la opción **Sí, quiero registrarme ahora**, se accederá a la Web de Registro online de Panda Software. Introduce los datos que se solicitan en ella. También puedes realizarlo después de instalar el antivirus.
15. Sólo si en el paso correspondiente de esta instalación indicaste que se debía instalar o activar el firewall -si marcaste la casilla Activar protección firewall (recomendado)-, puedes seleccionar una de las siguientes opciones: **Sí, deseo reiniciar el equipo ahora**, o **No, reiniciaré el equipo más tarde**. En cualquier caso, pulsa el botón **Finalizar**. Si marcaste la primera opción, el ordenador se reiniciará y actualizará el sistema para el correcto funcionamiento del antivirus.

    Aviso: recuerda que la protección permanente del firewall solamente entrará en funcionamiento si reinicias tu ordenador. Sin embargo, el antivirus y sus protecciones permanentes de archivos y de correo, funcionarán correctamente. La protección permanente del firewall, permanecerá inactiva hasta que reinicies tu ordenador.

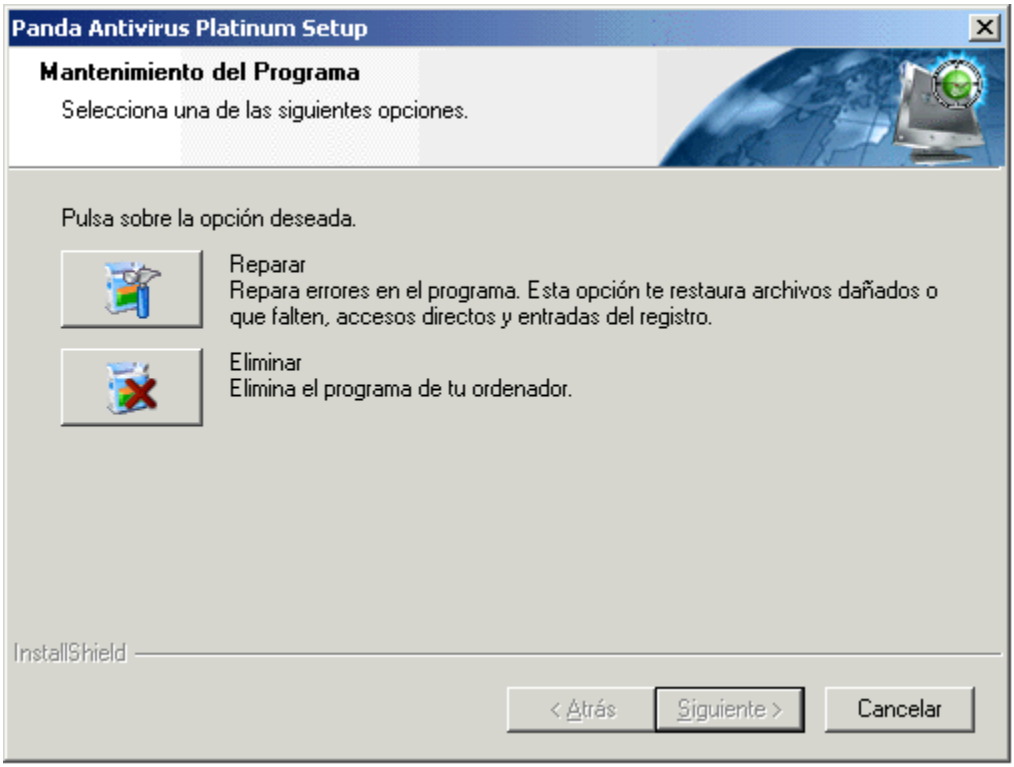
Nota: si durante el proceso de instalación de tu Panda Antivirus Platinum, no indicaste que debía instalarse / activarse el firewall, también podrás hacerlo después, tanto desde la opción de configuración de la protección permanente de firewall, como desde el botón **Inicio** de Windows. En el segundo caso, pulsa el botón **Inicio**, selecciona el grupo **Programas**, selecciona **Panda Antivirus Platinum** y pulsa sobre la opción **Desinstalar - Reparar**. Esto muestra un cuadro de diálogo en el que debes pulsar el botón **Reparar**. Si aun no has instalado el firewall, podrás hacerlo en este momento.

Desinstalación de Panda Antivirus Platinum

La desinstalación de Panda Antivirus Platinum, puede realizarse de diferentes formas, aunque todas ellas realizan las mismas operaciones (borran los ficheros del antivirus, eliminan las entradas del *Registro de Windows*,… etc.).

Desinstalación desde el grupo de programas del antivirus

1. Cierra los programas de correo que tengas abiertos.
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**.

Desinstalación desde el *Panel de Control de Windows*

1. Cierra los programas de correo que tengas abiertos.
2. Pulsa el botón **Inicio** de Windows.

3. Selecciona la opción **Configuración**.
4. Accede al grupo de programas **Panel de control**.
5. Con el ratón, haz doble clic sobre el icono **Agregar o quitar programas**.
6. Selecciona **Panda Antivirus Platinum**.
7. Pulsa el botón **Agregar / Quitar**.
8. Se eliminarán todos los ficheros.

Ejecución de Panda Antivirus Platinum

Una vez instalado el antivirus, éste puede ejecutarse (se puede abrir la ventana del antivirus -esto no significa que se realice o comience ningún análisis en ese instante-), de varias formas:

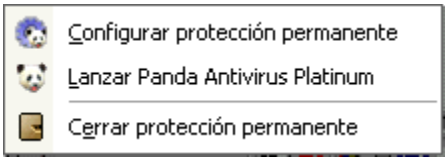
Desde en botón Inicio de Windows

1. Pulsa el botón **Inicio** de Windows.
2. Selecciona **Programas**.
3. Accede al grupo de programas **Panda Antivirus Platinum**.
4. Selecciona la opción **Panda Antivirus Platinum**.
5. Se abre la ventana del antivirus.

Desde el icono de protección permanente

Si el antivirus tiene activa la protección permanente (inmediatamente después de haberlo instalado, estará activa), aparecerá el icono de Panda Antivirus Platinum en la *Barra de tareas* -junto al reloj del sistema-. Desde él es posible realizar varias operaciones: **Configurar protección permanente** (determinar el funcionamiento de la protección permanente de archivos y correo), **Lanzar Panda Antivirus Platinum** (abre la ventana del antivirus) y **Cerrar protección permanente** (desactiva la protección permanente).

1. Si la protección permanente se encunetra cargada, aparece el icono de Panda Antivirus Platinum junto al reloj del sistema, en la *Barra de tareas de Windows*. Pulsa sobre él con el botón derecho del ratón. Esto abrirá un menú contextual con varias opciones.



2. Pincha sobre la opción **Lanzar Panda Antivirus Platinum**.
3. Se abre la ventana del antivirus.

Desde la *Barra de acceso rápido* (*Quick Launch*)

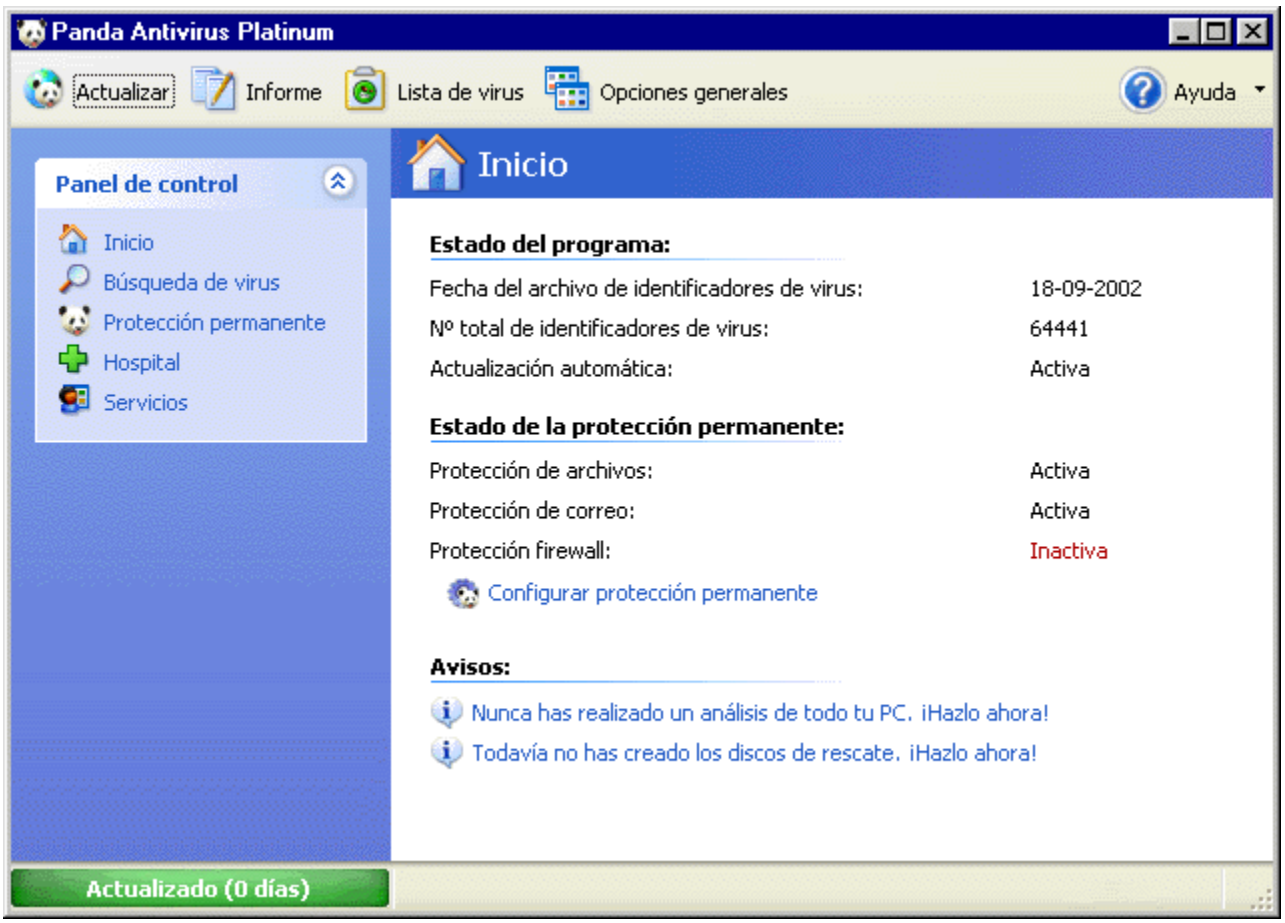
Cuando se instala el antivirus, éste crea un icono de acceso para la ejecución instantánea del antivirus desde la barra de acceso rápido o *Quick Launch* de Windows (si esta existe). En ella se muestra el icono de Panda Antivirus Platinum. Pulsando sobre él, se abre la ventana del antivirus.

Para obtener más información sobre la ventana inicial de Panda Antivirus Platinum, cómo trabajar con ella y las opciones accesibles desde ésta, se puede consultar el apartado Ventana Principal del Antivirus, de esta ayuda.

Ventana Principal del Antivirus

En la sección Ejecución de Panda Antivirus Platinum, de esta ayuda se pueden consultar las diferentes formas de abrir la ventana del antivirus. La ventana principal del antivirus se abre siempre en una determinada sección: sección de **Inicio**. Desde ella se nos informa sobre el estado actual del programa, de la protección permanente y se nos pueden presentar determinados avisos de interés.

Veamos cada una de las secciones de dicha ventana, que seguirán la misma forma de trabajo en el resto de las restantes secciones (**Búsqueda de virus**, **Protección permanente**, **Hospital** y **Servicios**).



Barra de herramientas o barra de botones
Se encuentra justo debajo de la *Barra de título* y contiene varios botones:

Actualizar. Se accede a un asistente que nos permite indicar cómo se debe actualizar tu Panda Antivirus Platinum. Desde él se podrá actualizar el antivirus. Puede obtenerse más información, consultando el apartado Actualización de Panda Antivirus Platinum, de esta ayuda.

Informe. Se muestra un informe en el que aparece todo lo sucedido durante los análisis realizados (siempre que no se haya borrado previamente el contenido de dicho informe). Puede obtenerse más información, consultando el apartado El Informe de los Análisis de esta ayuda.

 **Lista de virus.** Se muestra la lista con todos los virus que detecta el antivirus, así como las características de cada uno de ellos. Para obtener más información sobre el funcionamiento de ésta, se aconseja la consulta del apartado La Lista de Virus (Informaciones) de esta ayuda. Además, es posible obtener información más amplia sobre un determinado virus, en la Enciclopedia de Virus de Panda Software.

 **Opciones generales.** Se muestra un cuadro de diálogo con varias fichas: **General**, **Perfil de Correo**, **Actualización**, **Sonidos** y **Restricciones**. Cada una de ellas, contiene las opciones correspondientes para definir la configuración específica del antivirus, cada uno de esos casos. Para obtener más información sobre cada una de las fichas, se aconseja la consulta del apartado Configuración General del Antivirus de esta ayuda.

 **Ayuda.** Al pulsar sobre este botón, se abre una lista desplegable con varias opciones: **Registro online** (permite que te registres como usuario de Panda Antivirus Platinum y puedas acceder a los servicios que lo acompañan), **Contenido** (acceso a esta ayuda que estás consultando – también puedes pulsar la tecla de función F1), **¿Qué es esto?** (selecciona esta opción y pulsa sobre una sección de la ventana, para obtener información sobre ella), **Panda en la Web** (accesos directos a diferentes secciones en la Web de Panda Software), **Preguntas más frecuentes (FAQs)** (muestra las respuestas a la preguntas que se nos plantean más frecuentemente), **Novedades de Panda Antivirus** (accede a información sobre las nuievas características de Panda Antivirus), **Consejos** (se muestran 15 consejos que Panda Software sugiere para mantenerse alejado de los virus) y **Acerca de Panda Antivirus** (se muestra información sobre la versión del antivirus).

Panel de control

Se encuentra a la izquierda de la ventana. Por defecto (al abrir la ventana del antivirus), muestra un recuadro (panel) con varias opciones o tareas que se pueden realizar con Panda Antivirus Platinum.

Dependiendo de la sección en la que nos encontremos (**Inicio**, **Búsqueda de virus**, **Protección permanente**, **Hospital**, o **Servicios**), podrán aparecer paneles adicionales de opciones justo debajo del Panel de control inicial. Todos ellos, incluido el propio Panel de control inicial, son plegables-desplegables. Esto quiere decir que si pulsamos sobre las flechas que aparecen en el vértice superior derecho de los mismos o sobre sus títulos, se desplegarán (mostrando las opciones) y se plegarán (mostrando únicamente su título), según corresponda.

 **Inicio.** Seleccionando esta opción en el Panel de control (aparece seleccionada por defecto cuando se abre la ventana del antivirus), podrán consultarse datos de interés sobre las características del antivirus y de la protección permanente (**Antivirus**: de archivos y de correo y **Firewall**). Además podrán mostrarse avisos o sugerencias de interés que el propio Panda Antivirus Platinum nos hará personalmente.

La sección **Inicio**, no contiene ningún panel de opciones adicional. Se puede obtener más información, consultando el apartado Estado Actual del Antivirus, de esta ayuda.

 **Búsqueda de virus.** Desde esta sección, se podrá realizar cualquier tipo de análisis, seleccionando los elementos a analizar e indicando cómo y cuándo deben ser analizados.

Los diferentes tipos de análisis muestran un panel adicional denominado **Tareas de análisis**. Desde él es posible **Analizar**, **Configurar**, **Crear nuevo análisis**, **Editar análisis** y **Eliminar análisis** los análisis existentes. Si deseas obtener más información, consulta el apartado Tipos de Análisis, de esta ayuda.

Protección permanente. Permite consultar el estado actual de la Protección permanente o análisis permanente (de archivos y de correo electrónico) y de la protección del firewall. Del mismo modo, es posible determinar las características de los mismos y activarlos o desactivar dichas protecciones (Antivirus y Firewall).

Al situarnos en la sección de **Protección permanente**, se muestran dos paneles adicionales denominados **Antivirus** y **Firewall**. Desde ambos, es posible **Configurar**, **Activar** y **Desactivar** la Protección permanente (residente) sobre el correo electrónico y los archivos, así como la protección del firewall. Puedes ampliar esta información, consultando el apartado Análisis Permanente o Protección Permanentes Antivirus (Archivos y Correo) y Firewall, de esta ayuda.

Hospital. Ten un control absoluto sobre todos aquellos ficheros sospechosos de estar infectados por un virus. Podrás mantenerlos en Cuarentena para evitar infecciones y contagios de otros ficheros, enviarlos a Panda Software para que sean analizados, o restaurarlos en su lugar original.

Al situarnos en la sección **Hospital**, se muestra un panel central con los elementos incluidos en el Hospital. A través de él, es posible realizar cualquier operación con todos aquellos elementos (ficheros), que se encuentran en **Cuarentena**. Trabajaremos, por lo tanto, con los ficheros sospechosos que se han colocado (automática o manualmente) en cuarentena: **Enviar a Panda**, **Desinfectar y restaurar**, **Eliminar archivo**, **Añadir archivo** a la cuarentena y obtener **Ayuda sobre hospital**. Si deseas obtener más información sobre la cuarentena, consulta el apartado Hospital - Cuarentena, de esta ayuda.

Si deseas obtener más información, puedes consultar el apartado ¿Qué es el Hospital?, en esta ayuda.

Servicios. Mediante esta sección podrás acceder un grupo de los mejores servicios ofertados por Panda Software, que se incluyen junto con Panda Antivirus Platinum. No olvides que para poder utilizar todos los servicios que incluye el antivirus, debes registrarte previamente como usuario de Panda Software.

La sección **Servicios**, no contienen ningún panel de opciones adicional. Puedes obtener más información, consultando el apartado ¿Qué Servicios Incluye Panda Antivirus Platinum?, de esta ayuda.

Cuerpo central o sección central de contenidos y operaciones

Es la sección principal en la que se muestra todo el contenido, elementos y opciones accesibles desde cualquiera de las opciones del **Panel de control** (u otros paneles) en la que nos hayamos colocado.

Barra de estado y de actualización

Se encuentra en la parte inferior de la ventana -justo debajo del **Panel de control**-. En ella se podrá apreciar lo actualizado o desactualizado que está el antivirus. Mediante una barra de progreso, veremos una sección verde que indica lo actualizado que está el antivirus. En caso contrario, dicha barra será roja. Además en determinadas ocasiones se indicará, mediante una frase en la barra de esta, alguna de las operaciones que esté llevando acabo Panda Antivirus Platinum.

Operaciones Desde la Barra de Tareas de Windows


Siempre que se encuentre cargada la protección permanente del antivirus (protección permanente Antivirus: de archivos y de correo, así como la protección permanente del fFirewall), se mostrará el icono correspondiente de Panda Antivirus Platinum en la *Barra de estado de Windows* (junto al reloj del sistema). A través de dicho icono (el que se muestra al comienzo de este párrafo) es posible realizar varias operaciones.

Si se pulsa con el botón derecho del ratón sobre dicho icono, aparece un menú contextual con las siguientes opciones:

- **Configurar protección permanente.** Permite indicar las características que debe cumplir el análisis o protección permanente (Antivirus: de archivos y de correo, así como de Firewall). También es posible activar o desactivar cada una de estas protecciones. Si se desactivan ambas protecciones permanentes, el icono de la *Barra de tareas* aparecerá en color gris. También es posible acceder a la configuración pinchando una vez con el botón izquierdo del ratón o haciendo doble clic sobre él. Si deseas obtener información más ampliada, consulta el apartado Análisis Permanente o Protección Permanente Antivirus (Archivos y Correo) y de Firewall de esta ayuda.
- **Lanzar Panda Antivirus Platinum.** Abre la ventana de Panda Antivirus Platinum. Esto no implica que se ponga en marcha ningún análisis en ese momento.
- **Cerrar protección permanente.** Se nos pide confirmación para cerrar o finalizar (desactivar) la protección permanente (Antivirus: de archivos y de correo, así como de Firewall). Si pulsamos el botón **Si**, ésta se desactivará inmediatamente y el icono correspondiente desaparecerá de la *Barra de tareas de Windows*. Puede volver a activarse desde la opción **Protección permanente**, existente en la ventana del antivirus (entonces se volverá a mostrar el icono en la *Barra de tareas de Windows*). Si deseas más información sobre este tema, consulta el apartado Análisis Permanente o Protección Permanente Antivirus (Archivos y Correo) y de Firewall de esta ayuda.

Menús Contextuales

Para trabajar en la ventana de Panda Antivirus Platinum, además de utilizar las opciones de menú y botones de la barra de herramientas, es posible trabajar mediante los denominados menús contextuales. Para ello sólo es necesario pulsar con el botón derecho del ratón en cualquiera de los elementos o secciones de la ventana principal. Estos menús se encuentran disponibles en las siguientes secciones: **Búsqueda de virus** y **Hospital**.

Puedes obtener más información sobre este tipo de menús contextuales, en los siguientes apartados de esta ayuda:

Menú contextual en la Búsqueda de virus
Menú contextual en el Hospital

Por otra parte, desde el *Explorador de Archivos de Windows*, también es posible realizar análisis mediante el menú contextual. Para hacerlo solamente hay que seguir estos pasos:

1. Seleccionar un grupo de elementos (ficheros, directorios, unidades de disco,…) que se desean analizar.
2. Pulsar sobre ellos con el botón derecho del ratón.
3. Seleccionar la opción **Analizar con antivirus Platinum**.

Esto da comienzo al análisis de los elementos seleccionados. Cuando éste finaliza, se muestra el resultado del mismo. Desde este cuadro de diálogo, es posible consultar el **Informe** del antivirus, o cerrar el cuadro de diálogo pulsando el botón **Aceptar**.

Menú Contextual en los Análisis

Si nos hemos posicionado en la sección **Análisis exhaustivo** del **Panel de control**, podremos realizar cualquier tipo de análisis, crear análisis (o tareas de análisis) nuevos, modificar los ya existentes,… etc. Todas estas operaciones se pueden realizar mediante las opciones existentes en los paneles correspondientes. Del mismo modo, es posible realizarlas mediante las opciones de los diferentes menús contextuales (éstos son distintos dependiendo de la sección en la que pinchemos).

Menú contextual sobre los tipos de análisis

Dentro de la sección de análisis, existen tres grandes grupos: **Análisis Inmediatos**, **Analizar otros elementos** (dentro de los análisis inmediatos) y **Análisis Programados**. Si pulsamos con el botón derecho del ratón sobre cualquiera de estos títulos, aparecerá la opción **Nuevo análisis**. Pulsando sobre ella, se nos permite crear una nueva tarea de análisis. Si deseas obtener más información, consulta el apartado ¿Cómo Crear un Nuevo Análisis? (Inmediato / Programado), de esta ayuda.

Menú contextual sobre análisis predefinidos (inmediatos / programados) y sobre elementos a analizar

En primer lugar, hay que comentar que los "análisis predefinidos o predeterminados" son aquellos análisis que vienen definidos (ya creados) por defecto en el antivirus (**Analizar todo el sistema**, **Analizar discos duros**,…). Tanto los análisis inmediatos predefinidos (los que ya existen o aparecen por defecto), los elementos seleccionables en la opción sección **Analizar otros elementos**, como los análisis programados predefinidos cuentan con un menú contextual similar (con las mismas opciones). Si pulsamos con el botón derecho del ratón sobre cualquiera de los análisis inmediatos o programados que existen por defecto (predefinidos), o sobre los elementos de la sección **Analizar otros elementos**, aparecen las siguientes opciones:

- **Analizar.** En ese mismo instante, se realiza un análisis del elemento seleccionado.
- **Configurar.** Esta opción sólo está disponible en el caso de los análisis inmedialtos (no programados) predefinidos. Permite indicar las características que debería tener el análisis inmediato sobre el elemento que se encuentre seleccionado.
- **Editar análisis.** Esta opción sólo está disponible en el caso de los análisis programados (no inmediatos) predefinidos. Permite indicar las características que debería tener el la tarea de análisis programado (y su planificación o programación) sobre el elemento que se encuentre seleccionado.
- **Nuevo análisis.** Permite crear un nuevo análisis, sobre cualquier elemento

Menú contextual sobre los nuevos análisis, creados por el usuario

Desde la sección de **Análisis exhaustivo** es posible crear nuevas tareas de análisis, tanto inmediatas como programadas, así como configurar y eliminar las que ya existen.

Nota: solamente se pueden borrar las nuevas tareas que hayan sido creadas por el usuario, no las definidas por defecto -o predeterminadas- en el programa. Es imposible eliminar los análisis inmediatos predefinidos: **Analizar todo el sistema**, **Analizar discos duros**, **Analizar todo el correo electrónico**, **Analizar disquetera**, o **Analizar otros elementos**). Del mismo modo, tampoco es posible eliminar los análisis programados predefinidos: **Análisis al inicio del sistema** y **Análisis al inicio de Windows**.

Si se pulsa con el botón derecho del ratón sobre este tipo de análisis (los que hayan ido creando los

usuarios), aparecen las siguientes opciones:

- **Analizar.** En ese mismo instante, se pone en marcha la tarea de análisis seleccionada.
- **Editar análisis.** Permite indicar las características que debería tener la tarea de análisis sobre la que se haya pulsado. Se trata de la configuración del análisis.
- **Eliminar análisis.** Permite eliminar la tarea de análisis seleccionada. Como ya hemos comentado, esta opción no aparecerá en el menú contextual correspondiente a los análisis predefinidos por defecto, ya que éstos no se pueden borrar.
- **Nuevo análisis.** Permite crear una nueva tarea de análisis (inmediata y programada).

Si deseas obtener más información sobre la creación de tareas de análisis (inmediatas y programadas, predefinidas o no), consulta el apartado Tipos de Análisis, de esta ayuda.

Menú Contextual en el Hospital

Si nos hemos posicionado en la sección **Hospital** del **Panel de control**, podremos realizar cualquier operación sobre todos aquellos ficheros que consideremos sospechosos: ponerlos en cuarentena, analizarlos, enviarlos a Panda Software para su análisis, restaurarlos en su ubicación original, eliminarlos,… etc.

Todas estas operaciones se pueden realizar mediante las opciones existentes en los paneles correspondientes. Del mismo modo, es posible realizarlas mediante las opciones de los diferentes menús contextuales (éstos son distintos dependiendo de la sección en la que pinchemos).

Pulsando sobre el panel derecho o principal de la sección **Hospital** (el que se muestran el listado de los ficheros) con el botón derecho del ratón, se muestra el menú contextual correspondiente.

Menú contextual sobre los ficheros en Cuarentena

Cualquiera de los ficheros que existan en un directorio de una unidad de disco, se puede poner en cuarentena (manual, o automáticamente por el antivirus). Esto significa que desaparece de su ubicación original y pasa a formar parte del grupo de ficheros que mantenemos en cuarentena (aislados de los demás).

Si se trata de un fichero sospechoso (posiblemente infectado), evitaremos utilizarlo y lo mantendremos aislado de los demás (para obtener más información sobre los ficheros en cuarentena, consulta el apartado Hospital – Cuarentena, de esta ayuda). Pues bien, cuando exista algún fichero en cuarentena, es posible realizar determinadas acciones sobre ellos mediante el menú contextual. Éstas son las siguientes:

- **Desinfectar y restaurar.** Chequea los ficheros seleccionados en busca de virus (los analiza) y los desinfecta si estaban infectados. Puede realizarse la misma operación, mediante la tecla de función *F8*. Si el fichero no contiene virus o ha sido desinfectado, podrá ser restaurado en su ubicación (directorio o carpeta) original. Para ello, se mostrará un cuadro de diálogo donde se debe confirmar esta operación. Si se contesta afirmativamente, el fichero seleccionado, dejará de estar en cuarentena. Es decir, se saca de ella (se le da el "alta") y pasa al directorio en el que estaba originalmente (antes de incluirlo en la Cuarentena). Esta acción también se puede realizar a través de la opción **Desinfectar y restaurar**, en el panel **Cuarentena**.
- **Actualizar.** Refresca o muestra la información actual de cada uno de los ficheros en la lista. Es posible realizar la misma operación, mediante la tecla de función *F5*. Esta opción solamente se muestra en el menú contextual, pero no en el panel **Cuarentena**.
- **Mostrar información.** Muestra datos de carácter adicional sobre el fichero seleccionado en la cuarentena. Esta opción sólo aparece en el menú contextual. Esta opción solamente se muestra en el menú contextual, pero no en el panel **Cuarentena**.
- **Eliminar.** El fichero seleccionado es borrado definitivamente y no se puede recuperar. Se borra de la Cuarentena y del directorio en el que se encontraba originalmente. Esta acción también se puede realizar a través de la opción **Eliminar archivo**, en el panel **Cuarentena**.
- **Enviar.** Permite el envío del fichero que se encuentra seleccionado en la Cuarentena al Laboratorio de Virus de Panda Software. Allí será investigado y estudiado por nuestros expertos antivirus, para encontrar la solución los problemas que dicho fichero esté causando. Solamente podrás realizar el envío de los ficheros en cuarentena, cuando el antivirus se encuentre correctamente actualizado. En ese mismo instante serán analizados. Tanto si están infectados, como si no lo están, podrás enviarlos a Panda Software, para su estudio. Esta acción también se

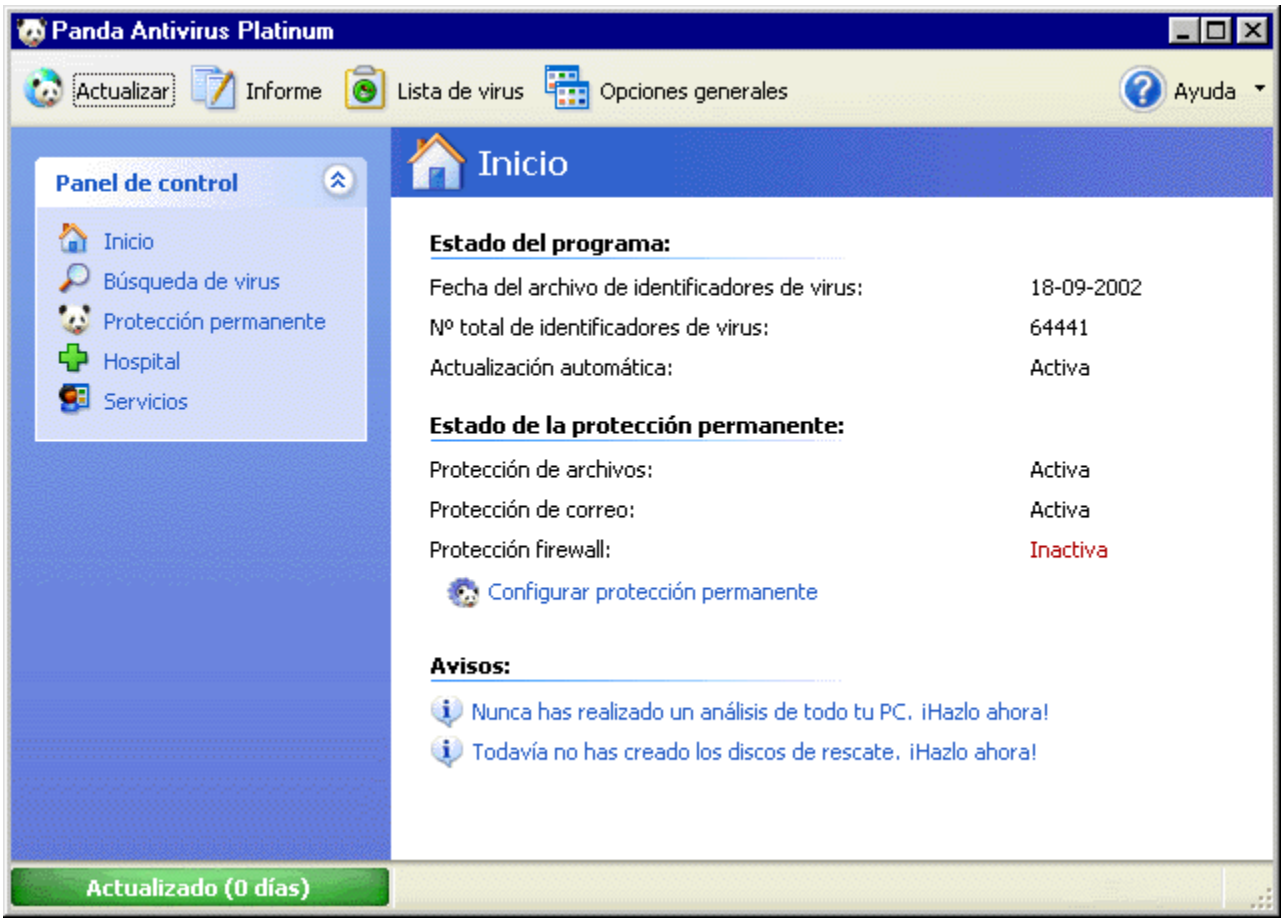
puede realizar a través de la opción **Enviar a Panda**, en el panel **Cuarentena**.

Si deseas consultar más información sobre cada una de las acciones que se pueden realizar sobre los ficheros de la cuarentena, consulta el apartado Acciones Sobre los Ficheros en Cuarentena, de esta ayuda.

Estado Actual del Antivirus

Cuando se abre la ventana de Panda Antivirus Platinum, ésta muestra inicialmente la sección **Inicio**. Si ya está abierta la ventana, pero nos encontramos en otra sección de la misma (**Búsqueda de virus**, **Protección permanente**,…etc.), podemos consultar el estado del antivirus, seleccionando la opción **Inicio**, en el panel izquierdo (**Panel de control**).

En dicha sección se muestran las características más importantes, correspondientes al estado actual del programa antivirus y de la protección permanente (Antivirus: archivos y correo electrónico, así como de Firewall) de éste. Además, en ocasiones, se nos indican determinados avisos o sugerencias de interés.



El estado del antivirus se define en dos secciones del panel central:

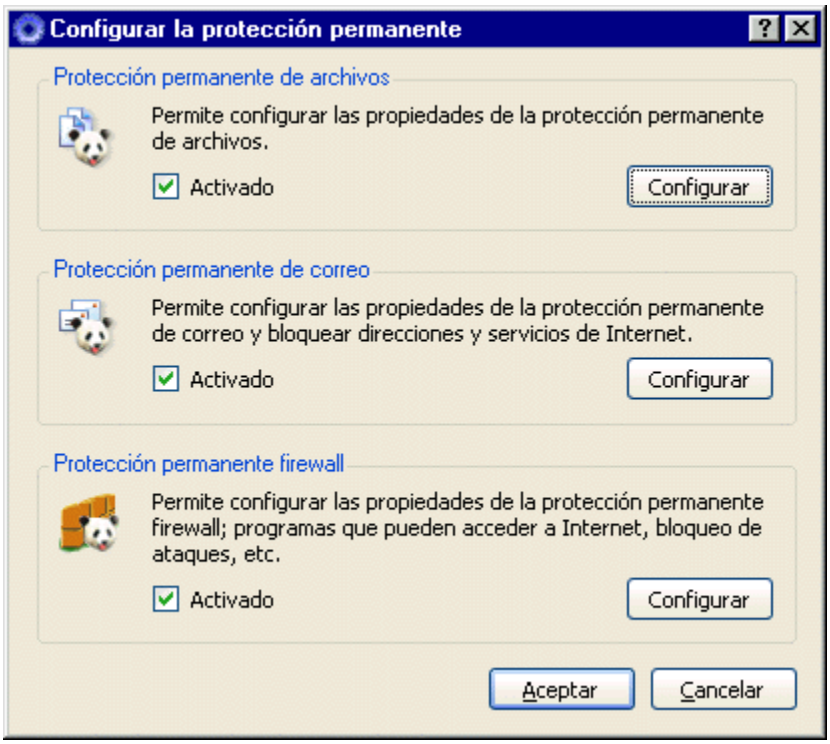
Estado del programa
A través de esta sección, se nos informa sobre la situación actual de Panda Antivirus Platinum. Los datos que en ella se muestran, son los siguientes:

- **Fecha del archivo de identificadores de virus:** este es el fichero que permite realizar las detecciones de virus. Es conveniente mantener este archivo actualizado para detectar los virus, de reciente aparición. La fecha que se muestra en esta sección indica el día en el que se actualizó por última vez dicho fichero.

- **Nº total de identificadores de virus:** muestra el número de virus que se pueden detectar (y por lo tanto desinfectar), con la versión actual del archivo de identificadores de virus. Además, el numero de éstos que Panda Antivirus Platinum es capaz de aniquilar, aumenta a diario (por este motivo es conveniente realizar actualizaciones diarias, ya sean automáticas o manuales).
- **Actualización automática:** el antivirus se encargará de poner al día el archivo de identificadores de virus y al propio programa antivirus, cuando detecte una conexión abierta a Internet. Tú mismo decides el momento en el que debe realizarse una actualización, pero también puedes confiar dicha responsabilidad a Panda Antivirus Platinum, mediante la **Actualización automática**. Esta sección indica si dicho tipo de actualización se encuentra activada o desactivada.

Estado de la protección permanente

En esta sección se indicará si la protección permanente (tanto la de ficheros, como la de correo electrónico y la de firewall) se encuentra Activa o Inactiva. Si deseas modificar su estado (activarla o desactivarla y/o determinar sus características), pulsa sobre la opción **Configurar protección permanente**. Entonces, se muestra el siguiente cuadro de diálogo. Si deseas obtener más información sobre la configuración de la protección permanente, consulta el apartado Análisis Permanente o Protección Permanente Antivirus (Archivos y Correo) y Firewall, de esta ayuda.



Mediante este cuadro de diálogo es posible indicar si cada una de las protecciones permanentes (*Protección permanente de archivos*, *Protección permanente de correo* y *Protección permanente firewall*) debe estar **Activada** o **Desactivada**. Además, en cualquiera de estos casos, es posible **Configurar** dichas protecciones, indicando las propiedades, o características que debe cumplir cada una de estas protecciones permanentes (residentes). Si deseas obtener más información sobre la configuración de la protección permanente, consulta el apartado Análisis Permanente o Protección Permanente Antivirus (Archivos y Correo) y Firewall, de esta ayuda.

Avisos

Cuando sea conveniente, esta sección mostrará notas sugiriendo que se realice alguna operación

concreta. Pulsando sobre ellas, podrás realizar dichas acciones en ese mismo instante. Por ejemplo, si aún no has realizado un análisis sobre todos los elementos de tu ordenador, se mostrará el aviso correspondiente (***Nunca has realizado un análisis de todo tu PC***), o si aun no has creado los discos de rescate (***Todavía no has creado los discos de rescate. ¡Hazlo ahora!***). A través de esta sección también se te indicará el tiempo que ha transcurrido desde la última vez que se actualizó el antivirus, hasta la fecha actual.

Finalmente, en la sección inferior izquierda de la ventana de Panda Antivirus Platinum (en la barra de estado -justo debajo del panel de opciones izquierdo, o **Panel de control**-), se muestra una barra de progreso. Dicha barra aparecerá siempre, estemos en la sección que estemos (**Inicio**, **Búsqueda de virus**, **Protección permanente**, **Hospital**, o **Servicios**). Su significado es mostrar el grado de actualización con el que cuenta tu Panda Antivirus Platinum. Cuando el antivirus está completamente actualizado, dicha barra aparecerá en verde. En caso contrario, aparecerá en rojo. Si pulsas sobre ella, aparecerá un cuadro de diálgo a través del cual se te informa sobre el estado de actualización de tu Panda Antivirus Platinum.

Análisis Permanente o Protección Permanente Antivirus (Archivos y Correo) y Firewall

Con tu Panda Antivirus Platinum puedes realizar análisis inmediatos o programados (éstos pueden ser predefinidos, haber sido creados por los usuarios, o análisis de elementos independientes-). Además, Panda Antivirus Platinum te protege en todo momento de los virus que puedan existir o llegar a través de:

- Archivos (protección permanente de archivos).
- Correo electrónico (protección permanente de correo -Microsoft Outlook Express y Microsoft Exchange/Outlook, por ejemplo-).
- Firewall (protección permanente de los accesos de ciertos programas a Internet, bloqueos, ataques de programas o usuarios, etc).

Así, tanto los ficheros con los que se trabaja y los que llegan a través de cualquier puerto de comunicaciones (punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa), como los mensajes y ficheros que se transmiten a través de correo electrónico, y los accesos a través del firewall estarán continuamente analizándose.

Para que esto sea posible basta con tener activa la protección permanente (Antivirus -de archivos y de correo- y Firewall) y configurarla debidamente (además de tener correctamente actualizado su Panda Antivirus Platinum). Dichas protecciones consisten en el análisis continuo de TODOS los ficheros que intervienen en cualquier operación que realizamos.

Este tipo de análisis o protección se denomina **Protección Permanente** (también conocido como análisis residente) y se aplica a los archivos, a los mensajes de correo electrónico y a los accesos o transferencias de información a través del firewall. Por lo tanto, existirá protección permanente para correo electrónico, archivos y accesos o transferencias de información. Dichas protecciones permanentes tienen como misión supervisar todas las operaciones que se ejecuten en el ordenador en busca de virus o accesos no autorizados. De esta manera, cada vez que se intente ejecutar, copiar, etc, un fichero o acceder, enviar, mensajes, el permanente correspondiente lo analizará para determinar que esté libre de virus y desinfectarlo en caso de infección.

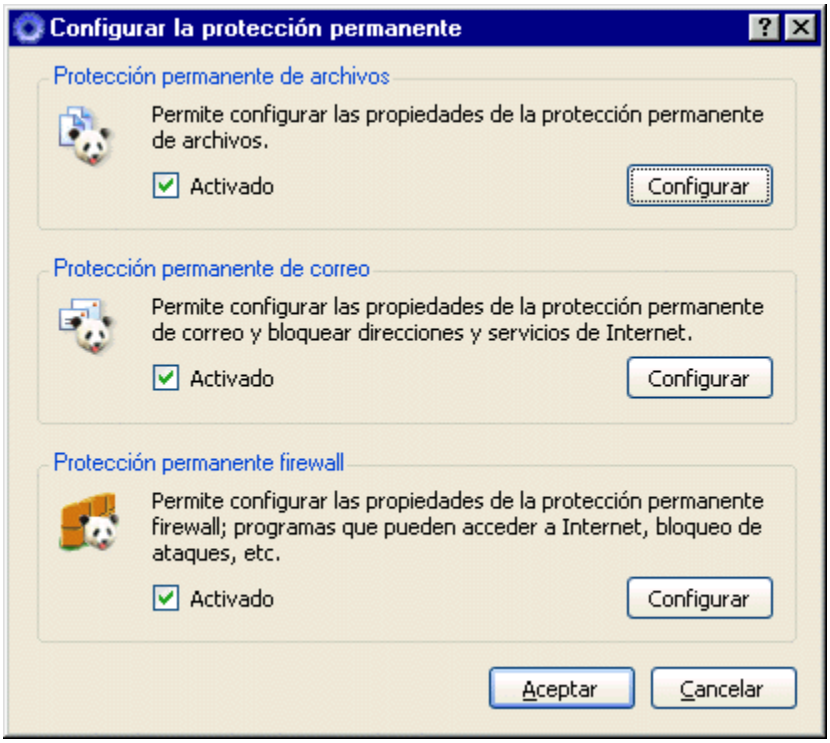
Por tanto, el permanente de Antivirus (archivos y correo) / Firewall se encarga de ofrecer una protección continua (siempre que esté activa y el antivirus está correctamente actualizado) en todo lo que se refiere a la manipulación de archivos, mensajes y accesos. En esto se incluye cualquier copia de ficheros desde o hacia un ordenador conectado en red, a Internet, …etc.

Aunque este tipo de análisis se encuentra continuamente chequeando el estado de los archivos, mensajes y de los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa), afecta mínimamente al rendimiento del sistema y ofrece los mayores niveles de protección (siempre y cuando esté activo y el antivirus se encuentre correctamente actualizado). Por consiguiente, siempre es recomendable tenerlo activado. Una vez que se haya activado y hasta su desactivación, la protección permanente de archivos, la de correo y la de firewall se pondrá en marcha cada vez que se arranque el ordenador.

En la *Barra de tareas de Windows* (junto al reloj del sistema), se podrá observar el icono representativo de Panda Antivirus Platinum. Esto quiere decir que la protección permanente se

encuentra cargada. Sobre él podremos actuar pulsando el botón derecho del ratón. Al hacer esto, se presentarán varias posibles opciones:

- **Configurar protección permanente:** permite indicar el modo en el que las protecciones permanentes (residentes) deberían comportarse. También es posible acceder a la configuración pinchando sobre el icono con el botón derecho del ratón, o haciendo doble clic sobre él. Para obtener más información, puedes consultar el apartado ¿Cómo Configurar un Análisis? (Inmediato / Programado / Permanente), en esta ayuda.



La opción de configuración del firewall incluido en Panda Antivirus Platinum solamente estará disponible si lo has instalado.

- **Lanzar Panda Antivirus Platinum:** ejecuta -abre la ventana- de Panda Antivirus Platinum, desde la *Barra de tareas de Windows*.
- **Cerrar protección permanente:** finaliza la ejecución de la protección permanente (los análisis residentes Antivirus -de archivos y de correo- y de Firewall).

Es posible consultar cada una de las incidencias ocurridas, el estado de cada una de las protecciones

permanentes (Antivirus -de archivos y de correo- y de Firewall), y realizar operaciones con dichos tipos de protecciones, pinchando sobre la opción **Protección permanente**, del **Panel de control** (en la ventana del antivirus).

Esto mostrará una lista con todas las incidencias que hayan tenido lugar. La información sobre cada una de ellas, se mostrará en las siguientes columnas del panel central: **Incidencia**, **Notificado por**, **Información adicional**, **Fecha-Hora** y **Redultado**. En la sección inferior de esta ventana, aparece un resumen con la información de los ficheros chequeados por las protecciones permanentes (de archivos, de correo y firewall):

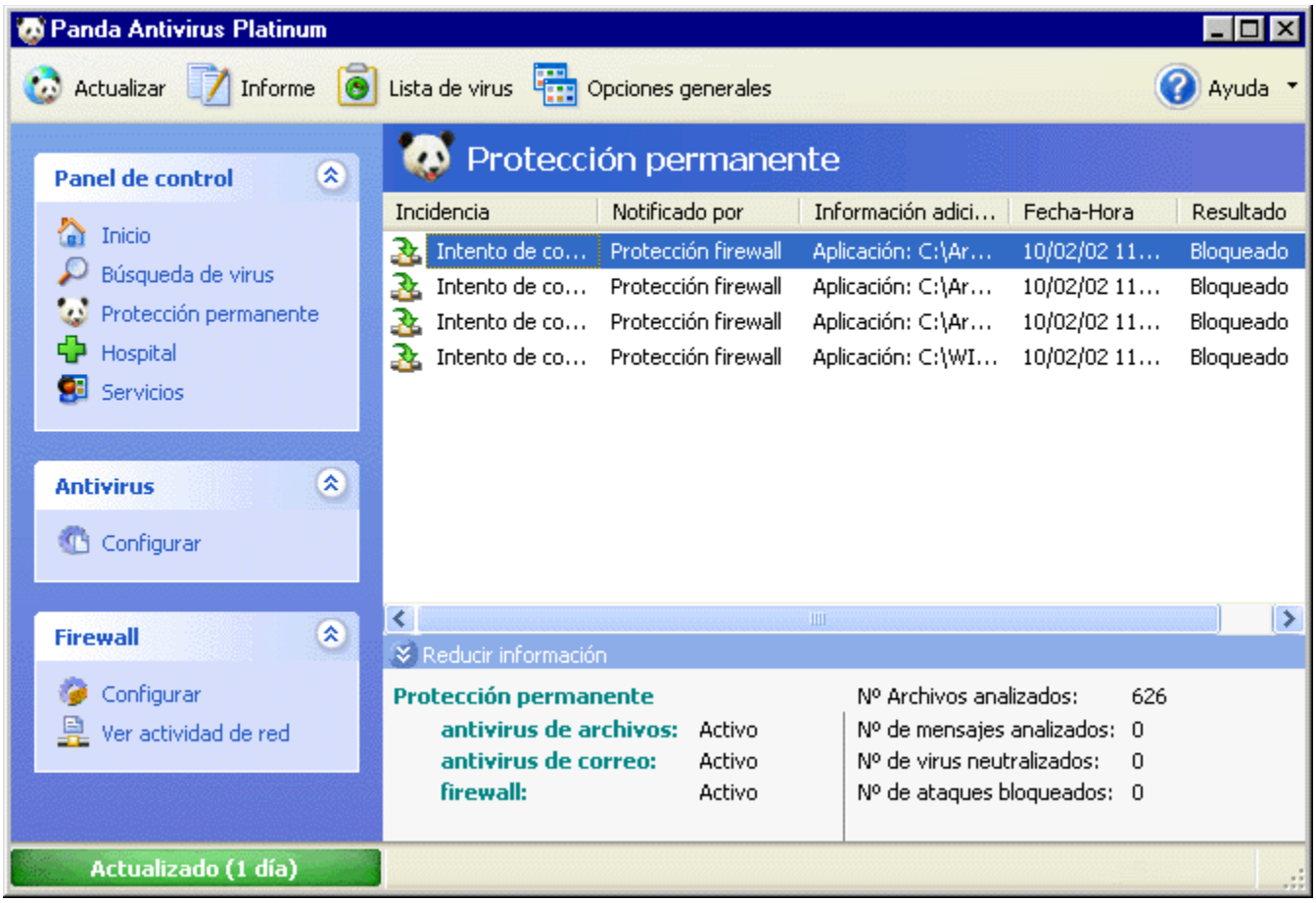
Protección permanente

Antivirus de archivos. Nos indicará el **Nº Archivos analizados** y el **Nº de virus neutralizados** en todos ellos.

Antivirus de correo. Nos indicará el **Nº de mensajes analizados**, el **Nº archivos analizados**, y el **Nº de virus neutralizados** en todos ellos.

Firewall. Nos indicará el **Nº de virus neutralizados** y el **Nª de ataques neutralizados**.

Para ampliar o reducir la información que se muestra en dicha sección, pulsaremos sobre el símbolo de doble flecha que aparece junto al título de la misma: **Ampliar información** y **Reducir información**. En el caso de que se esté mostrando la información reducida, solamente se nos indicará el **Nº Archivos analizados**.



Por otra parte, desde la propia ventana de Panda Antivirus Platinum se puede conocer el estado de la protección permanente y determinar las características de funcionamiento de la misma (configuración). Seleccionando la opción **Inicio** en el **Panel de control** de la ventana del antivirus, podrás ver (en la sección **Estado de la protección permanente**) si las protecciones permanentes (*Protección de archivos, Protección de correo* y *Protección firewall*) están *Activas* o *Inactivas*. Desde esta misma sección podrás **Configurar la protección permanente**.

Con la protección permanente (también denominada análisis permanente, o residente –Antivirus de archivos y Antivirus de correo-, así como Firewall), es posible realizar varias operaciones. Éstas se pueden llevar a cabo a través los paneles correspondientes en el **Panel de control** izquierdo: **Antivirus** (Configurar el residente de archivos y el de correoy **Firewall** (**Configurar** y **Ver actividad en la red**). o a través de las opciones del menú contextual correspondiente a cada uno de ellos:

Operaciones a realizar mediante el panel Protección **Antivirus** (archivos)

¿Cómo **Configurar** la Protección Permanente (residente) de archivos?

¿Cómo **Activar / Desactivar** la Protección Permanente (residente) de archivos?

Operaciones a realizar mediante el panel Protección **Antivirus** (correo):

¿Cómo **Configurar** la Protección Permanente (residente) de correo?

¿Cómo **Activar / Desactivar** las tareas de correo?

Operaciones a realizar mediante el panel Protección **Firewall**:

¿Cómo **Configurar** la Protección Permanente de Firewall?

¿Cómo **Activar / Desactivar** la Protección Permanente de Firewall?

¿Cómo **Ver la actividad de red** a través del Firewall?

Tipos de Análisis (Búsqueda de virus)

Panda Antivirus Platinum permite realizar diferentes tipos de análisis, indicar en cada uno de ellos los elementos que se deben analizar, crear determinados análisis, e indicar las características de cada uno de ellos.

En un principio, Panda Antivirus Platinum presenta un árbol con todos los posibles tipos de análisis y los elementos a analizar. Dicho árbol engloba dos grandes secciones, tipos o tareas de análisis dentro de la sección **Búsqueda de virus** del **Panel de control**.

- **Análisis inmediatos.** Son aquellos análisis que se ponen en marcha cuando -una vez creado-, se indica que comience el análisis. Es decir, no se activan o ponen en marcha por sí solos en un determinado momento.
- **Análisis programados.** Son aquellos análisis que se ponen en marcha por sí solos en un momento concreto, que previamente habremos prefijado. Además, pueden ejecutarse automáticamente de forma periódica en el tiempo. Esto dependerá de las características indicadas para cada uno de ellos, durante su creación.

Por otra parte, Panda Antivirus Platinum realiza o permite realizar otro tipo de análisis que nos mantiene protegidos en todo momento: el Análisis o Protección Permanente Antivirus (de archivos y de correo) y Firewall.

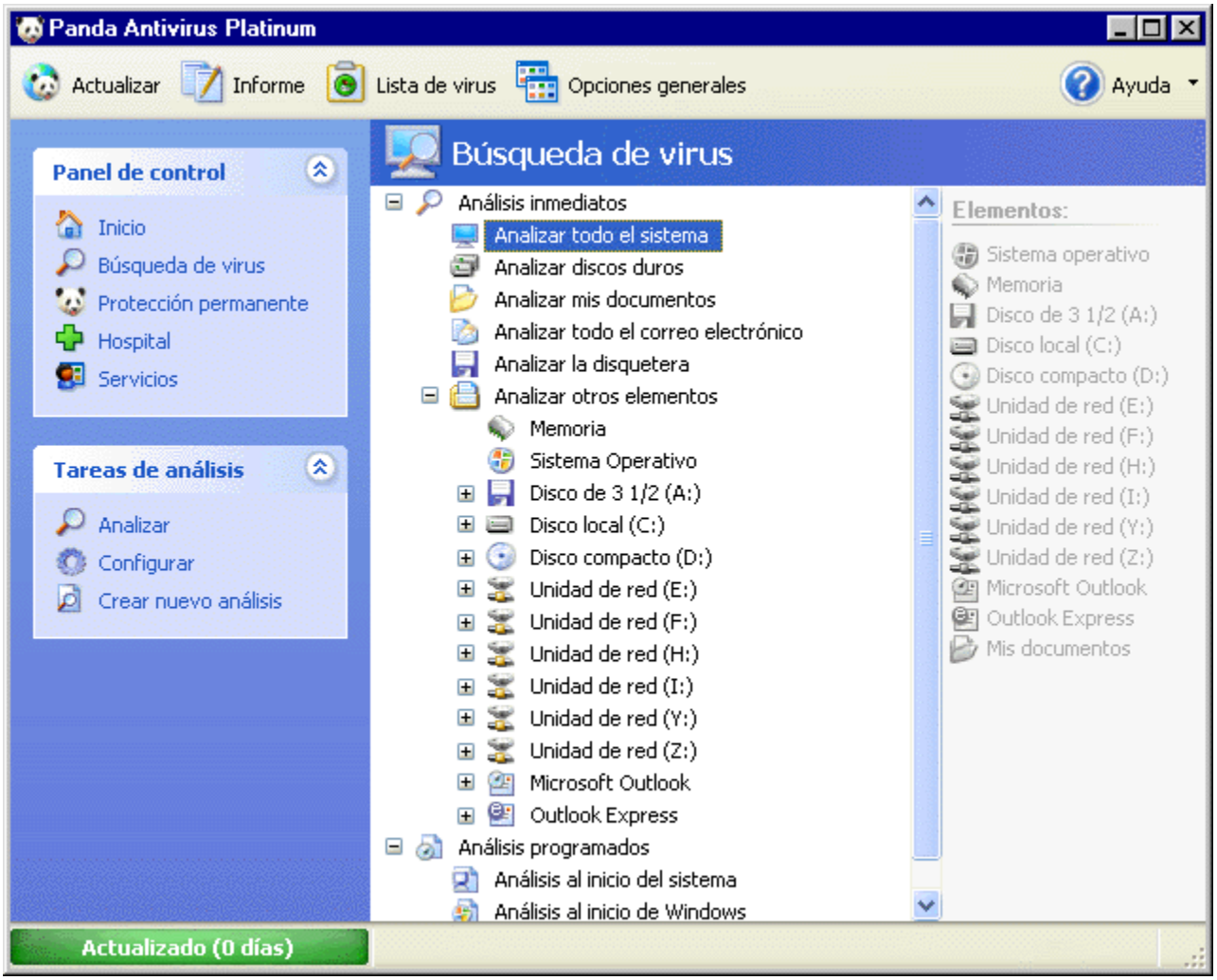
Por otra parte, también es posible realizar un análisis inmediato sobre cualquiera de los elementos (ficheros, directorios, unidades de disco,…) accesibles desde el *Explorador de Archivos de Windows*. Para hacerlo, seleccionaremos los elementos y pulsaremos con el botón derecho del ratón sobre ellos. Esto mostrará la opción **Analizar con antivirus Platinum**. Al pinchar sobre ella, todos los elementos seleccionados, serán analizados.

Nota: aunque en casi todas las ocasiones hablaremos de análisis, éstos se pueden entender realmente en Panda Antivirus Platinum como *Tareas de Análisis*. Esto es debido a que se pueden crear, modificar, configurar / editar, eliminar,…etc.

Análisis Inmediato

Los análisis inmediatos permiten analizar cualquier parte o elemento del ordenador en busca de virus, en un momento determinado. Los análisis inmediatos ofrecen la posibilidad de escoger qué área/s o elemento/s se desean analizar y se llevan a cabo en ese mismo instante, de forma inmediata. Estas características hacen que los análisis inmediatos estén especialmente indicados para verificar la no existencia de virus en nuevos ficheros que se hayan recibido por cualquier medio como disquete, correo electrónico, o se hayan bajado de Internet.

Tu Panda Antivirus Platinum cuenta con ciertos análisis inmediatos típicos, establecidos o definidos por defecto: *análisis inmediatos predefinidos o predefinidos*. Éstos son los que se usan habitualmente, por lo que el antivirus los presenta por defecto. De este modo, será mucho más sencillo, cómodo y rápido realizar un análisis en busca de virus sobre determinados elementos del ordenador. Realmente, éstos pueden estar definidos como tareas de análisis inmediato, como las siguientes:



- **Analizar todo el sistema.** Cuando este análisis o tarea de análisis predefinido se pone en marcha, son analizados todos los elementos existentes (ver el panel derecho): Memoria, Sistema Operativo, Disco de 3 ½ (disqueteras), Disco local (todos los discos duros que estuviesen

instalados en el ordenador), Disco compacto (todas las unidades de CD-ROM instaladas en el ordenador), Unidad de red (todas las unidades de disco accesibles a través de una red de ordenadores), Microsoft Outlook Express (si está instalado este programa de correo electrónico), Microsoft Outlook (si está instalado este programa de correo electrónico), y Lotus (si está instalado este programa).

- **Analizar discos duros.** Cuando este análisis o tarea de análisis predefinido se pone en marcha, son analizados todos los ficheros contenidos en los discos duros instalados en nuestro ordenador (no los accesibles a través de una red de ordenadores).
- **Analizar mis documentos.** Cuando este análisis o tarea de análisis predefinido se pone en marcha, son analizados todos los ficheros contenidos en la carpeta `Mis documentos`.
- **Analizar todo el correo electrónico.** Cuando este análisis o tarea de análisis predefinido se pone en marcha, son analizadas todas las carpetas de correo electrónico (mensajes y ficheros incluidos en éstos) gestionadas por los programas de correo electrónico instalados en nuestro ordenador.
- **Analizar la disquetera.** Cuando este análisis o tarea de análisis predefinido se pone en marcha, son analizados todos los ficheros contenidos en las unidades de disquete que estén insertadas en las disqueteras de nuestro ordenador.

Cuando se pincha sobre una de estas tareas de análisis o análisis predefinidos, se muestra a la derecha (en el panel derecho) todos los elementos que serán chequeados al ejecutar dicho análisis.

Además, si pulsamos sobre título o sección **Análisis inmediatos** del árbol, será posible crear un nuevo análisis inmediato: mediante la opción **Crear nuevo análisis** en el panel **Tareas de análisis**, o a través de la opción **Nuevo análisis** del menú contextual.

Sobre cada uno de estos análisis inmediatos predefinidos o tareas inmediatas predefinidas, es posible realizar diferentes acciones. Éstas se pueden llevar a cabo a través del panel izquierdo: **Tareas de análisis** (dicho panel se muestra cuando seleccionamos uno de los análisis o elementos predefinidos) o a través de las opciones del menú contextual correspondiente:

¿Cómo Realizar un análisis inmediato?

¿Cómo Configurar un análisis inmediato?

¿Cómo Crear un nuevo análisis inmediato?

¿Cómo Editar o Modificar un análisis inmediato?

¿Cómo Borrar o Eliminar un análisis inmediato?

Por otra parte, dentro de la sección de **Análisis inmediatos**, existe un apartado de especial interés: **Analizar otros elementos**. A través de él podemos indicar que se analicen elementos aislados (independientes de los tipos de análisis predefinidos), o crear nuevas tareas de análisis inmediato.

Análisis Programado

Los análisis programados permiten analizar cualquier elemento del ordenador en busca de virus, de forma automática, en determinados momentos indicados de antemano (periódicamente, o no).

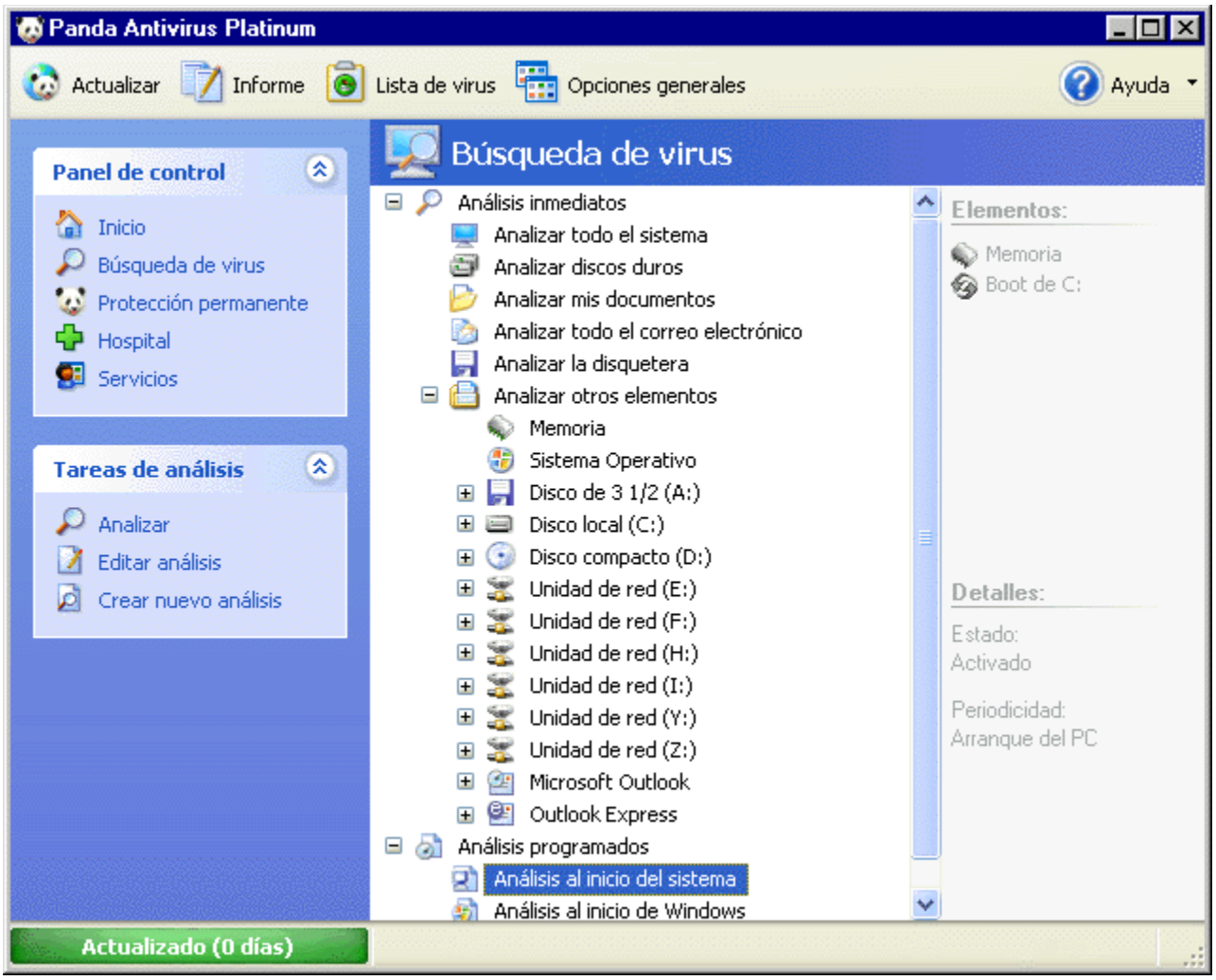
La gran utilidad de los análisis programados es la posibilidad de indicar al antivirus que debe activarse y analizar buscando virus en elementos concretos, en un momento determinado. De esta manera, se crea una ‘‘agenda’’ de análisis que facilita al máximo al usuario la tarea de mantener su ordenador limpio de virus.

Los análisis programados funcionan de igual manera que los análisis inmediatos. Se puede decir que un análisis o tarea programada es, en realidad, un conjunto de análisis inmediatos que se ejecutan en unos momentos concretos de forma automática.

Dado que los análisis programados son semejantes que los inmediatos, ambos cuentan con opciones y posibilidades de configuración similares. Ambos análisis ofrecen la posibilidad de escoger qué área o áreas se desean analizar. Sin embargo, en la creación, definición o edición de análisis programados, encontraremos una ficha de configuración adicional: **Programador**. El análisis o tarea programada se lleva a cabo en el momento que se indique. Estas características hacen que los análisis programados estén especialmente indicados para analizar el ordenador de una manera regular y autónoma manteniéndolo así libre de virus.

Al igual que en los análisis inmediatos, los análisis programados también cuentan con una serie de tareas predeterminadas de antemano (definidas por defecto por el antivirus). Se puede escoger uno de estos análisis, o se puede crear un nuevo análisis en función de las necesidades que se tenga. También existe la posibilidad de variar las opciones de análisis. Estas opciones permiten configurar el análisis para adaptarlo a las propias necesidades.

Tu Panda Antivirus Platinum cuenta con ciertos análisis programados típicos, establecidos o definidos por defecto, *análisis predefinidos o predeterminados*. Dichos análisis -o tareas de análisis- son los que se utilizan habitualmente. Por lo tanto, el antivirus los presenta por defecto en una lista. De este modo, será mucho más sencillo, cómodo y rápido realizar un análisis en busca de virus sobre determinados elementos del ordenador. Éstos pueden aparecer en la lista como tareas de análisis programado predefinidas:



- **Análisis al incio del sistema.** Cuando esta tarea de análisis programada predefinida se pone en marcha, es analizado todo el sistema de arranque del ordenador. Esto implica que son analizados todos los ficheros implicados en el funcionamiento del sector de arranque de disquetes (Boot) y del disco duro (Boot de `C:`). Con ellos se garantiza el correcto inicio del ordenador en sistemas con Windows 98/95, asegurando la detección y limpieza de los virus que puedan existir.
- **Análisis al inicio de Windows.** Cuando esta tarea de análisis programada predefinida se pone en marcha, son analizados al iniciar Windows, la memoria del ordenador así como los ficheros implicados en el funcionamiento del Sistema Operativo. Este análisis nos garantiza el correcto inicio de Windows, asegurando la detección y limpieza de los virus que puedan existir.

Al pinchar sobre una de estas tareas de análisis o análisis predefinidos, se mostrarán en el panel derecho todos los elementos que serán chequeados al ejecutar dicho análisis.

Además, si pulsamos sobre título o sección **Análisis Programados** del árbol, será posible crear un nuevo análisis programado: mediante la opción **Crear nuevo análisis** en el panel **Tareas de análisis**, o a través de la opción **Nuevo análisis** del menú contextual.

Cada uno de estos análisis programados predefinidos o tareas programadas predefinidas, permite realizar diferentes acciones sobre ellos. Dichas acciones se pueden llevar a cabo a través del panel de

control izquierdo: **Tareas de análisis** (éste se muestra cuando seleccionamos uno de estos análisis) o a través de las opciones del menú contextual correspondiente:

¿Cómo Realizar un análisis programado?

¿Cómo Configurar un análisis programado?

¿Cómo Crear un nuevo análisis programado?

¿Cómo Editar o Modificar un análisis programado?

¿Cómo Borrar o Eliminar un análisis programado?

¿Cómo Realizar un Análisis? (Inmediato / Programado)

Como ya sabemos, los análisis inmediatos y programados pueden ser predefinidos y podemos realizar análisis inmediatos o programados de elementos indepedientes (memoria, discos,…), así como crear nuevas tareas de análisis, tanto inmediatas como programadas.

En cualquier caso, todos los elementos a analizar, tanto mediante los análisis inmediatos como con los programados, pueden chequearse (la tarea de análisis en cuestión puede ponerse en marcha) cuando se desee. Para realizar o poner en marcha en un determinado momento una tarea de análisis (ya sea esta inmediata o programada), seguiremos estos pasos:

1. Tanto para realizar un análisis inmediato como un programado, selecciona previamente los elementos que deseas analizar mediante:

    - Análisis predefinidos de antemano. Tanto los inmediatos (**Analizar todo el sistema**, **Analizar discos duros**, **Analizar mis documentos**, **Analizar todo el correo electrónico**, **Analizar la disquetera**), como programados (**Análisis al incio del sistema** -en equipos con Windows 98/95-, **Análisis al inicio de Windows**).
    - Cualquiera de los elementos independientes (memoria, Sistema Operativo, discos,…), que se encuentran dentro de la sección **Analizar otros elementos**.
    - Análisis creados (Inmediatos o programados) por el usuario.

2. Pon en marcha el análisis (la tarea de análisis), seleccionando la opción **Analizar**. Dicha opción es seleccionable de varias formas:

    - Desde el panel **Tareas de análisis**. En este caso, simplemente pincha sobre la opción **Analizar**.
    - Desde el menú contextual. En este caso, habiendo pulsado con el botón derecho del ratón sobre el análisis en cuestión, selecciona la opción **Analizar**.
    - A través de las teclas de función. En este caso, habiendo seleccionado el tipo de análisis, pulsaremos la tecla de función *F8*.

En ambos casos (análisis inmediatos y programados), el análisis se pondrá en marcha. Si se detecta un virus, Panda Antivirus Platinum avisará de esta circunstancia y ejecutará una acción determinada (desinfección, eliminación,…) en función de nuestras indicaciones (a través de la configuración). Para obtener más información sobre el curso de los análisis, se sugiere la consulta del apartado Curso de los Análisis y Posibles Incidencias, en esta ayuda.

¿Cómo Configurar un Análisis? (Inmediato / Programado / Permanente)

Las opciones de análisis permiten configurar cómo se llevará a cabo el análisis en busca de virus. Para acceder a dichas opciones, hay que seleccionar el tipo de análisis, o el elemento que se desea analizar (salvo en el caso de la protección permanente). Entonces debemos seleccionar la opción correspondiente en el panel **Tareas de análisis**.

En el caso de los análisis inmediatos predefinidos, o si se ha seleccionado un elemento independiente, seleccionaremos la opción **Configurar**. Si hemos seleccionado un análisis programado predefinido, o uno creado por los usuarios, debemos seleccionar la opción **Editar análisis**.

En el caso de la protección permanente, seleccionaremos la opción **Configurar**, correspondiente al panel **Antivirus**, o al panel **Firewall**, según nos interese.

Todas las opciones de análisis están agrupadas en una misma ventana pero separadas en distintas pestañas para facilitar así su gestión. Estas pestañas pueden ser diferentes en función del tipo de análisis (inmediato, programado, protección permanente,…), o elemento a analizar (memoria, disco duro, sistema operativo,…).

Aunque las opciones de configuración son similares en los diferentes tipos de análisis, la siguiente tabla muestra todas opciones de configuración disponibles para cada uno de ellos:

Opciones de configuración de los análisis Inmediatos, Programados y de la Protección Permanente (Antivirus -archivos y correo- y Firewall)

Configuración de los análisis Inmediatos

Análisis
Acciones
Exclusiones
Alertas

Configuración de los análisis Programados

Análisis
Acciones
Exclusiones
Alertas
Programador

Configuración de la Protección Permanente (Antivirus)

De Archivos

Análisis
Acciones
Exclusiones

Alertas

De Correo

E-mail – News
Acciones
Alertas

Configuración de la Protección Permanente (Firewall)

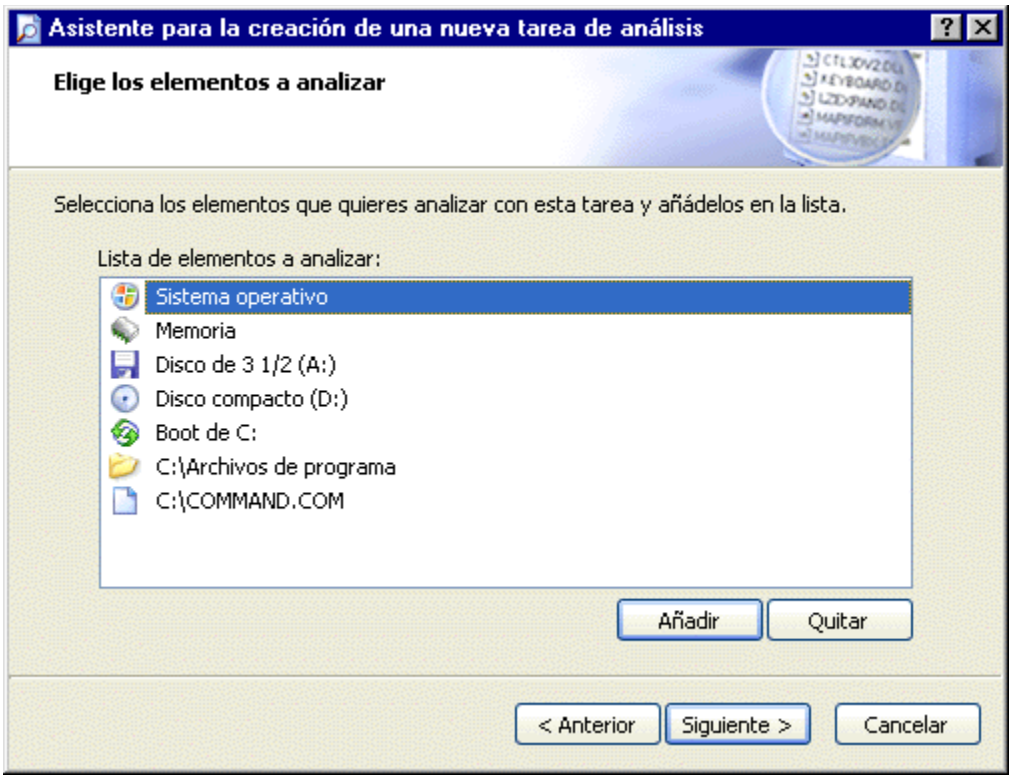
Accesos
Seguridad
Conexiones telefónicas
Reglas
Programas

¿Cómo Crear un Nuevo Análisis? (Inmediato / Programado)

Los análisis (inmediatos y programados) que Panda Antivirus Platinum realiza, pueden considerarse como tareas de análisis que se pueden crear, modificar y eliminar (borrar). Sin embargo los análisis predeterminados -los análisis que ya tiene definidos el antivirus, tanto inmediatos como programados-, no podrán ni crearse ni eliminarse. No obstante, los análisis predefinidos o predeterminados sí se pueden configurar. Además, también es posible crear nuevas tareas de análisis (inmediatas o programadas), con características similares o idénticas a las de éstos.

Es muy sencillo crear una nueva tarea de análisis (inmediata o programada). Solamente deben seguirse estos pasos:

1. En la ventana del antivirus y dentro del **Panel de control**, pincha en la sección **Búsqueda de virus**.
2. En el panel **Tareas de análisis**, selecciona **Crear nuevo análisis**. Esto abre el asistente para la creación del nuevo análisis (común para los inmediatos y para los programados). También puede comenzarse pulsando con el botón derecho del ratón sobre cualquiera de los tipos análisis (inmediatos o programados) y seleccionando la opción **Nuevo análisis**.
3. Pantalla de bienvenida al asistente para la creación de una nueva tarea de análisis. Pulsa el botón **Siguiente**, para continuar.
4. Indica los elementos (unidades, ficheros, directorios,…) que el nuevo análisis que estás creando, deberá analizar. Para hacerlo, pulsa el botón **Añadir**.
5. Utilizando los signos + de la lista (o árbol), selecciona uno a uno los elementos que se desea analizar y pulsa el botón **Aceptar**. Así se irán agregando de uno en uno a la lista total de elementos a analizar. Si desea eliminar alguno de ellos de dicha lista, selecciónalo y pulsa el botón **Quitar**.



6. Cuando hayas preparado la lista con todos los elementos que el nuevo análisis debe chequear, pulsa el botón **Siguiente**.
7. Indica las características que debe tener el análisis y si éste debe ser programado o no.

   Botón **Configuración**. Pulsa este botón, para acceder a las opciones de configuración del análisis. Mediante las fichas **Análisis**, **Acciones**, **Exclusiones** y **Alertas**, indica las propiedades o características que debe tener el nuevo análisis. Si deseas obtener más información sobre la configuración, consulta el apartado ¿Cómo Configurar un Análisis? (Inmediato / Programado / Permanente), de esta ayuda.

   Casilla de verificación **Quiero que esta tarea se realice periódicamente.** Márcala si deseas que el análisis sea programado y que se ponga en marcha de forma automática y periódica. En tal caso se activa el botón **Planificación**. Púlsalo para programar la periodicidad con la que el análisis programado debe ejecutarse automáticamente. Puedes consultar el apartado Configuración de los Análisis Programados - Ficha Programador, en esta ayuda.

8. Escribe el nombre que quieres asignar a la tarea de análisis que estás creando, y pulsa el botón **Siguiente**.
9. Para terminar la definición de la nueva tarea de análisis que estás creando, pulsa el botón **Finalizar**.
10. Al final de la lista de análisis (inmediatos o programados, según hayas especificado durante la creación del mismo), aparecerá el nombre del análisis que se acaba de crear. Si en su definición no se indicó ninguna planificación, éste se encontrará al final de los análisis inmediatos. Si se definió una planificación, éste se encontrará al final de los análisis programados.

Puedes consultar las características de cualquiera análisis, seleccionándolo . Al hacerlo, el panel

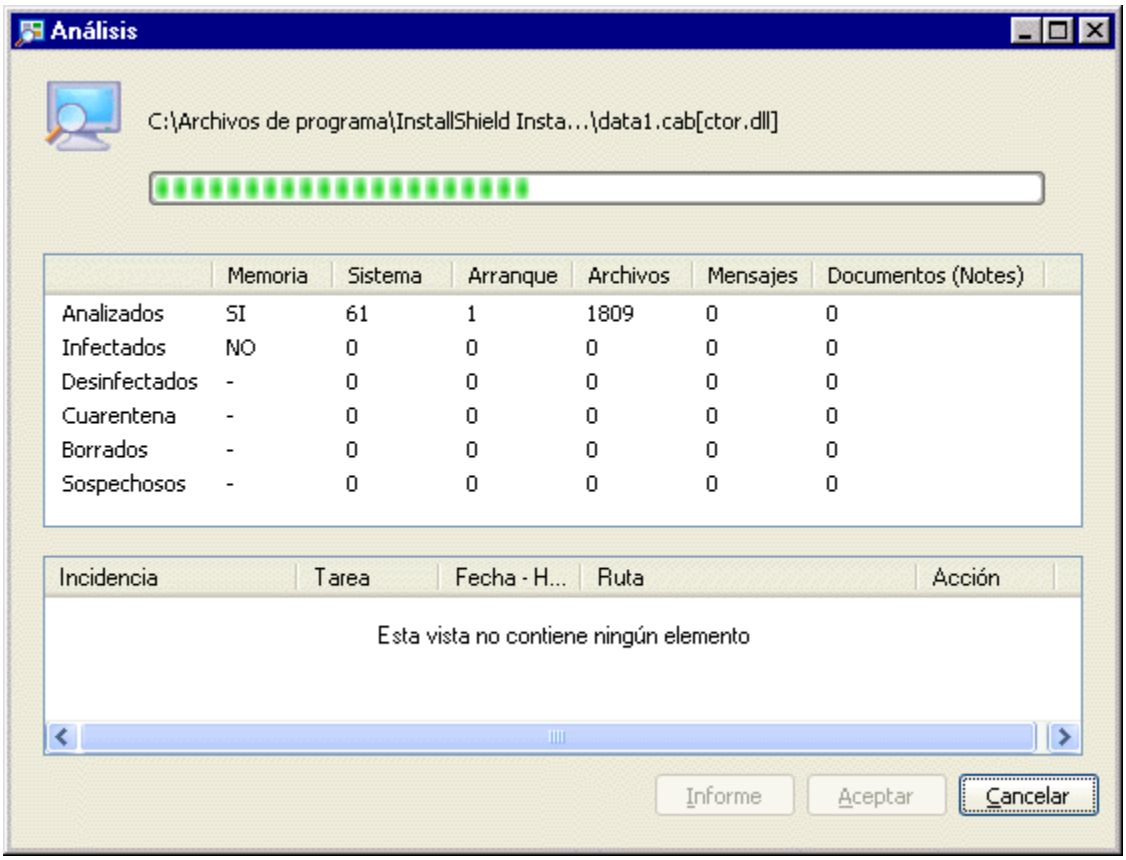
derecho de la pantalla mostrará cada una de sus propiedades: **Elementos** que analizará y otros **Detalles** (éste último, sólo en el caso de los análisis programados).

Si deseas cambiar el nombre a uno de los análisis (tareas de análisis) que has definido, pincha una vez sobre él con el ratón y, cuando esté seleccionado, vuelve a pinchar en él. Con esto se edita el nombre en un cuadro de texto. Modifica su título y pulsa la tecla *intro*.

Curso de los Análisis y Posibles Incidencias

Al indicarlo mediante la opción **Analizar**, el tipo de análisis que hayamos seleccionado o el chequeo del elemento seleccionado, se pondrá en marcha. Entonces será visible un cuadro de diálogo, donde aparecerá una barra de progreso. Ésta nos indica el curso del análisis (el ‘‘porcentaje’’ realizado del mismo, así como los elementos que se van analizando).

Mientras el proceso de análisis tiene lugar, la barra de progreso se incrementa y se van mostrando los datos correspondientes al número de elementos (**Memoria**, **Sistema**, **Arranque**, **Mensajes**, o **Documentos**) que han sido Analizados, Infectados, Desinfectados, colocados en Cuarentena, Borrados y marcados como Sospechosos, en cada una de las secciones analizadas.



En la sección inferior de este cuadro de diálogo se mostrará -en el caso de que sucedan-, todas las incidencias que hayan ocurrido. Se detalla el nombre de la **Incidencia**, la **Tarea** en la que ocurrió, la **Fecha** – **Hora** de la misma, la **Ubicación** o lugar en el que se produjo y la **Acción** llevada a cabo.

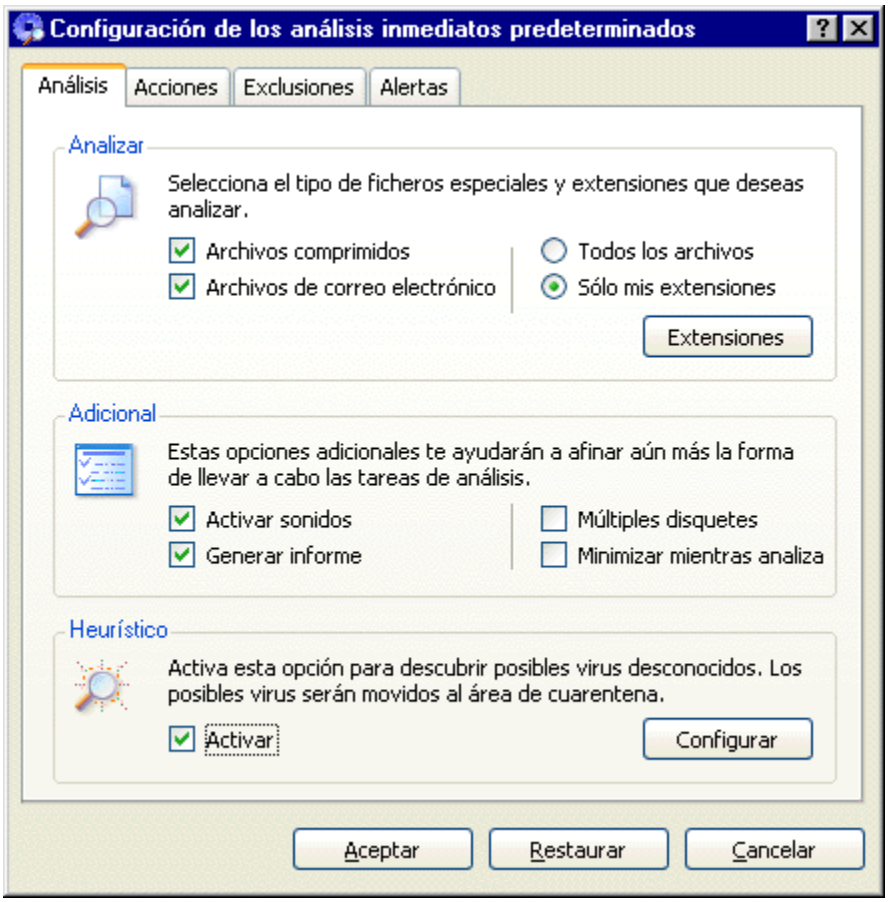
Cuando el análisis finaliza, se activan los botones **Informe** y **Aceptar**. Pulsando el primero de ellos, **Informe**, se accede a un listado con la información correspondiente a todos los análisis realizados. Para obtener más información sobre el resultado de los análisis realizados, se aconseja la consulta del apartado Informe de esta ayuda. Si se pulsa el botón **Aceptar**, el cuadro de diálogo que mostraba el progreso del análisis se cerrará.

Configuración de los Análisis - Ficha Análisis (Inmediatos / Programados / Permanente de Archivos)

Dentro de esta pestaña hay diversas opciones que se agrupan para mayor comodidad, en lo que respecta a la configuración o determinación de las propiedades que deben tener los análisis:

NOTA: esta ficha de configuración, NO existe en el caso de la protección permanente de correo electrónico (o residente de correo).

Ficha correspondiente a la configuración de los análisis en el caso de tareas de análisis inmediato y programado.



Sección **Analizar**

Dentro de esta sección se encuentran disponibles todas las opciones que nos permiten indicar el tipo de ficheros a analizar y determinar si es necesaria la generación de informes.

- **Archivos Comprimidos:** si esta opción está marcada, se analizarán todos aquellos ficheros comprimidos (tipo *ZIP*, *RAR*, *ARJ*, *LZH*, *LZA*, etc) que se encuentren. Estos ficheros sólo se analizarán si se marca esta opción, no es suficiente con seleccionar la opción correspondiente a todas las extensiones. En el caso de los análisis correspondientes a la protección permanente (o residente) de archivos, esta opción llevará el nombre de **Comprimidos**.

- **Archivos de correo electrónico:** si se marca esta opción, el antivirus analizará todos aquellos ficheros de correo electrónico (mensajes y ficheros incluidos en ellos) que encuentre, independientemente de lo que se indique en el apartado **Extensiones**. El antivirus es capaz de analizar los ficheros de correo electrónico correspondientes a varios programas clientes de correo electrónico (entre ellos Microsoft Outlook -fichero *PST*- y Microsoft Outlook Express, etc.). Estos ficheros sólo se analizarán si se marca esta opción, no es suficiente con seleccionar todas las extensiones. Esta opción NO está disponible para la Protección permanente de archivos y de correo.
- **Generar informe:** Esta opción SÓLO está disponible para la Protección permanente de ficheros. Sí se marca esta opción, los datos relativos al análisis en cuestión se registrarán en el informe.
- **Todos los archivos:** seleccionando esta opción se analizarán todos los ficheros, independientemente de su extensión -a excepción de los ficheros comprimidos-, los del sistema y los ficheros de correo electrónico que se deben marcar aparte para ser analizados.
- **Sólo mis extensiones:** esta opción permite indicar que se deben analizar sólo aquellos ficheros cuya extensión se encuentre en la lista de extensiones. A esta lista se accede pulsando el botón **Extensiones** (que estará activo solamente cuando se haya seleccionado la casilla **Sólo mis extensiones**).

En el caso de la configuración correspondiente a la protección permanente de archivos, esta sección incluye un botón adicional, con el título **Opciones avanzadas**. Pulsando este botón, podremos definir cómo se debe comportar la protección permanente de archivos en las **Unidades de Red**.

Esta sección SÓLO está disponible en el caso de la Protección permanente de archivos (Protección archivos). NO está disponible en la configuración de los análisis inmediatos y programados. Tampoco lo está en la configuración de los análisis para la protección de correo (ya que esta ficha de configuración no existe en dicho tipo de análisis o protección). Mediante las dos casillas de verificación que incorpora, es posible determinar el funcionamiento de la Protección permanente de archivos en las unidades de red a las que tengamos acceso desde nuestro ordenador.

- **Analizar:** las unidades de red, a las que tengamos acceso desde nuestro ordenador, serán analizadas (por la protección permanente de archivos), si esta casilla se encuentra marcada.
- **Bloquear en caso de infección:** si esta casilla se encuentra marcada y se detecta un virus (ya sea en una unidad de la red a la que se tiene acceso, o en cualquier elemento del ordenador en el se está trabajando -local-), se bloquea el acceso a la red. Con esto se evita, en caso de infección, la propagación del virus al resto de ordenadores conectados a la red.

Nota: estas dos opciones anteriores son las que se muestran en el caso de Windows, Millennium, Windows 98, o Windows 95. Para el caso de sistemas con Windows XP, Windows 2000 Pro, o Windows NT, se mostrarán las siguientes:

- **Red de Microsoft:** si se marca esta casilla, serán analizadas las unidades de red, siempre que la red sea Microsoft.
- **Red de Novell:** si se marca esta casilla, serán analizadas las unidades de red, siempre que la red sea Novell.

Sección **Adicional**

Esta sección NO está disponible en el caso de la Protección permanente (Protección de correo y Protección de archivos), pero sí en la configuración de los análisis inmediatos y programados. Dentro de esta sección se encuentran disponibles opciones complementarias para mejorar en lo posible las características y funcionamiento de los análisis.

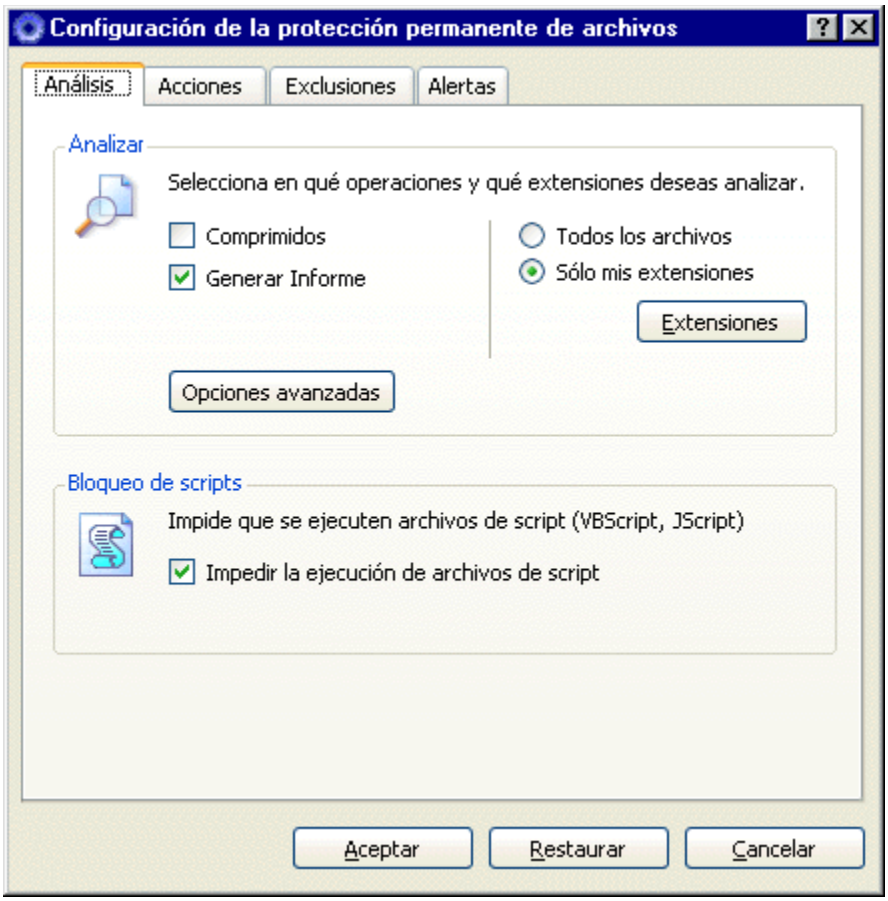
- **Activar sonidos:** si se marca esta opción, se activarán los sonidos durante los procesos de análisis que se lleven a cabo, de acuerdo a la configuración que se haya realizado en el apartado correspondiente en la Configuración General del Antivirus.
- **Generar informe:** si se marca esta opción, los datos relativos al análisis en cuestión se registrarán en el informe.
- **Múltiples disquetes:** permite indicar que se desean analizar varios disquetes de manera consecutiva. De esta forma, cuando se acabe de analizar un disquete se solicitará la introducción del siguiente en la disquetera.
- **Minimizar mientras analiza:** si se marca esta opción, la ventana del antivirus se minimizará (aparecerá como un botón en la *Barra de tareas de Windows*) automáticamente cuando comience el análisis, siguiendo el curso del mismo hasta que éste finalice o se indique que debe finalizar.

Sección **Heurístico**

Esta sección NO está disponible en el caso de la Protección permanente de correo y ni en la de archivos, pero si en la configuración de los análisis inmediatos y programados. Los análisis que emplean técnicas heurísticas permiten localizar y descubrir posibles nuevos virus. Éstos serán desconocidos hasta el momento y el actual archivo de identificadores de virus, podría no detectarlos.

- **Activar:** si se marca esta opción, cada fichero será sometido a un análisis adicional en busca de posibles nuevos virus. Este segundo análisis se realiza en base a técnicas diseñadas para detectar virus no conocidos.
- Botón **Configurar**: este botón permite configurar el análisis heurístico, solamente cuando se haya marcado la casilla **Activar**. Es posible elegir uno, entre tres niveles distintos de sensibilidad: **Máxima sensibilidad**, **Sensibilidad media (recomendada)**, o **Mínima sensibilidad**.

Ficha correspondiente a la configuración de los análisis en el caso de la protección permanente de archivos.



Sección **Analizar**
Dentro de esta sección se encuentran disponibles todas las opciones que nos permiten indicar el tipo de ficheros a analizar y determinar si es necesaria la generación de informes.

- **Comprimidos:** si esta opción está marcada, se analizarán todos aquellos archivos comprimidos (tipo *ZIP*, *RAR*, *ARJ*, *LZH*, *LZA*, etc) que se encuentren. Estos archivos sólo se analizarán si se marca esta opción, no es suficiente con seleccionar la opción correspondiente a todas las extensiones.
- **Generar informe:** Sí se marca esta opción, los datos relativos al análisis de la protección permanente de archivos, se registrarán en el informe.
- **Todos los archivos:** seleccionando esta opción se analizarán todos los archivos, independientemente de su extensión -a excepción de los archivos comprimidos- y los del sistema que se deben marcar aparte para ser analizados.
- **Sólo mis extensiones:** esta opción permite indicar que se deben analizar sólo aquellos archivos cuya extensión se encuentre en la lista de extensiones. A esta lista se accede pulsando el botón **Extensiones** (que estará activo solamente cuando se haya seleccionado la casilla **Sólo mis extensiones**).

Sección **Bloqueo de scripts**

Mediante esta sección, que sólo existe en la ficha de configuración de la protección permanente de archivos, puedes impedir que se ejecuten los ficheros escritos en lenguaje Script (VBSsript, o JScript).

- **Impedir la ejecución de archivos de script:** si marcas esta casilla, tu Panda Antivirus Platinum,

impedirá la ejecución de los ficheros escritos en algún lenguaje de programación de tipo script (Visual Basic Script, o Java Script).

En la parte inferior de las pantallas de configuración, aparecen varios botones de interés:

Aceptar: los cambios realizados en la configuración, se guardarán y se aplicarán.

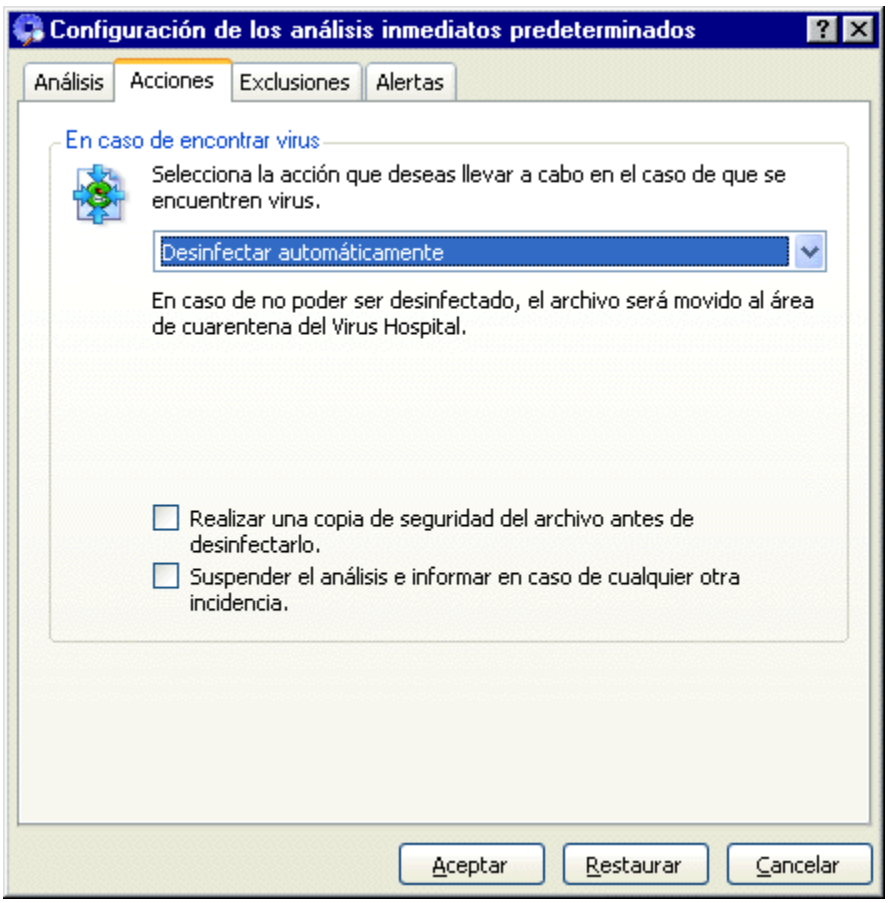
Restaurar: hace posible seleccionar la configuración establecida por defecto para los análisis. Se preguntará **¿Seguro que desea restaurar la configuración de fábrica?**. Contesta **Sí** (el antivirus vuelve a estar configurado como lo estaba tras su instalación), o **No**.

Cancelar: los cambios realizados en la configuración, no se guardarán ni se aplicarán.

Configuración de los Análisis - Ficha Acciones (Inmediatos / Programados / Permanente)

A través de esta pestaña es posible determinar cuál es la acción que el antivirus debe llevar a cabo cuando éste encuentra un virus. En función de la acción escogida, existirán determinadas opciones, particulares y correspondientes a las características concretas de dicho caso.

NOTA: la lista de acciones a realizar siempre muestra las mismas opciones en el caso de los análisis inmediatos y de los análisis programados (ya sean éstos predefinidos de antemano, o creados por el usuario). Sin embargo, dicha lista varía en el caso de la Protección permanente (o residente) de archivos y de correo.



Cuando desplegamos la lista de acciones, nos encontramos con las siguientes acciones (ten en cuenta el tipo de análisis, pues dicha lista varía de un tipo a otro):

Impedir acceso al archivo
Esta opción de la lista SÓLO está disponible en al caso de la Protección Permanente de archivos. Por lo tanto, NO estará disponible para la Protección Permanente de correo, ni para cualquier otro tipo de análisis (ni Inmediatos, ni en los Programados, ya sean éstos predefinidos o creados por el usuario).

Esta opción (**Impedir acceso al archivo**) indica que el antivirus no debe detener el análisis al detectar un virus en un fichero infectado y además, no permite utilizar dicho fichero. Es decir, se mostrará

información sobre la incidencia, pero no se llevará a cabo ninguna otra acción.

Ignorar y continuar analizando

Esta acción hace que el antivirus no lleve a cabo ninguna acción cuando detecte un virus. El análisis continuará de forma normal. Aparece además la casilla de verificación **Suspender el análisis e informar en caso de cualquier otra incidencia** (no aparece en el caso de la protección permanente). Si se marca esta opción, el análisis se detendrá momentáneamente si se produce algún problema inesperado durante el mismo para así poder informar de dicha incidencia. Aceptado el aviso se podrá continuar con el análisis normalmente.

Nota: esta opción (**Ignorar y continuar analizando**) NO existe en el caso de la Protección permanente de archivos, pero SÍ en los análisis Inmediatos y Programados (ya sean estos últimos predefinidos o creados por el usuario).

Desinfectar automáticamente

Mediante esta opción se le puede indicar al antivirus que desinfecte de manera automática todos aquellos ficheros infectados que detecte.

Si el virus no se puede desinfectar, el fichero infectado será movido automáticamente al área de cuarentena, correspondiente al **Hospital**. Esto significa que dicho fichero desaparecerá de su ubicación original.

Además, al seleccionar la opción **Desinfectar automáticamente** en la lista desplegable, aparecerán dos casillas de verificación en la sección inferior de la ficha:

- **Realizar una copia de seguridad del archivo antes de desinfectarlo**. En el caso de que el antivirus desinfecte el fichero, éste creará una copia del mismo, antes de realizar la desinfección. De este modo, si el fichero quedase inservible tras la desinfección, seguiría existiendo una copia del mismo. Podrás tener acceso a la copia de dicho fichero, así como restaurarla en su ubicación original,… etc., utiliza la sección Hospital del antivirus.
- **Suspender el análisis e informar en caso de cualquier otra incidencia.** Esta casilla de verificación NO está disponible en el caso de la Protección permanente de archivos y de correo. SÓLO estará disponible en el caso de los análisis Inmediatos y Programados (ya sean estos predefinidos, creados por el usuario, o análisis de elementos independientes). Si se marca esta casilla, el análisis se detendrá momentáneamente si se produce algún problema inesperado durante el mismo para así poder informar de dicha incidencia. Aceptado el aviso se podrá continuar con el análisis normalmente.

Borrar el archivo infectado

Seleccionando esta opción, se borrarán todos aquellos ficheros infectados que detecte el antivirus. Aparece además la casilla de verificación **Suspender el análisis e informar en caso de cualquier otra incidencia.** Si se marca esta opción, el análisis se detendrá momentáneamente si se produce algún problema inesperado durante el mismo para así poder informar de dicha incidencia. Aceptado el aviso se podrá continuar con el análisis normalmente.

Mover a cuarentena el archivo infectado

Seleccionando esta opción, se moverán de su ubicación original todos aquellos ficheros infectados que se detecten. Éstos pasarán a formar parte de la Cuarentena. Aparece además la casilla de verificación **Suspender el análisis e informar en caso de cualquier otra incidencia.** Sin embargo,

aunque la acción de **Mover a cuarentena el archivo infectado** sí aparece en la configuración de la Protección permanente (de archivos y de correo), la opción **Suspender el análisis e informar en caso de cualquier otra incidencia** NO aparece en el caso de la Protección permanente de archivos y de correo. Si se marca esta opción, el análisis se detendrá momentáneamente si se produce algún problema inesperado durante el mismo para así poder informar de dicha incidencia. Aceptado el aviso se podrá continuar con el análisis normalmente.

Preguntar por la acción a realizar

Mediante esta opción se le indica al antivirus que deberá preguntar por la acción a realizar cada vez que detecte un virus. Esto permite indicar distintas acciones en un mismo análisis. Para hacer más flexible la configuración, se pueden elegir las opciones que se mostrarán en el momento de la detección del virus. Las casillas de verificación que se marquen, serán las acciones que podremos seleccionar en el momento en el que el antivirus nos pregunte sobre la acción que debe realizar. Dependiendo del tipo de análisis que se esté configurando (inmediato, programado, o protección de correo), las casillas de verificación disponibles cambiarán.

Nota: esta opción NO está disponible en el caso de la Protección Permanente de archivos y tampoco en el caso de los análisis programados predefinidos al inicio del sistema.

- **Mover a cuarentena:** si se indica esta opción, se moverán a la cuarentena del **Hospital** todos aquellos ficheros infectados que se detecten.
- **Borrar:** si se indica esta opción, se borrarán todos aquellos ficheros infectados que se detecten.
- **Desinfectar:** si se marca esta casilla y se detecta un virus en un fichero, éste será desinfectado.

Realizar copia de seguridad del fichero en caso de desinfección. Si el antivirus desinfecta algún fichero, éste pasará automáticamente a la Cuarentena. Allí el antivirus mantienen los ficheros que son sospechosos. Para obtener más información sobre esta característica del antivirus, consulta el apartado Hospital, de esta ayuda.

Suspender el análisis e informar en caso de cualquier otra incidencia. Si se marca esta opción, el análisis se detendrá momentáneamente si se produce algún problema inesperado durante el mismo para así poder informar de dicha incidencia. Aceptado el aviso se podrá continuar con el análisis normalmente. Esta opción NO está disponible en la configuración de la Protección Permanente (ni en la Protección de archivos, ni en la Protección de correo).

En la parte inferior de las pantallas de configuración, aparecen varios botones de interés:

Aceptar: los cambios realizados en la configuración, se guardarán y se aplicarán.

Restaurar: hace posible seleccionar la configuración establecida por defecto para los análisis. Se preguntará **¿Seguro que desea restaurar la configuración de fábrica?**. Contesta Sí (el antivirus vuelve a estar configurado como lo estaba tras su instalación), o No.

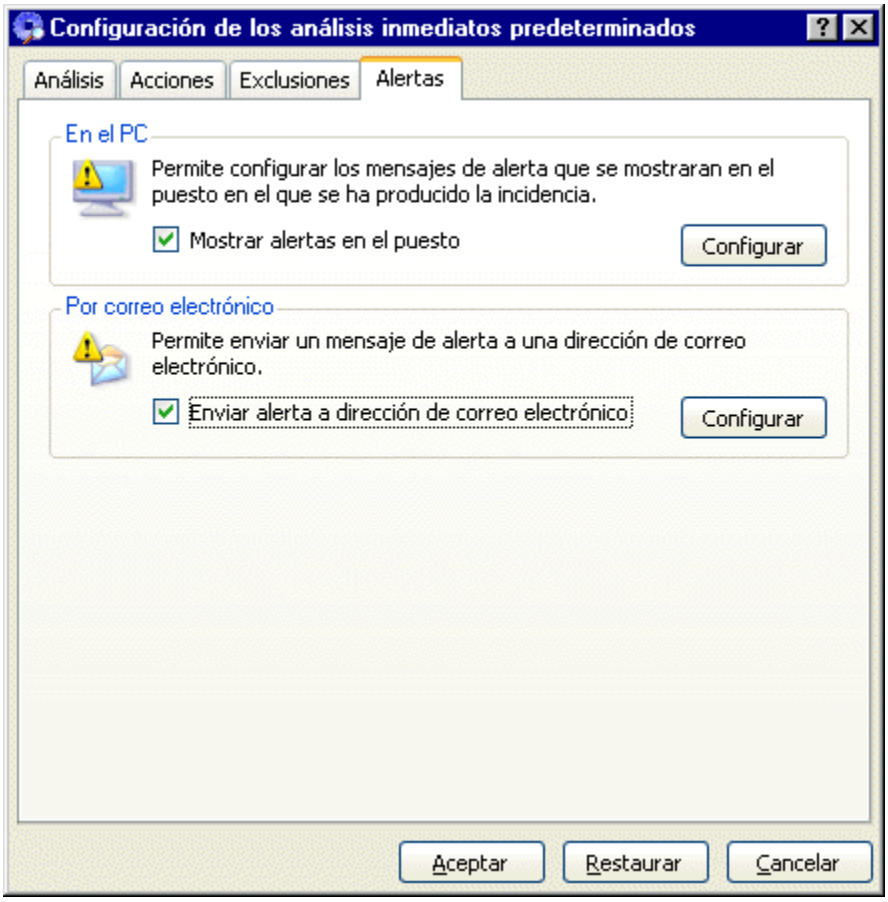
Cancelar: los cambios realizados en la configuración, no se guardarán ni se aplicarán.

Configuración de los Análisis - Ficha Alertas (Inmediatos / Programados / Permanente)

Las alertas son aquellos avisos que genera el antivirus indicando que ha detectado un virus. Dada la importancia de este tipo de avisos, su configuración es flexible y potente para asegurar que el aviso de virus llegue a la persona indicada.

Esta ficha de configuración es idéntica en el caso de los análisis inmediatos y programados (predefinidos o creados por el usuario). Sin embargo existe alguna excepción:

- En el caso de la Protección permanente archivos, SÓLO se permite el envío de alertas en el PC (ningún otro tipo de alertas), para el caso de sistemas con Windows Me/98/95. Además, las características de dichas alertas en el PC, no pueden ser configuradas. En sistemas con Windows XP/2000 Pro/NT, también se permite el envío de alertas por correo electrónico.
- En el caso de la Protección permanente de correo, se permite el envío de alertas en el PC y cualquier otro tipo de alertas (por correo electrónico). De todas formas, no será posible configurar las características de las alertas en el PC.
- La ficha para la configuración de las alertas, no existe en el caso de los análisis programados al inicio del sistema.



Nota: imagen correspondiente a la cofiguración en un sistema Windows Me/98/95.

Para activar un sistema de alertas concreto (**En el PC**, o **Por correo electrónico**), basta con marcar la casilla de verificación que aparece a su lado. Si además se pretende controlar cómo deben producirse

dichas alertas, es necesario pulsar el botón **Configurar**. Las opciones de estas alertas pueden variar de un tipo de análisis a otro. Los tipos de alertas que se pueden presentar son:

En el PC. Mediante esta opción, se puede escoger cómo se avisará de la detección de un virus en el ordenador donde se ha detectado un virus. Si se desea ver alertas de virus en ese PC, se deberá marcar la casilla **Mostrar alertas en el puesto** y pulsar el botón **Configurar** para indicar el formato de los avisos, mediante las siguientes secciones:

NOTA: en el caso de la Protección permanente de archivos (alertas en el PC) y de correo (alertas Locales), solamente es posible activar o desactivar este tipo de alertas, pero no configurar su funcionamiento.

Alerta sonora

- **Alerta Sonora:** reproduce un sonido en el momento de la detección del virus.
- **Beep:** si se escoge esta opción, sonará un pitido cada vez que se detecte un virus.
- **Fichero WAV:** si se escoge esta opción, cada vez que se detecte un virus se reproducirá un archivo de sonido de tipo `WAV`. Se puede indicar qué archivo `WAV` se desea escuchar, mediante el botón que aparece a la derecha.

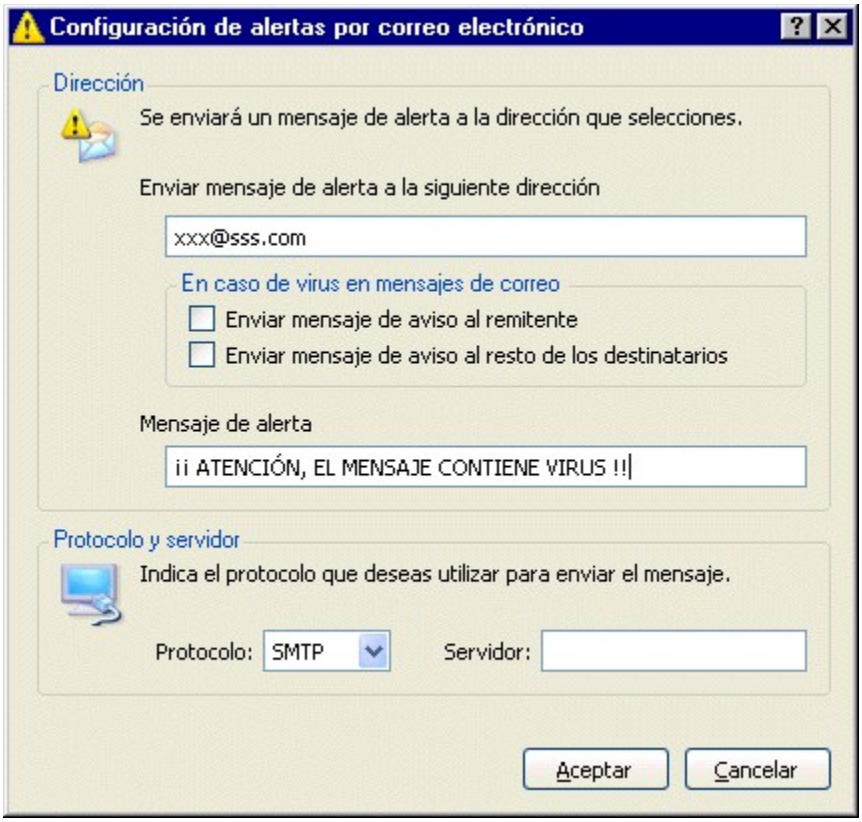
Mensaje de alerta

- **Mostrar el siguiente mensaje de alerta:** marca esta casilla para indicar que el texto que aparece en el recuadro inferior, será el texto de la alerta. Escribe en dicho recuadro el texto que debería ser el mensaje. Éste se mostrará cada vez que se detecte un virus.
- **Eliminar mensaje de alerta pasados "N" segundos:** si esta casilla está marcada, se podrá

especificar el tiempo (en segundos) durante el cual se deben mostrar los mensajes de alerta en el puesto.

Por correo electrónico. Esta opción permite avisar de la detección de un virus en un ordenador, a través de mensajes de correo electrónico. Si de desea recibir alertas de virus como mensajes de correo electrónico, se debe marcar la casilla **Enviar alerta a dirección de correo electrónico** y pulsar el botón **Configurar** para indicar el formato de los avisos, mediante las siguientes secciones:

NOTA: el envío de alertas por correo electrónico no está disponible en el caso de la Protección permanente de archivos, para sistemas Windows Me/98/95, pero sí en sistemas Windows XP/2000 Pro/NT.



Dirección

- **Enviar mensaje de alerta a la siguiente dirección:** sirve para indicar que se debe enviar un mensaje de correo electrónico cada vez que se detecte un virus. En dicha casilla se debe introducir la dirección de correo electrónico a la que se enviarán los mensajes de detección de virus.
- **Enviar mensaje de aviso al remitente:** el aviso lo recibirá también el usuario que haya enviado el mensaje infectado, en el caso de que el virus se encuentre en un mensaje de correo electrónico.
- **Enviar mensaje de aviso al resto de los destinatarios:** el aviso lo recibirán también los demás usuarios a los que se les envía el mensaje infectado, en el caso de que el virus se encuentre en un mensaje de correo electrónico.
- **Mensaje de alerta:** es el mensaje que se mostrará cada vez que se detecte un virus.

Protocolo y servidor

- Lista desplegable con los tipos de Protocolo (conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí): en esta lista desplegable, selecciona el tipo de protocolo utilizado para el envío del mensaje de alerta: **MAPI** o **SMTP** (correo saliente).
- **Servidor:** permite escribir el nombre del servidor a través del cual se enviarán los mensajes de alerta.

En la red. Este tipo de mensajes de alerta, sólo existirán en sistemas con Windows XP, Windows 2000 Pro, o Windows NT. Permite enviar avisos sobre la detección de un virus en un determinado ordenador de la red, a todos los conectados también a él a través de dicha red. Si deseas recibir alertas de virus a través de la red, marca la casilla **Enviar alertas a los puestos de la red** y pulsa el botón **Configurar** para indicar el formato de los avisos, mediante las siguientes secciones:

NOTA: el envío de alertas a través de la red a la que está conectado el equipo infectado, no está disponible en el caso de la Protección permanente de archivos.

Analizar

- **Enviar mensaje:** se puede escoger mandar el mensaje de detección de virus a un puesto concreto de la red. Indica en el recuadro inferior, el *puesto* al que se quiere enviar el mensaje de detección de virus.
- **Mensaje de alerta:** es el mensaje que se mostrará cada vez que se detecte un virus.
- **Enviar mensaje al dominio:** se puede escoger mandar el mensaje de detección de virus a todos los puestos pertenecientes a un mismo dominio. Indica en el recuadro inferior, el *dominio* al que se quiere enviar el mensaje de detección de virus.
- **Mensaje de alerta al dominio:** es el mensaje que se mostrará cada vez que se detecte un virus.

Servidor

- **Servidor:** escribe el nombre del servidor a través del cual se enviarán los mensajes de alerta.

En Lotus Notes. Esta opción permite avisar de la detección de un virus en Lotus Notes. El aviso puede ir destinado al autor del documento, al usuario que lo utiliza o a otros usuarios.

Destinatarios: en este cuadro de texto se escribirán, separados por comas, los nombres de los usuarios que recibirán el mensaje de alerta.

Enviar alerta al autor del documento: se notifica la detección al usuario que creó el documento.

Enviar alerta al usuario del documento: se notifica la detección al usuario que trabaja con ese documento.

Mensaje de alerta: texto del mensaje que será enviado como aviso de la detección.

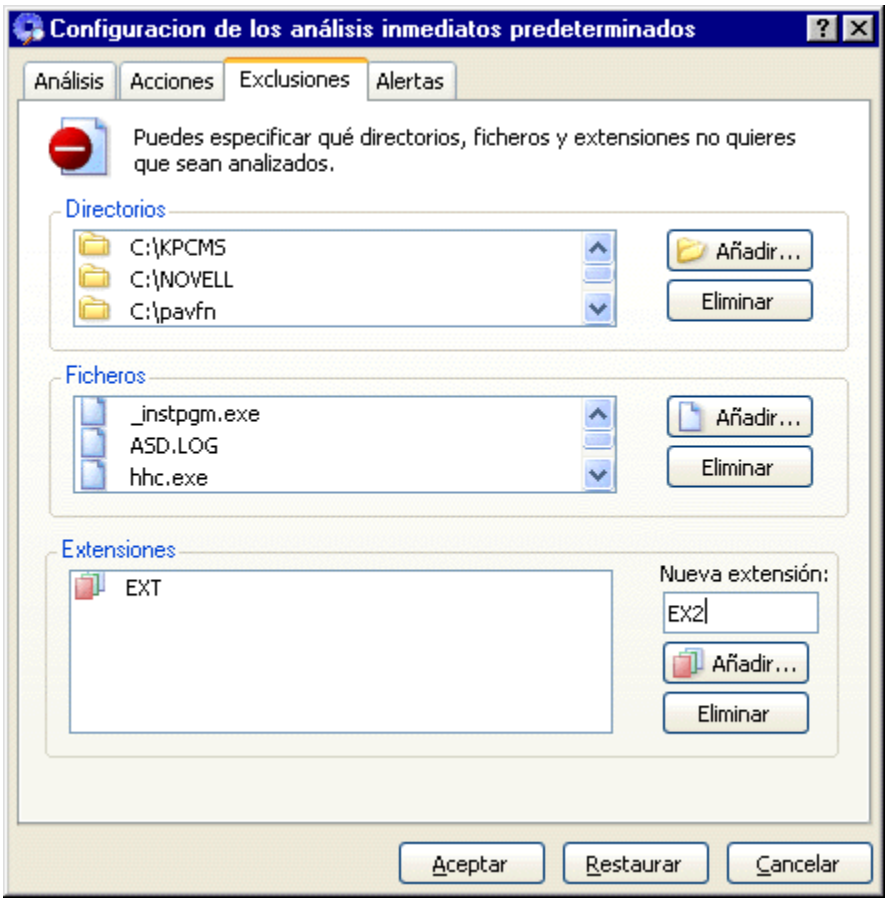
En la parte inferior de las pantallas de configuración de las alertas, aparecen dos botones de interés: **Aceptar** (guarda y aplica los cambios realizados en la configuración) y **Cancelar** (no guarda ni aplica ninguno de los cambios realizados en la configuración).

En la ventana inicial, desde la que es posible indicar los tipos de alertas que se desean activar, también aparecen estos botones y otro adicional: **Restaurar**. Pulsándolo, es posible cargar la configuración por defecto o de fábrica del antivirus. Se preguntará **¿Seguro que desea restaurar la configuración de fábrica?**. Contesta **Sí**, o **No**.

Configuración de los Análisis - Ficha Exclusiones (Inmediatos / Programados / Permanente de Archivos)

La configuración de las exclusiones permite indicar los directorios, ficheros y/o extensiones que el antivirus no debe analizar. A través de esta pestaña es posible determinar cuáles deben ser éstos.

NOTA: esta ficha de configuración, no existe en el caso de la Protección permanente de correo electrónico.



Dentro de esta pestaña de configuración de exclusiones, encontramos tres secciones:

Directorios
Como parte de las exclusiones, se pueden indicar directorios completos para que no sean analizados por el antivirus. Se puede excluir un directorio únicamente o un directorio junto con todos sus subdirectorios.

- **Añadir…:** mediante este botón se accede a una ventana desde la cual es posible indicar los directorios que no se analizarán. A la izquierda encontraremos el *Árbol de Selección* de unidades de disco. Pulse sobre el signo + que se encuentran a la izquierda de una unidad de disco. Se muestra entonces la estructura de directorios de dicha unidad. Para llegar hasta el directorio deseado, iremos abriendo la estructura de directorios correspondiente (camino, ruta o path) y seleccionando el directorio final. Cuando lo tengamos, pulsaremos el botón que contiene una flecha apuntando a la derecha. Cuando hayamos seleccionado todos los directorios deseados,

pulsaremos el botón **Aceptar**. Si se desea obtener más información, se aconseja la consulta del apartado ¿Cómo Preparar las Listas de Exclusiones?, de esta ayuda.

- **Eliminar:** este botón sirve para eliminar directorios de la lista de directorios que no serán analizados. Para hacerlo, seleccionaremos un directorio y pulsaremos el botón **Eliminar**.

Ficheros

En las exclusiones también se pueden añadir ficheros para que no sean analizados por el antivirus. Se puede indicar que no se analice un cierto fichero, o que no se analice ninguna de las ocurrencias de dicho fichero a lo largo de todo el análisis. Es decir, podemos indicar al antivirus que no debe analizar un fichero, y que tampoco debe analizarlo en cada una de las ocasiones que lo vuelva a encontrar, durante ese mismo análisis. Por ejemplo, si tenemos el fichero *EJEMPLO.EXE* en varias localizaciones, podemos excluir sólo alguna de dichas ocurrencias o todas ellas.

- **Añadir…:** mediante este botón se accede a una ventana desde la cual es posible indicar los ficheros que no se analizarán. A la izquierda encontraremos el *Árbol de Selección* de unidades de disco. Pulsaremos sobre el signo + que se encuentran a la izquierda de una unidad de disco. Se muestra entonces la estructura de directorios de dicha unidad. Para llegar hasta el fichero deseado, iremos abriendo la estructura de directorios correspondiente (camino, ruta o path), seleccionando el directorio final y en su interior, el fichero deseado. Cuando lo tengamos, pulsaremos el botón que contiene una flecha apuntando a la derecha. Cuando hayamos seleccionado todos los ficheros que deseamos, pulsaremos el botón **Aceptar**. Si se desea obtener más información, se aconseja la consulta del apartado ¿Cómo Preparar las Listas de Exclusiones?, de esta ayuda.
- **Eliminar:** este botón sirve para eliminar ficheros de la lista de ficheros que no serán analizados. Para hacerlo, seleccionaremos un directorio y pulsaremos el botón **Eliminar**.

Extensiones

También se pueden excluir de los análisis todos aquellos ficheros que tengan una cierta extensión. Es decir, es posible excluir de los análisis determinados tipos de ficheros. Es decir, se trata de indicar que extensiones no deben ser analizadas (que tipos de ficheros no deben ser analizados).

- **Nueva Extensión:** en este cuadro de edición se debe escribir la extensión que se desea incorporar a la lista de extensiones excluidas.
- **Añadir…:** pulsando este botón, la extensión indicada en la caja de edición a tal efecto se añade a la lista de extensiones que no se analizarán.
- **Eliminar:** elimina la extensión seleccionada en la lista (sólo las seleccionadas en ella).

En la parte inferior de las pantallas de configuración, aparecen varios botones de interés:

Aceptar: los cambios realizados en la configuración, se guardarán y se aplicarán.

Restaurar: hace posible seleccionar la configuración establecida por defecto para los análisis. Se preguntará **¿Seguro que desea restaurar la configuración de fábrica?**. Contesta **Sí** (el antivirus vuelve a estar configurado como lo estaba tras su instalación), o **No**.

Cancelar: los cambios realizados en la configuración, no se guardarán ni se aplicarán.

¿Cómo Preparar las Listas de Exclusiones?

La lista de Exclusiones (directorios, ficheros y extensiones que el antivirus no debería analizar) puede ser definida desde la configuración de los análisis. No obstante, la protección permanente de correo, no permite la configuración ni la utilización de las exclusiones.

Desde la ficha de configuración de las exclusiones, podemos preparar y personalizar la lista de elementos (Directorios, Ficheros y Extensiones) que Panda Antivirus Platinum no debería analizar. Para todos los elementos debemos pulsar el botón **Añadir**, con el fin de incluir los elementos deseados en su lista correspondiente de exclusiones.

En el caso de los Directorios y Ficheros, aparecerá un cuadro de diálogo con dos columnas y varios botones entre ambas. La columna de la izquierda, muestra el *Árbol de Selección*. En él seleccionaremos los elementos (Directorios o Ficheros) que no deseamos que el antivirus analice. A la derecha encontraremos la columna *Elementos a Excluir*. Esta otra lista muestra los elementos (Directorios y Ficheros) que acabamos de agregar, para que no sean analizados.

Cómo agregar elementos a la lista de *Elementos a Excluir*

1. Utilizando los signos + que aparecen a la izquierda de cada unidad de disco y directorio, se irá abriendo la ruta de directorios, hasta llegar al elemento deseado (Directorio o Fichero).
2. Cuando se haya seleccionado éste, se debe pulsar el botón  . Entonces, el elemento marcado en el *Árbol de Selección*, pasará a la lista de *Elementos a Excluir*.

Cómo eliminar elementos de la lista de *Elementos a Excluir*

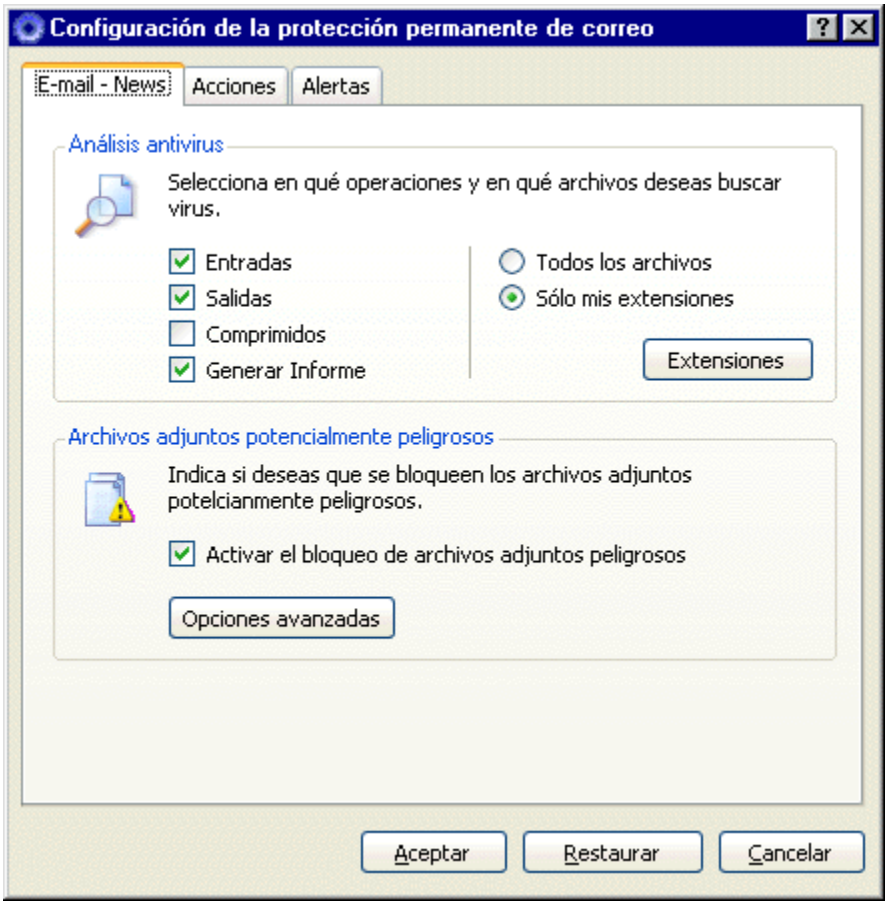
1. Se debe seleccionar un elemento (Directorio o Fichero) en la lista de *Elementos a Excluir*.
2. Para eliminar de ella solamente los elementos marcados, se debe pulsar el botón  .

   Si se desea eliminar de ella todos los elementos, se debe pulsar el botón 

La exclusión de extensiones funciona de forma diferente. Con sólo escribir la extensión a excluir en el cuadro **Nueva extensión** y pulsar el botón **Añadir**, ésta se agregará a la lista final de exclusiones.

Configuración de los Análisis - Ficha E-mail - News (Permanente de Correo)

Dentro de este apartado se engloban las opciones de configuración correspondientes al análisis del correo electrónico y de los grupos de noticias.



Analizar antivirus
Mediante las opciones existentes en esta sección, podrás indicar cuáles son las operaciones que el análisis permanente debe controlar, así como los tipos de ficheros que deben ser analizados:

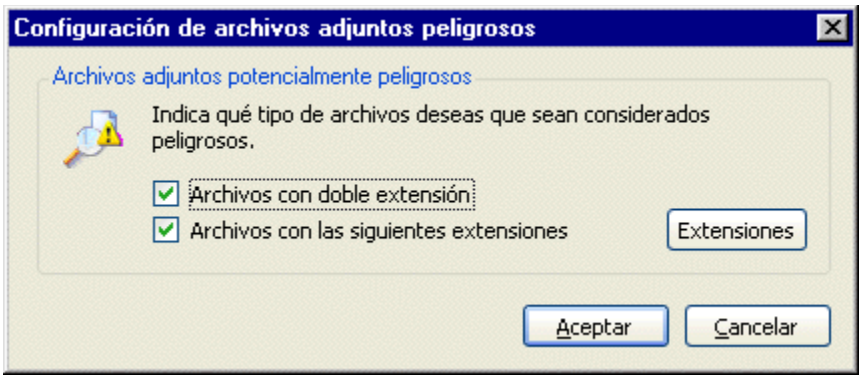
- **Entradas:** indica que se analizarán todas las entradas de correo electrónico (mensajes que se reciban).
- **Salidas:** indica que se analizarán todas las salidas de correo electrónico (mensajes que se envíen).
- **Comprimidos:** indica que se analizarán todos los ficheros comprimidos que se encuentren asociados a cualquier mensaje que se analice.
- **Generar informe:** si se marca esta opción, los datos relativos al análisis en cuestión se registrarán en el informe.
- **Todos los ficheros:** seleccionando esta opción se analizarán todos los ficheros independientemente de su extensión.
- **Sólo mis extensiones:** esta opción permite indicar que se deben analizar todos aquellos ficheros cuya extensión se encuentre en una lista. A esta lista se accede mediante el botón **Extensiones**. Si deseas obtener más información, consulta el apartado Lista de Extensiones a Analizar, de esta

ayuda.

Archivos adjuntos potencialmente peligrosos

Mediante esta sección de la ficha, puedes indicar si deseas que la protección permanente de correo bloquee los ficheros adjuntos que considere peligrosos (si están incluidos en mensajes de correo electrónico).

- **Activar el bloqueo de archivos adjuntos peligrosos:** marca esta casilla para que la protección permanente bloquee los archivos que considere peligrosos, siempre que estos estén incluidos en un mensaje de correo electrónico (adjuntos).
- Botón **Opciones avanzadas:** pulsa este botón para determinar cuáles son los archivos que deben considerarse como peligrosos. Tienes estas posibilidades:



Archivos con doble extensión: serán bloqueados (siempre que tengas marcada la casilla **Activar el bloqueo de archivos adjuntos peligrosos**), los ficheros que tengan dos extensiones (por ejemplo, NOMBRE.EXE.VBS).

Archivos con las siguientes extensiones: serán bloqueados (siempre que tengas marcada la casilla **Activar el bloqueo de archivos adjuntos peligrosos**), los tipos de ficheros cuya extensión incluyas en la lista, pulsando el botón **Extensiones**.

En la parte inferior de las pantallas de configuración, aparecen varios botones de interés:

Aceptar: los cambios realizados en la configuración, se guardarán y se aplicarán.

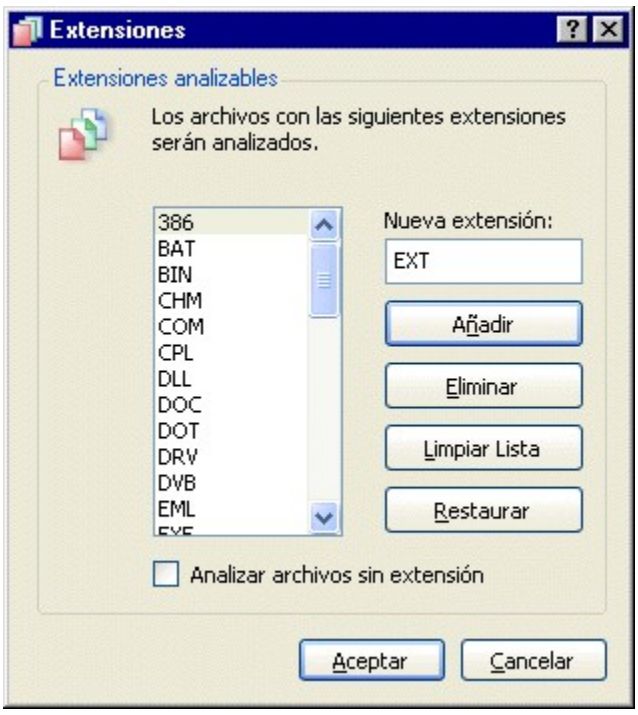
Restaurar: hace posible seleccionar la configuración establecida por defecto para los análisis. Se preguntará **¿Seguro que desea restaurar la configuración de fábrica?**. Contesta **Sí** (el antivirus vuelve a estar configurado como lo estaba tras su instalación), o **No**.

Cancelar: los cambios realizados en la configuración, no se guardarán ni se aplicarán.

Configuración de las Extensiones a Analizar

Tu Panda Antivirus Platinum cuenta con una lista de extensiones creada por defecto de fábrica. En ella se engloban todas las extensiones (tipos de ficheros) que el antivirus debe chequear durante sus análisis.

En cualquier momento, puedes agregar a ésta otros tipos de extensiones, o eliminar de ella cualquiera de los tipos ya incluidos. Esto es posible hacerlo a través de la configuración de los análisis (inmediatos, programados, permanentes,…), marcando la casilla **Sólo mis extensiones** y pulsando el botón **Extensiones**.



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**.

Analizar ficheros sin extensión. Marca esta casilla de verificación si lo que deseas es que el antivirus analice también los ficheros que tienen nombre pero no extensión (además de aquellos cuya extensión se encuentra en la lista).

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

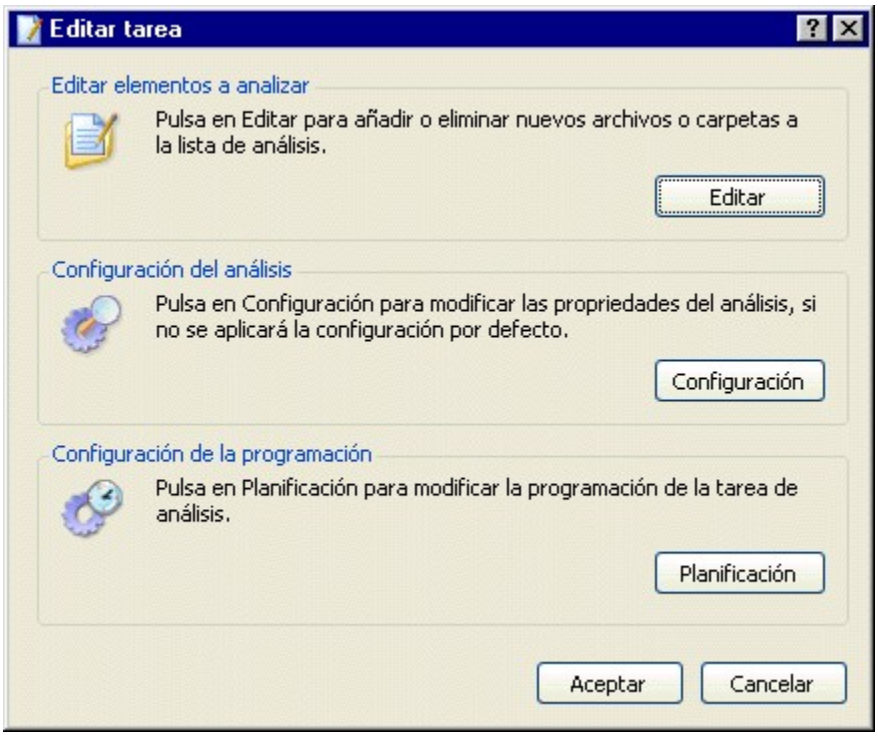
Configuración de los Análisis - Ficha Programador (Programados)

El programador tiene como objeto establecer la periodicidad con que se ejecutará un cierto análisis programado (ya sea al inicio del sistema -sólo en el caso de Windows 98/95-, de Windows, o uno que haya sido creado por el usuario). Por un lado habrá que indicar la periodicidad o frecuencia y por otro lado, el rango de fechas durante el cual estará activo el análisis programado en cuestión.

La forma de acceder a las opciones de configuración del **Programador** son iguales, tanto si se trata de un análisis programado predefinido de antemano, como si se trata de un análisis programado que el usuario (nosotros mismos) ha creado.

- Utilizando el panel **Tareas de análisis**. Selecciona el análisis programado predefinido de antemano (al inicio del sistema -sólo en el caso de Windows 98/95-, o al inicio de Windows) y pulsa la opción **Editar análisis**, en el panel de **Tareas de análisis**.
- Utilizando el menú contextual. Pulsa con el botón derecho del ratón sobre el análisis programado predefinido de antemano (al inicio del sistema o al inicio de Windows). Entonces, selecciona la opción **Editar**.

También el cuadro de diálogo que se muestra presenta las mismas posibilidades, tanto para el caso de análisis programados predefinidos de antemano, como para los análisis programados que haya creado el usuario (nosotros mismos):



- **Editar elementos a analizar.** Pulsa el botón **Editar**, si lo que deseas es modificar (agregar o quitar) los elementos que el análisis seleccionado debería analizar. Puedes obtener más información sobre los elementos a analizar, en la sección ¿Cómo Realizar un Análisis? (Inmediato / Programado) de esta ayuda.

- **Configuración del análisis.** Pulsa el botón **Configuración**, si lo que deseas es definir las características generales del análisis, acciones que debe realizar, exclusiones y alertas (dependiendo del tipo de análisis). Puedes obtener más información sobre la configuración, en la sección ¿Cómo Configurar un Análisis? (Inmediato / Programado / Permanente) de esta ayuda.
- **Configuración de la programación.** Pulsa el botón **Planificación**. De este modo podrás determinar cuándo y cómo debe ejecutarse este análisis programado. Esto mostrará una ficha u otra en función del tipo de análisis programado del que se trate (predefinido de antemano -al inicio del sistema y al inicio de Windows-, o análisis programados creados por el usuario).

  Las diferencias en la configuración de la programación / planificación, entre los análisis programados predefinidos de antemano (inicio del sistema -sólo en equipos con Windows 98/95- e inicio de Windows) y los análisis programados creados por los usuarios (los que nosotros hayamos creado), se puede apreciar cuando se pulsa el botón **Planificación**.

  Programación de análisis programados predefinidos (inicio del sistema y de Windows)
  Programación de análisis programados creados por los usuarios

¿Cómo Editar o Modificar un Análisis? (Inmediato / Programado)

Además de permitir la creación de nuevas tareas de análisis (tanto inmediatas como programadas), Panda Antivirus Platinum, trata cada uno de los análisis que creamos, como tareas de análisis que podemos configurar, modificar (editar) y borrar (eliminar). Una vez que hayamos creado una determinada tarea de análisis (ya sea ésta inmediata o programada), con una determinadas características de funcionamiento, podremos modificarlas haciendo lo siguiente:

1. En la lista de análisis, selecciona el análisis definido por el usuario, que deseas modificar. Éste puede ser uno de los análisis programados, o un análisis inmediato predefinido por el usuario.
2. Selecciona la opción **Editar análisis** (para los análisis programados) / **Configurar** (para los análisis inmediatos) existente en el panel de control **Tareas de análisis**, o la que está accesible al pulsar con el botón derecho del ratón sobre el análisis á modificar.
3. Aparece un cuadro de diálogo, con las siguientes secciones:

    - **Editar elementos a analizar** (para tareas inmediatas y en los programadas). Si pulsas el botón **Editar**, verás la lista de todos los elementos (memoria, discos,…) que el análisis seleccionado, debe analizar. Podrás agregar a ella cualquier otro elemento mediante el botón **Añadir**, para que éste sea analizado. También puedes hacer que alguno de los elementos de la lista no sea analizado, seleccionándolo y pulsando el botón **Quitar**.

      Si deseas añadir un nuevo elemento a la lista, pulsa **Añadir** y utilice los signos + que aparecen en la lista (o árbol). Selecciona uno a uno los elementos que deseas analizar y pulsa el botón **Aceptar**. Esto los irá agregando uno a uno a la lista total de elementos a analizar.

    - **Configuración del análisis** (para tareas inmediatas y en los programadas). Si pulsas el botón **Configurar**, podrás determinar todas las propiedades del análisis. Aunque tienen opciones comunes, dichas características de configuración serán diferentes si se trata de un análisis inmediato o programado. Puedes consultar más información sobre la configuración de los análisis o tareas de análisis en el apartado ¿Cómo Configurar un Análisis? (Inmediato / Programado), de esta ayuda.

    - **Configuración de la programación** (sólo para tareas programadas, no inmediatas). Sí el análisis que estás editando es programado, además aparecerá esta sección. A través de ella puedes modificar las características periódicas, particulares de los análisis programados. Si pulsas el botón **Planificación**, aparecerá la ficha **Programador**, correspondiente a la configuración de los análisis programados. Puedes consultar más información sobre la configuración de los análisis o tareas de análisis en el apartado Configuración de los Análisis - Ficha Programador (Programados), de esta ayuda.

4. Cuando finalices la edición de las características del análisis, pulsa el botón **Aceptar** para que los cambios realizados se apliquen. Si pulsas el botón **Cancelar**, los cambios en la edición de las propiedades del análisis, no tendrán efecto.

¿Cómo Borrar o Eliminar un Análisis? (Inmediato / Programado)

Ya sabemos que los análisis inmediatos y programados se pueden considerar como tareas de análisis y que cada una de ellas se puede crear (no los que están predeterminados), editar (no los que están predeterminados), configurar (no los que crea el usuario)… Además, podremos eliminar cualquiera de las tareas inmediatas o programadas que nosotros mismos hayamos creado, pero nunca las tareas predefinidas de antemano.

Para eliminar o borrar alguno de los análisis personalizados que se hayan creado, debes hacer los siguiente:

1. En la lista de análisis (ya sean éstos inmediatos o programados), selecciona el análisis creado que deseas eliminar.
2. En el panel de control **Tareas de análisis**, pincha sobre la opción **Eliminar análisis**. También puedes hacerlo, pulsando sobre la misma opción en el menú contextual (botón derecho del ratón sobre el análisis a borrar).
3. Se solicita confirmación para eliminar la tarea de análisis seleccionada. Contesta afirmativa o negativamente, pulsando el botón **Sí** o **No** respectivamente.

¿Cómo Activar / Desactivar el Análisis o Protección Permanente?

Tras la instalación de Panda Antivirus Platinum, la Protección permanente (Antivirus -de archivos y de correo- y Firewall) se encuentra siempre activa. Esto asegura nuestra protección continua, inmediatamente después de la instalación del antivirus. Ten en cuenta que si esta protección permanente no se encuentra activa, no estarás protegido contra los virus.

Como sabemos, la Protección permanente cuenta con varios tipos de tareas: *Protección Antivirus - correo* (continua protección antivirus respecto a todas las transferencias de mensajes y ficheros a través de correo electrónico) y *archivos* (continua protección antivirus respecto a todos los archivos que se utilizan en el sistema), así como la *Protección firewall* (continua protección de los programas que pueden acceder a Internet, bloqueos de ataques, etc).

Cuando una o varias o todas las Protecciones permanentes (Protección Antivirus -de correo y e archivos- y Protección Firewall) se encuentran cargadas, se muestra el icono de Panda Antivirus Platinum en la *Barra de tareas de Windows* (junto al reloj del sistema). Desde él también es posible activar y desactivar (además de configurar) cada una de las Protecciones permanentes (residentes). Si deseas obtener más información sobre el icono de Panda Antivirus Platinum en la *Barra de tareas de Windows*, te aconsejamos la consulta el apartado Operaciones Desde la *Barra de Tareas de Windows*, de esta ayuda.

En cualquier momento, y de diversas formas, podremos desactivar y activar cada una de dichas Protecciones permanentes (*Antivirus -de correo* y *de archivos- y Firewall*).

¿Cómo Activar / Desactivar la Protección Permanente Antivirus de archivos?

Es posible activar / desactivar la Protección permanente Antivirus de archivos (residente de archivos), desde la ventana del antivirus, o desde el icono correspondiente a la protección permanente en la *Barra de tareas de Windows*. Ten en cuenta que si esta protección permanente no se encuentra activa, no estarás protegido contra los virus.

Para activar o desactivar la protección desde la ventana del antivirus, hazlo siguiente:

1. En la ventana del antivirus, selecciona la opción **Protección permanente**, del **Panel de control**.
2. Pulsa el botón **Configurar,** en el panel Antivirus..
3. En la sección **Protección permanente de archivos**, marca / desmarca la casilla **Activado**.
4. Pulsa el botón **Aceptar**.

También puedes activar o desactivar dicha protección desde el icono del antivirus en la *Barra de tareas de Windows* (junto al reloj). Si el icono del antivirus aparece en la *Barra de tareas de Windows* y tiene color, indicará que una, varias o todas las Protecciones permanentes, se encuentra activa (al menos una de ellas). Sin embargo, si el icono aparece en tonos grises, indicará que las protecciones están desactivadas. Para activar o desactivar dichas protecciones desde el icono de la *Barra de tareas de Windows*, haz lo siguiente:

1. Pulsa con el botón derecho del ratón, sobre el icono de la *Barra de tareas de Windows*.
2. Selecciona la opción **Configurar protección permanente**. Esto abre un cuadro de diálogo como el siguiente.

La opción de configuración del firewall incluido en Panda Antivirus Platinum solamente estará disponible si lo has instalado.

3. En la sección **Protección permanente de archivos**, marca la casilla **Activado** o desmárcala (en función de lo que quiera hacer). Además, si deseas configurar el funcionamiento de esta protección de archivos, pulsa el botón **Configurar**.

En cualquiera de los casos (activación / desactivación mediante las opciones en la ventana del antivirus, o desde el icono en la *Barra de tareas*), se indicará (en la sección inferior del panel central), que la **Protección permanente** de **antivirus de archivos** está *Inactiva* o *Activa*.

Para volver a activar la protección, realiza los mismos pasos que llevaste a cabo para desactivarla. Cuando lo hayas hecho, se indicará (en la sección inferior del panel central), que la **Protección permanente** de **antivirus de archivos** está *Activa*.

¿Cómo Activar / Desactivar la Protección Permanente Antivirus de Correo?

Es posible activar / desactivar la Protección permanente Antivirus de correo (residente de correo), desde la ventana del antivirus, o desde el icono correspondiente a la protección permanente en la *Barra de tareas de Windows*. Ten en cuenta que si esta protección permanente no se encuentra activa, no estarás protegido contra los virus.

Para activar o desactivar la protección desde la ventana del antivirus, hazlo siguiente:

1. En la ventana del antivirus, selecciona la opción **Protección permanente**, del **Panel de control**.
2. Pulsa el botón **Configurar**, en el panel **Antivirus**.
3. En la sección **Protección permanente de correo**, marca / desmarca la casilla **Activado**.
4. Pulsa el botón **Aceptar**.

También se puede activar o desactivar dicha protección desde el icono del antivirus en la *Barra de tareas de Windows* (junto al reloj). Si el icono del antivirus aparece en la *Barra de tareas de Windows* y tiene color, indicará que una, varias o todas las Protecciones permanentes, se encuentra activa (al menos una de ellas). Sin embargo, si el icono aparece en tonos grises, indicará que ambas protecciones están desactivadas.

Para activar o desactivar dichas protecciones desde el icono de la *Barra de tareas de Windows*, haz lo siguiente:

1. Pulsa con el botón derecho del ratón, sobre el icono de la *Barra de tareas de Windows*.
2. Selecciona la opción **Configurar protección permanente**. Esto abre un cuadro de diálogo como el siguiente.

La opción de configuración del firewall incluido en Panda Antivirus Platinum solamente estará disponible si lo has instalado.

3. En la sección **Protección permanente de correo**, marca la casilla **Activado** o desmárcala (en función de lo que quieras hacer). Además, si deseas configurar el funcionamiento de esta protección de correo, pulsa el botón **Configurar**.

En cualquiera de los casos (activación / desactivación mediante las opciones en la ventana del antivirus, o desde el icono en la *Barra de tareas*), se indicará (en la sección inferior del panel central), que la **Protección permanente** de **antivirus de archivos** está *Inactiva* o *Activa*.

Para volver a activar la protección, realiza los mismos pasos que llevaste a cabo para desactivarla. Cuando lo hayas hecho, se indicará (en la sección inferior del panel central), que la **Protección permanente** de **antivirus de correo** está *Activa*.

¿Cómo Activar / Desactivar la Protección Permanente Firewall?

Es posible activar / desactivar la Protección permanente firewall, desde la ventana del antivirus, o desde el icono correspondiente a la protección permanente en la *Barra de tareas de Windows*. Ten en cuenta que si esta protección permanente no se encuentra activa, no estarás protegido contra los virus.

Para activar o desactivar la protección desde la ventana del antivirus, hazlo siguiente:

1. En la ventana del antivirus, selecciona la opción **Protección permanente**, del **Panel de control**.
2. Pulsa el botón **Configurar** en el panel **Firewall**.
3. Marca / desmarca la casilla **Activado**.
4. Pulsa el botón **Aceptar**.

También puedes activar o desactivar dicha protección desde el icono del antivirus en la *Barra de tareas de Windows* (junto al reloj). Si el icono del antivirus aparece en la *Barra de tareas de Windows* y tiene color, indicará que una, varias o todas las Protecciones permanentes, se encuentran activas (al menos una de ellas). Sin embargo, si el icono aparece en tonos grises, indicará que las protecciones están desactivadas. Para activar o desactivar dichas protecciones desde el icono de la *Barra de tareas de Windows*, haz lo siguiente:

1. Pulsa con el botón derecho del ratón, sobre el icono de la *Barra de tareas de Windows*.
2. Selecciona la opción **Configurar protección permanente**. Esto abre un cuadro de diálogo como el siguiente.

La opción de configuración del firewall incluido en Panda Antivirus Platinum solamente estará disponible si lo has instalado.

3. En la sección **Protección permanente firewall**, marca la casilla **Activado** o desmárcala (en función de lo que quiera hacer). Además, si deseas configurar el funcionamiento de esta protección de archivos, pulsa el botón **Configurar**.

En cualquiera de los casos (activación / desactivación mediante las opciones en la ventana del antivirus, o desde el icono en la *Barra de tareas*), se indicará (en la sección inferior del panel central), que la **Protección permanente** de **firewall** está *Inactiva* o *Activa*.

Para volver a activar la protección, realiza los mismos pasos que llevaste a cabo para desactivarla. Cuando lo hayas hecho, se indicará (en la sección inferior del panel central), que la **Protección permanente** de **firewall** está *Activa*.

Además de Activar / Desactivar, desde una de las opciones accesibles mediante el icono del antivirus en la *Barra de tareas de Windows*, es posible cerrar la Protección permanente. Esto se puede hacer del siguiente modo:

1. Pulsa con el botón derecho del ratón sobre el icono del antivirus en la *Barra de tareas de Windows*.
2. Selecciona la opción **Cerrar protección permanente**.
3. Se solicita confirmación para cerrar las dos Protecciones permanentes (o residentes), de Antivirus (archivos y de correo) y Firewall.
4. Si contestas afirmativamente (**Sí**), se desactivarán automáticamente ambas protecciones y el icono del antivirus en la *Barra de tareas de Windows* desaparecerá. Solamente se podrán volver a activar desde la ventana del antivirus (sección **Protección Permanente**, opciones **Activar**, en cada uno de los paneles de control correspondientes.

Configuración General del Antivirus

Mediante la configuración general del antivirus es posible determinar de forma centralizada, cada una de las distintas capacidades, posibilidades o características de funcionamiento con las que éste puede trabajar.

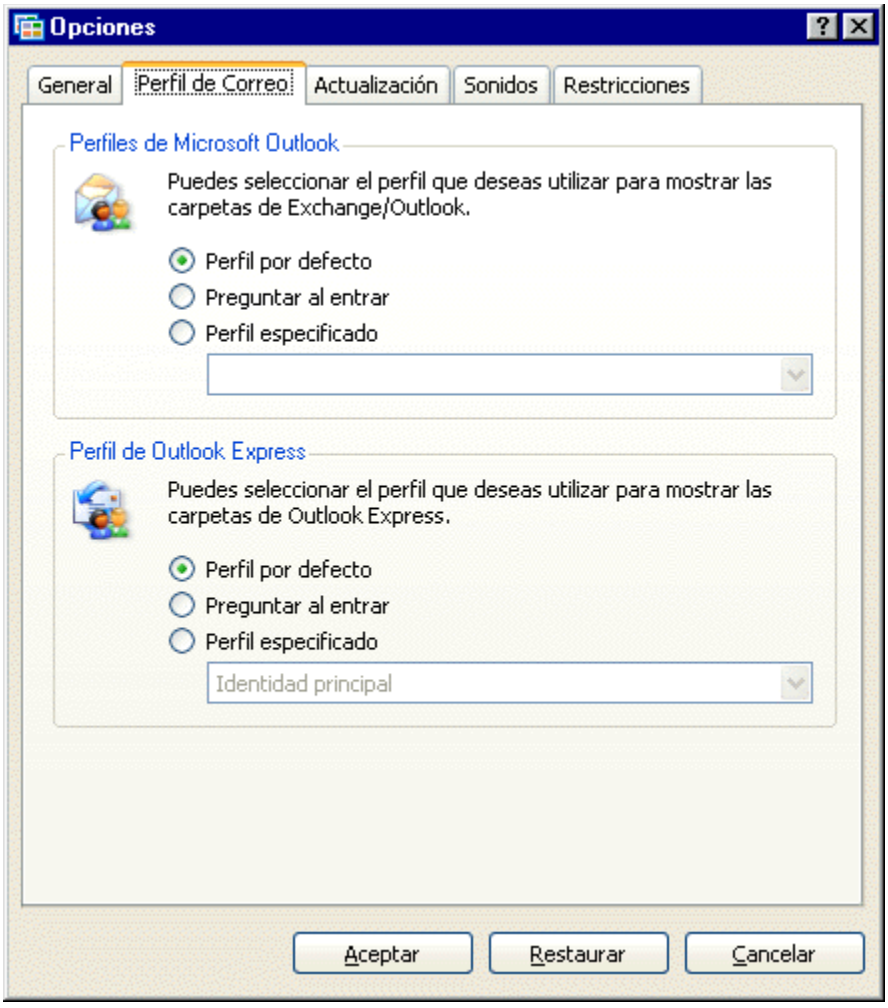
Desde este apartado se pueden configurar un conjunto de opciones generales, las opciones de actualización y los perfiles de correo electrónico (Microsoft Outlook y Microsoft Outlook Express). Asimismo, son configurables los sonidos que presentará el antivirus y la contraseña de acceso a las opciones del programa, así como otras características de carácter general (elementos analizables, control de carga de la CPU, o análisis de Boot).

Para acceder a la configuración general del antivirus, pulse el botón **Opciones generales** que se encuentra en la barra de herramientas de la ventana de Panda Antivirus Platinum. Esto mostrará un cuadro de diálogo en el que aparecen varias fichas. Cada una de ellas permite determinar las características de funcionamiento del antivirus en determinados aspectos. Éstas son las siguientes:

Configuración General del Antivirus - Perfil de Correo

Panda Antivirus Platinum es capaz de mostrar las carpetas que contienen los mensajes de correo electrónico de los programas Microsoft Outlook y Microsoft Outlook Express con el fin de que éstas se puedan seleccionar para realizar un análisis sobre ellas. Estos programas de correo electrónico permiten tener definidos varios perfiles y cada uno con sus características. Gracias a esta pestaña de configuración, es posible indicarle al antivirus cuál de los perfiles existentes en cada caso, debe escoger.

Para cada uno de los casos o aplicaciones de correo electrónico (tanto Microsoft Outlook, como Microsoft Outlook Express), las opciones de configuración son las mismas, disponiéndose en dos secciones separadas: **Perfiles de Microsoft Outlook** y **Perfiles de Outlook Express**.



- **Perfil por defecto.** Esta opción indica que se abrirá el perfil por defecto de acuerdo con la configuración con la que cuente el programa de correo electrónico Microsoft Outlook, o Microsoft Outlook Express.
- **Preguntar al entrar.** Esta opción provoca que el antivirus pregunte por el perfil que debe abrir, ofreciendo una lista de todos los perfiles definidos en el programa de correo electrónico Microsoft Outlook y Microsoft Outlook Express.

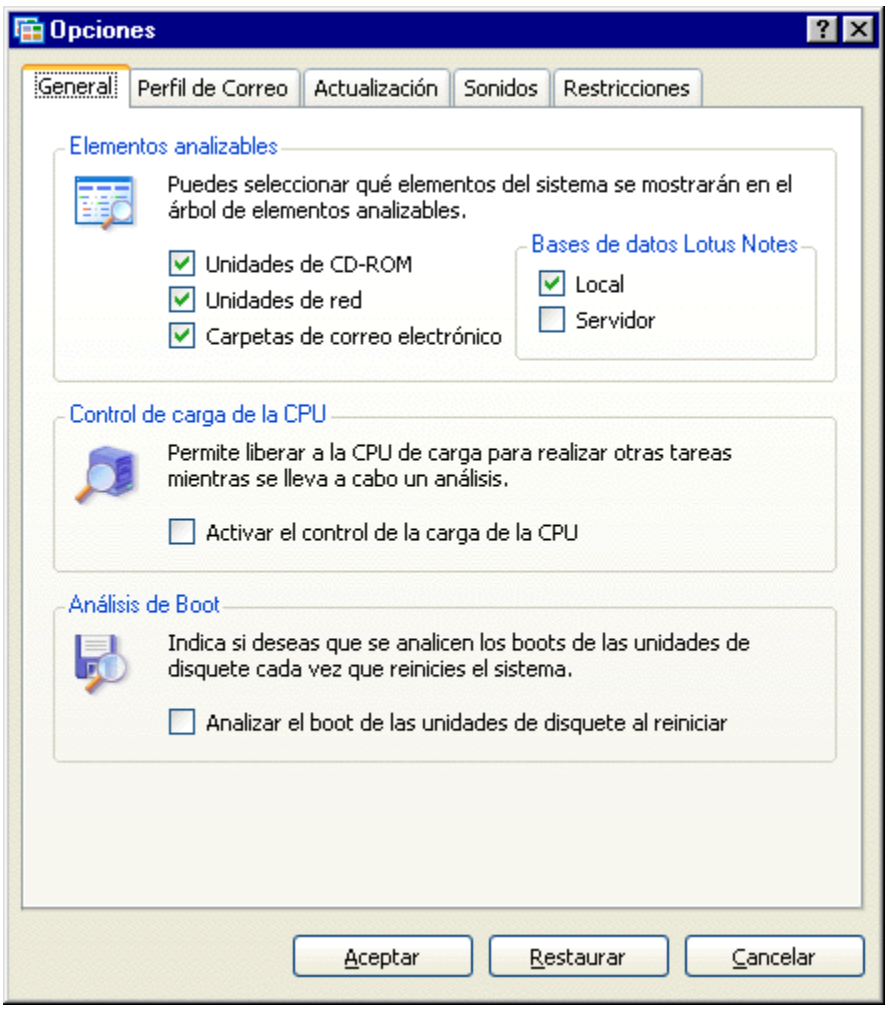
- **Perfil especificado.** Gracias a esta opción se puede indicar un perfil concreto para que el antivirus siempre trabaje con él.

La lista desplegable que aparece en cada una de las secciones (*Perfiles de Microsoft Outlook* y *Perfiles de Outlook Express*), permite indicar cuál es ese perfil con el que se desea trabajar (siempre que se haya marcado la casilla **Perfil especificado**).

En la sección inferior de esta ficha aparecen varios botones. Pulsando el botón **Aceptar**, se guardan los cambios realizados en la ficha. Pulsando el botón **Restaurar** se vuelven a cargar en la ficha los valores que estaban establecidos en ella por defecto, tras la instalación inicial del antivirus. Si se pulsa el botón **Cancelar**, ninguno de los cambios realizados en la lista, serán almacenados ni tenidos en cuenta.

Configuración General del Antivirus - General

El apartado de configuración general permite indicar qué elementos de los que se citan a continuación se desea que aparezcan en el árbol de selección de elementos a analizar. Esta opción afectará a todas aquellas partes del programa en las que se presenten las posibles áreas de análisis. Su configuración es accesible a través de la ficha **General**, que se muestra al pulsar el botón **Opciones generales**, de la barra de herramientas del antivirus.



Elementos analizables. Selecciona, de entre los posibles, cada uno de los elementos que deseas se muestren en las listas de elementos que es posible seleccionar para realizar un análisis.

- **Unidades de CD-ROM.** Cuando esta casilla está marcada, indica que se deben mostrar las unidades de CD-ROM. Si se desmarca, éstas no se mostrarán en las listas de elementos a analizar.
- **Unidades de red.** Cuando esta casilla está marcada, indica que se deben mostrar las unidades de red (unidades de disco accesibles desde los ordenadores de la red). Si se desmarca, éstas no se mostrarán en las listas de elementos a analizar.
- **Carpetas de correo electrónico.** Cuando esta casilla está marcada, indica que se deben mostrar

las carpetas de correo electrónico (correspondientes a los programas Microsoft Outlook y Microsoft Express). Si se desmarca, éstas no se mostrarán en las listas de elementos a analizar.

- Bases de datos de Lotus Notes - **Local.** Cuando esta casilla está marcada, indica que se deben mostrar las bases de datos y elementos de Lotus Notes, que se encuentran en nuestro ordenador (de forma local, donde está instalado el antivirus).
- Bases de datos de Lotus Notes - **Servidor.** Cuando esta casilla está marcada, indica que se deben mostrar las bases de datos y elementos de Lotus Notes, que se encuentran en el servidor de bases de datos de Lotus Notes.

Control de carga de la CPU. Marcando la casilla **Activar el control de la carga de la CPU**, se libera parte del trabajo de la CPU y se agiliza la realización de otras tareas durante los análisis.

Análisis de Boot

El sector de arranque o Boot de los disquetes que se encuentren en la disquetera cuando el ordenador se apaga o se reinicia, son analizados automáticamente siempre que esta casilla de verificación esté marcada. Si no deseas el análisis del Boot de los disquetes en estas situaciones, desmarca la casilla **Analizar el boot de las unidades de disquete al reiniciar**.

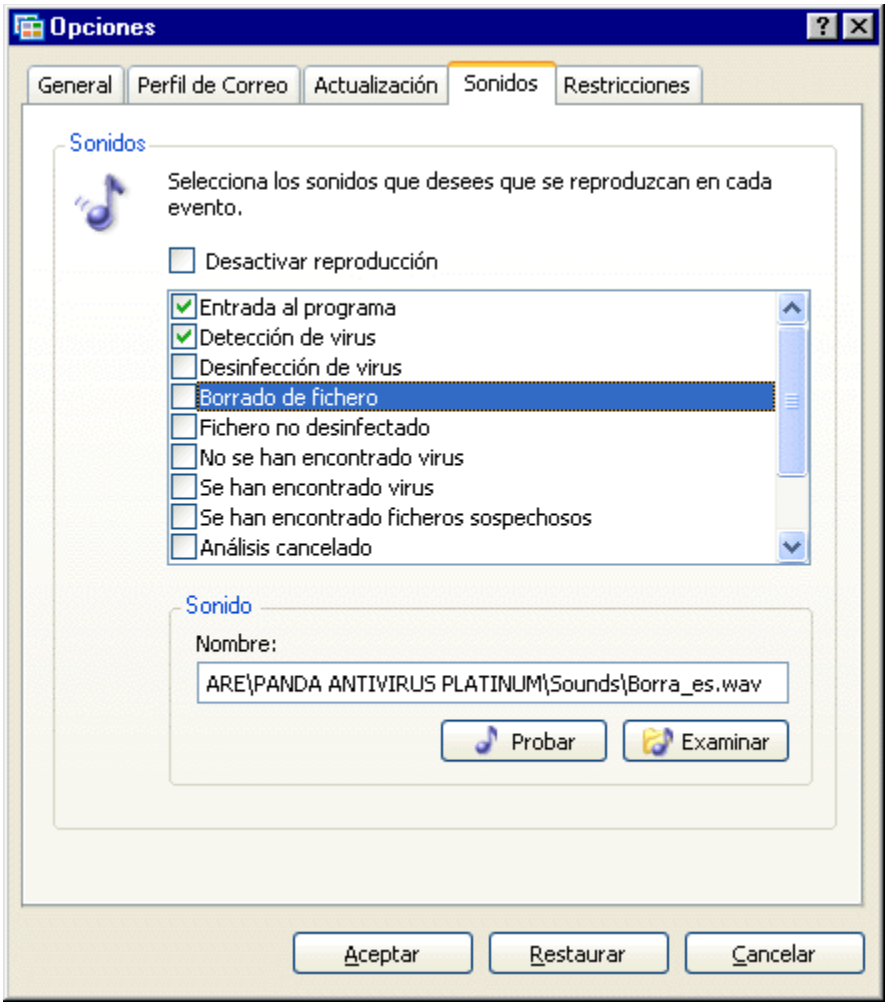
En la sección inferior de esta ficha aparecen varios botones. Pulsando el botón **Aceptar**, se guardan los cambios realizados en la ficha. Pulsando el botón **Restaurar** se vuelven a cargar en la ficha los valores que estaban establecidos en ella por defecto, tras la instalación inicial del antivirus. Si se pulsa el botón **Cancelar**, ninguno de los cambios realizados en la lista, serán almacenados ni tenidos en cuenta.

Sistemas Operativos

Esta opción solamente aparece en el caso de equipos con Windows XP, o Windows Millennium. Si se marca, la carpeta *Restore*, no será incluida en los análisis que se realicen.

Configuración General del Antivirus - Sonidos

Es posible determinar y definir los sonidos que Panda Antivirus Platinum debe emitir en determinadas circunstancias. El apartado de sonidos tiene como objeto permitir elegir qué sucesos del antivirus irán acompañados de sonidos. Para cada suceso se puede escoger el sonido que se oirá cuando el suceso se produzca. Además y para completar la funcionalidad de este apartado, un botón permite oír cada sonido para elegir el deseado. Para acceder a la configuración de los sonidos del antivirus, se debe acceder a la ficha **Sonidos**, a través del botón **Opciones generales**, en la barra de herramientas del antivirus. Esto mostrará la siguiente ficha.



En ella selecciona los sonidos que deseas se reproduzcan en cada evento: los sucesos que se muestran en esta lista pueden asociarse a un sonido. De esta forma, cada vez que se produzca el suceso se reproducirá el sonido indicado. Si se quiere que un determinado suceso vaya acompañado de un sonido, deberá marcarse el suceso. Si se desea el efecto contrario, el suceso deberá desmarcarse.

Desactivar Reproducción: si se marca esta casilla, el antivirus dejará de reproducir los sonidos asociados a cada uno de los eventos en la lista. Es decir, el antivirus no emitirá ningún sonido, en ningún caso.

Nombre: es el nombre del fichero de sonido (fichero tipo *WAV*) que se quiere asociar a un cierto suceso, que se encuentra seleccionado en la lista en ese instante.

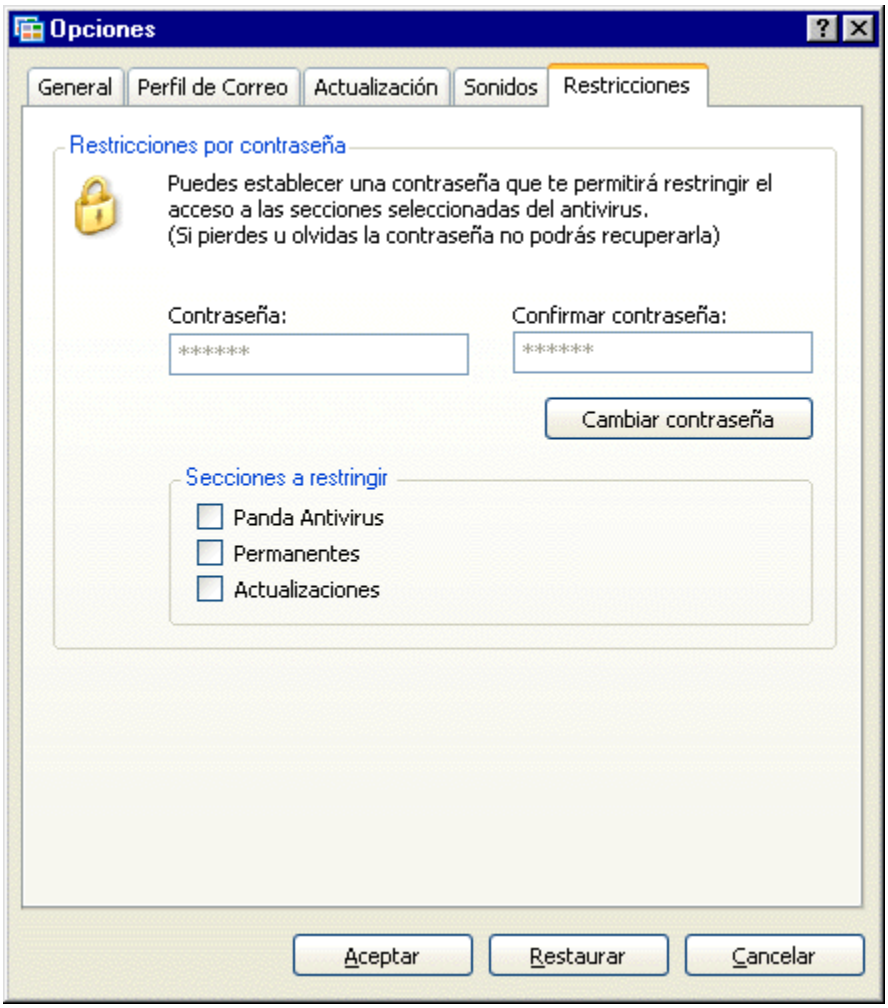
Botón **Examinar:** este botón muestra la ventana estándar de elección de ficheros para escoger el fichero de sonido (tipo *WAV*) que se desea asociar a un cierto suceso.

Botón **Probar:** pulsando este botón se reproducirá el sonido que se haya escogido para poder así probarlo sin necesidad de provocar el suceso concreto al que esté asociado el sonido.

En la sección inferior de esta ficha aparecen varios botones. Pulsando el botón **Aceptar**, se guardan los cambios realizados en la ficha. Pulsando el botón **Restaurar** se vuelven a cargar en la ficha los valores que estaban establecidos en ella por defecto, tras la instalación inicial del antivirus. Si se pulsa el botón **Cancelar**, ninguno de los cambios realizados en la lista, serán almacenados ni tenidos en cuenta.

Configuración General del Antivirus - Restricciones

Este apartado permite proteger, mediante una contraseña el acceso, determinadas secciones, apartados o elementos del antivirus. Con ello se garantiza que dichas secciones no sean alterados por nadie, sin tu permiso. Para indicar o asociar contraseñas a determinadas secciones del antivirus (análisis programados, al inicio, permanentes,…), accede a la ficha **Restricciones**, pulsando el botón **Opciones generales** en la barra de herramientas del antivirus. Esto muestra una pantalla como la siguiente.



Secciones a restringir. Presenta los distintos apartados, secciones o elementos del antivirus que se van a proteger mediante una cierta contraseña. Es posible seleccionar cada uno de ellos, marcando la casilla de verificación que aparece a su izquierda.

- **Panda Antivirus:** marcando esta casilla, se evita la manipulación de todo el antivirus, de todo Panda Antivirus Platinum.
- **Permanentes:** protegiendo este apartado, se puede evitar que una persona no autorizada pueda cambiar la configuración o incluso desactivar la Protección permanente (Protección de correo y Protección de archivos).
- **Actualizaciones:** se puede bloquear el acceso a esta parte del antivirus para que nadie altere los

datos introducidos, necesarios para la realización de las actualizaciones del antivirus.

Contraseña. Permite introducir una contraseña para proteger los elementos que se hayan escogido.

- **Contraseña:** Escribe la contraseña que deseas asignar o que ya tienes asignada.
- **Confirmar contraseña:** Repite la contraseña que has escrito en el recuadro **Contraseña**.

Si deseas establecer una nueva contraseña, pulsa el botón **Cambiar contraseña**. Entonces, se mostrarán las siguientes opciones:

- **Introduce la contraseña anterior:** Si anteriormente has indicado alguna contraseña, puedes cambiarla por una nueva, pero previamente debes escribir la contraseña anterior en esta sección.
- **Nueva contraseña:** se debe introducir aquí la contraseña con la que se quiere proteger el acceso a ciertas partes, secciones o elementos del antivirus (los que se hayan marcado en la lista anterior).
- **Confirmar la nueva contraseña:** si, ya se ha introducido una contraseña de acceso a estos elementos y su configuración y deseamos modificarla por algún motivo, se puede hacer gracias a esta opción.

En la sección inferior de esta ficha aparecen varios botones. Pulsando el botón **Aceptar**, se guardan los cambios realizados en la ficha. Pulsando el botón **Restaurar** se vuelven a cargar en la ficha los valores que estaban establecidos en ella por defecto, tras la instalación inicial del antivirus. Si se pulsa el botón **Cancelar**, ninguno de los cambios realizados en la lista, serán almacenados ni tenidos en cuenta.

¿Qué es una Actualización?

Los antivirus son programas (software) que permiten la detección y eliminación de otros programas dañinos, destructivos o al menos molestos, denominados virus. Los virus son reconocibles y, por lo tanto detectados, teniendo en cuenta una serie de características especiales de cada uno de ellos. Dichas características o propiedades, se conocen como *identificadores de los virus*, o *firmas de los virus*.

Por lo tanto, los antivirus localizan el identificador o firma de cada uno de los virus (los que el antivirus es capaz de detectar). Pero, ¿dónde se guardan los identificadores o firmas de los virus que detecta el programa antivirus?. Éstos están almacenados en un fichero concreto, conocido como *Archivo de Identificadores de Virus*, o *Fichero de Firmas de Virus*. Este fichero siempre debe acompañar al antivirus ya que, gracias a él, éste detecta los virus.

Todos los días surgen nuevos virus. ¿Qué significa esto?. Quiere decir que, si hoy tenemos un determinado archivo de identificadores de virus (archivo de firmas), mañana éste no contendrá los identificadores de los virus que han surgido en ese tiempo (de hoy a mañana -unos 20 diarios-).

Panda Software actualiza a DIARIO el archivo de identificadores de virus, con las nuevas firmas, cadenas, o nuevos identificadores que surgen todos los días (los nuevos virus). Es decir, se incluyen a diario todas las características de todos los nuevos virus que surgen. Esto implica que, si contamos con el último archivo de identificadores de virus, estaremos siempre actualizados y protegidos contra los nuevos virus que surjan. TODOS LOS DÍAS Panda Software pone a disposición de sus clientes registrados, el nuevo archivo de identificadores de virus. Éste se puede descargar todos los días desde la página de actualizaciones en la Web de Panda Software. Cuando incorporamos el nuevo archivo de identificadores de virus al antivirus, estamos actualizando el antivirus. Es lo que se conoce como ***Update***.

Además, por tratarse de un programa software, el antivirus también puede incorporar cambios en cuanto a su motor de análisis, posibilidades de configuración, formato,… etc. El antivirus completo (el programa y el archivo de identificadores de virus) también debería ser actualizado. Esto quiere decir que deberían actualizarse también los cambios en el programa que hayan tenido lugar desde que lo instalamos o lo actualizamos por última vez (de una versión a otra posterior). Esto es lo que se conoce como ***Upgrade***.

Tu Panda Antivirus Platinum siempre se actualiza de forma completa (tanto si la actualización se realiza manualmente a través de las opciones pertinentes, como si la actualización se realiza de forma automática). Es decir, Panda Antivirus Platinum realiza de forma simultánea tanto **Updates**, como **Upgrades**, consiguiendo siempre una actualización COMPLETA.

Veamos ahora algunos temas relacionados con el sistema de actualizaciones de Panda Antivirus Platinum.

¿Cómo Configurar la Actualización del Antivirus?
¿Cómo Actualizar el Antivirus (Asistente de Actualización)?
Actualización Automática del Antivirus

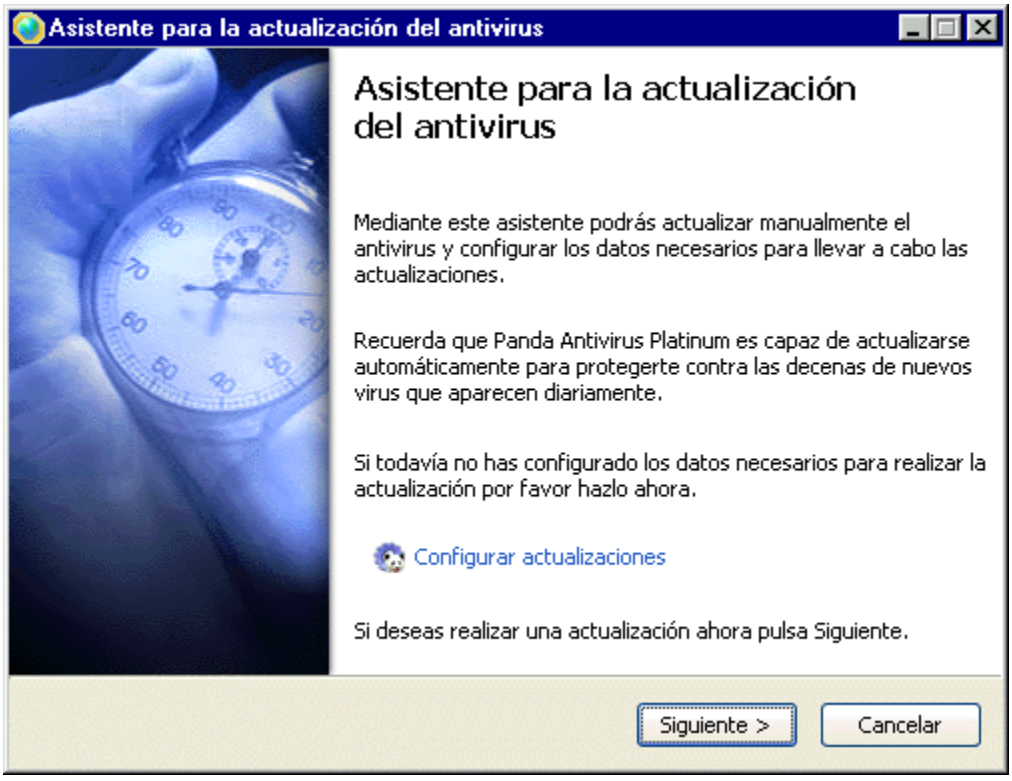
¿Cómo Actualizar el Antivirus (Asistente de Actualización)?

Antes de comentar cómo se debe llevar a cabo el proceso de actualización del antivirus, es necesario tener en cuenta lo siguiente:

- La actualización del antivirus es un servicio de Panda Software, incluido en Panda Antivirus Platinum.
- Para que sea posible realizar una actualización, es NECESARIO registrarse previamente como cliente de Panda Software. Para obtener más información sobre el registro, consulta el apartado Registro online de esta ayuda.
- La actualización a través de Internet, sólo tendrá lugar cuando se encuentre correctamente configurada (usuario y contraseña de registro) y nos conectamos a Internet.
- El antivirus no debe estar ya actualizado. Antes de comenzar con el proceso de actualización, tu Panda Antivirus Platinum comprobará automáticamente si necesita actualizarse, o no.

Para realizar una ***actualización manual*** en un determinado instante, sigue estas instrucciones:

1. En la ventana principal del antivirus, pulsa el botón **Actualizar** que se encuentra en la barra de herramientas.
2. Esto abre un asistente que te guiará en el proceso de actualización del antivirus, para que ésta se realice de forma correcta.



3. Si deseas indicar las características que debe tener la actualización, pincha sobre la opción **Configurar actualizaciones**.

4. Tanto si especificaste las características de configuración de las actualizaciones, como si no lo hiciste, pulsa el botón **Siguiente** del asistente.
5. En este momento, el proceso de actualización del antivirus se pone en marcha, localizando el archivo de identificadores de virus (y otros necesarios) en la ubicación indicada. Si se debe realizar la actualización, los ficheros necesarios serán copiados y actualizados en el ordenador donde se encuentra instalado el antivirus.
6. Al finalizar la actualización, se procederá a reconstruir el fichero de firmas de virus (archivo de identificadores de virus). Esto es debido a que el antivirus solamente descarga las diferencias entre el actual fichero y el nuevo. De esta forma el proceso es mucho más rápido y consume menos recursos.
7. Finalmente se muestra el resultado de la actualización. Se indica el número de identificadores de virus que se han incorporado (número de virus nuevos que detectará el antivirus) y el número total de virus que éste detecta en total, a partir de ese momento. Pulsa el botón **Finalizar**.

Si el proceso de actualización manual no se puede llevar a cabo por algún motivo, aparecerá un cuadro de diálogo indicándolo. Desde él podrás seleccionar la opción **Configurar ahora**, o volver a intentar la actualización, pulsando el botón **Reintentar**.

Además, tu Panda Antivirus Platinum es capaz de actualizarse por sí sólo de forma automática. Si deseas consultar información sobre las actualizaciones automáticas del antivirus, accede al apartado Actualización Automática del Antivirus, de esta ayuda.

Actualización Automática del Antivirus

Para que Panda Antivirus Platinum pueda actualizarse a sí mismo de forma automática e inteligente, cuando lo crea necesario y detecte una conexión abierta a Internet, deben cumplirse unos requisitos previos. Éstos son los siguientes:

- Haberse registrado como usuario de Panda Antivirus Platinum (Registro online).
- Haberlo indicado en la sección correspondiente de la configuración, mediante la casilla **Activar** (configuración de las actualizaciones).
- Estar trabajando en una conexión abierta a Internet.
- Que el antivirus no se encuentre actualizado. Antes de comenzar con el proceso de actualización, tu Panda Antivirus Platinum comprobará si necesita actualizarse, o no.

En cualquier caso, si deseas que el antivirus realice por su cuenta una ***actualización automática***, cuando lo necesite y detecte una conexión a Internet, sigue estos pasos:

1. En la ventana del antivirus, pulsa el botón **Opciones generales** de la barra de herramientas.
2. Colócate en la ficha **Actualización**, pinchando sobre su título.
3. En la sección **Actualizaciones automáticas**, marca la casilla **Activar actualizaciones automáticas**.
4. Si además deseas que el antivirus muestre un mensaje indicando que se ha producido la actualización y cuál ha sido el resultado de la misma, marca la casilla **Notificarme al realizar una actualización automática**.

   El sistema de actualización automático se ejecutará de forma independiente, siempre que tu Panda Antivirus Platinum detecte una conexión abierta a Internet y sea necesario realizar la actualización (ten en cuenta que para poder actualizarte, debes haberte registrado previamente). Este proceso es transparente al usuario, de tal forma que no muestra síntomas visibles, hasta que no finaliza el proceso (o ocurre alguna incidencia al respecto). Del mismo modo, no afecta en ningún aspecto al rendimiento del sistema, ni de las tareas que se estén realizando en ese momento. La actualización será incremental (sólo se actualizan partes concretas de los ficheros), haciendo que el proceso sea rápido y liberando de carga innecesaria al PC que se actualiza.

   Si deseas obtener más información, en lo que a la actualización automática se refiere, consulta el apartado Configuración General del Antivirus - Actualización, de esta ayuda.

¿Qué es el Hospital?

En ocasiones pueden existir ficheros que consideramos sospechosos, o que no se pueden desinfectar. También pueden aparecer nuevos virus. Si no hemos actualizado nuestro antivirus diaria y correctamente, el nuevo virus no sería detectado (es aconsejable realizar una actualización, al menos una vez a la semana).

Ante estas situaciones, Panda Antivirus Platinum incorpora una herramienta de gestión de ficheros sospechosos, muy útil: el **Hospital**. Éste se concibe de forma similar a los hospitales destinados al tratamiento clínico de las personas. La única diferencia es que no se trata de un hospital de prevención y solución de infecciones para personas, sino para ficheros.

Es decir, el **Hospital** de Panda Antivirus Platinum es un "centro de atención clínica" que permite ingresar en él los ficheros que consideramos infectados, o sospechosos de infección. El cometido del **Hospital** es atender a estos pacientes (ficheros posiblemente infectados por algún virus informático -sospechosos-), vigilar la evolución de su estado, encontrar la vacuna o solución a su "enfermedad" y mantenerlos aislados de otros (en cuarentena) para evitar la extensión de la hipotética infección.

Cuando Panda Antivirus Platinum realiza un análisis y encuentra un fichero infectado o un fichero sospechoso, debe realizar una acción sobre él. La determinación que el antivirus tome en ese instante sobre el fichero y la acción a realizar, depende de lo que se le haya indicado en su configuración. Dentro de la ficha **Acciones** de la configuración, se puede establecer -por ejemplo- que la acción a realizar debe ser **Mover a cuarentena el archivo infectado**, o **Borrar el archivo infectado**, etc, entre otras. Algunas de las acciones definidas allí (en la configuración de las acciones), afectan directamente al **Hospital**.

Para el correcto tratamiento clínico de los ficheros infectados, o sospechosos de estar infectados, el **Hospital** cuenta la denominada **Cuarentena**. Se trata de una sección del Hospital donde se mantienen (los incluimos nosotros, o lo hace al antivirus por sí mismo automáticamente) los ficheros sospechosos o ficheros infectados. De esta forma estarán aislados del resto, evitando que propaguen su infección a otros ficheros. Para obtener más información, se aconseja la lectura del apartado Hospital - Cuarentena, de esta ayuda.

Como ya hemos comentado, con los ficheros que se encuentran en alguna de las "dependencias" o secciones del **Hospital**, o **Cuarentena**, se pueden realizar acciones concretas: desinfectar, enviarlos a Panda Software para su estudio, eliminar, o añadir ficheros a la cuarentena.

A través de la configuración de los análisis podemos indicar que deseamos **Realizar una copia de seguridad del fichero, en caso de desinfección**. Es decir, si durante un análisis se detecta un fichero infectado, éste será desinfectado. De forma adicional, se creará una copia de dicho fichero, antes de proceder a su desinfección.

Cuando esto ocurra y siempre que todavía exista algún fichero del que se ha generado una copia de seguridad, Panda Antivirus Platinum mostrará una nueva área dentro del **Hospital**. Éste área levará el nombre **Copia de seguridad**. Desde ella podremos volver a analizar dichas copias y restaurar los ficheros originales.

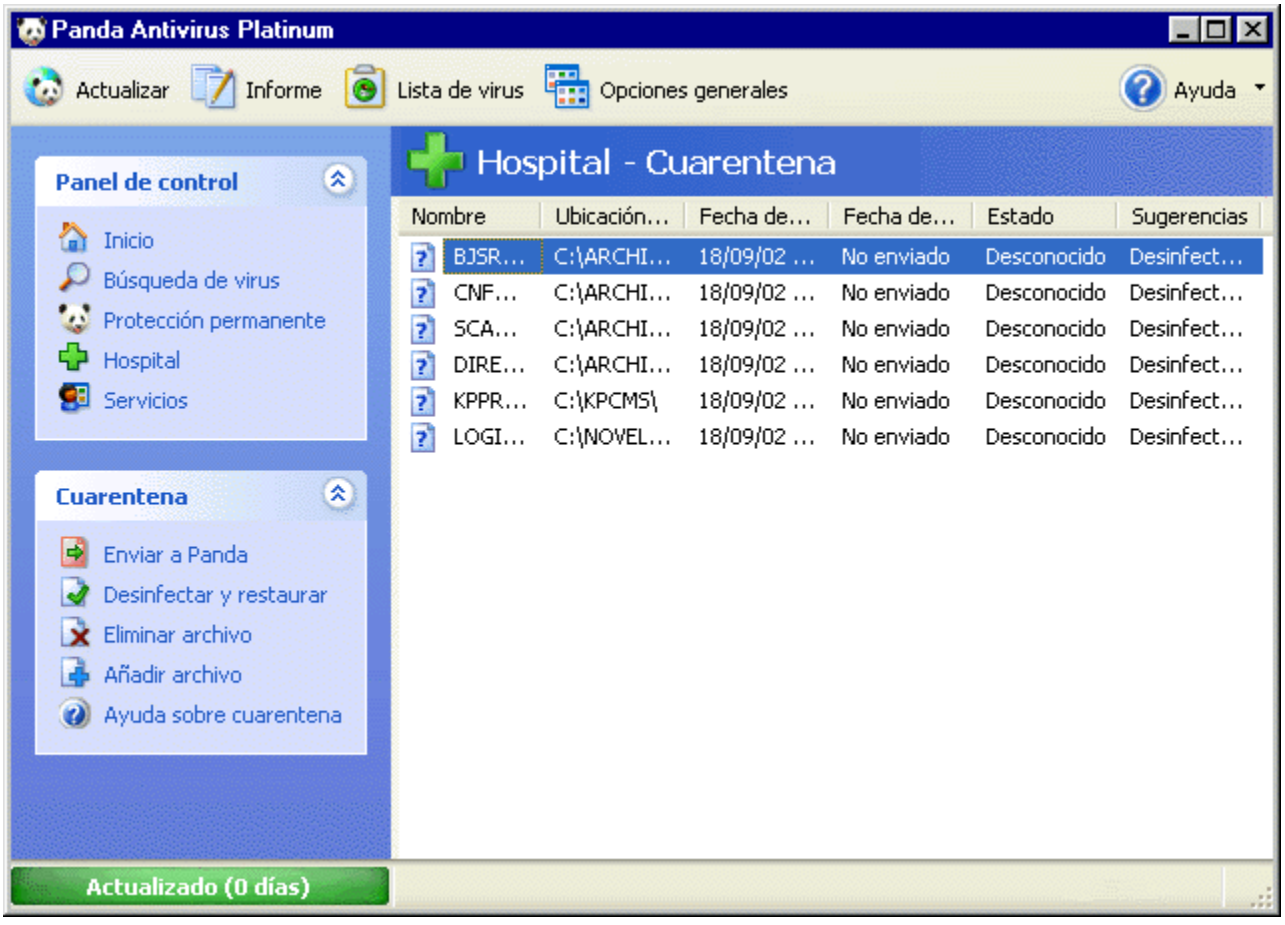
Hospital - Cuarentena

El objetivo principal de la Cuarentena, incluida en Panda Antivirus Platinum es mantener aislados todos aquellos ficheros considerados sospechosos de infección, o cualquier otro fichero incluido en la cuarentena (por el antivirus de forma automática, o por nosotros mismos de forma manual).

Al incluir un fichero sospechoso o infectado en la **Cuarentena**, se evita el posible contagio de otros ficheros (en ese ordenador, o en otros a través de las posibles conexiones de éste). Los ficheros que estén en cuarentena, no podrán ser utilizados (solamente desde el antivirus) y por lo tanto, no podrán provocar infecciones en otros ficheros.

Nota: todos los ficheros que se incluyen (de forma manual por el usuario, o automática por el propio antivirus) en **Cuarentena**, desaparecen de su ubicación original, hasta que son reestablecidos en su ubicación original.

En realidad cuando se incluye un fichero en la sección **Cuarentena** del **Hospital**, se está moviendo desde su directorio original (en el que estaba), al directorio que el antivirus utiliza para almacenar los ficheros en cuarentena. Esto implica que dichos ficheros no podrán ser utilizados. Es cómo si no existiesen para otras aplicaciones. Sólo existen para el antivirus y éste trata a dichos ficheros de un modo especial.



Cuando la **Cuarentena** contiene ficheros, éstos se muestran en un listado, junto con algunas de sus características, en cada columna:

- **Nombre.** Es el nombre del fichero que está en cuarentena.
- **Ubicación original.** Indica el directorio o carpeta en la que se encontraba el fichero, antes de pasar al estado de cuarentena. Recuerda que cuando se incluye un fichero en cuarentena, éste desaparece del directorio en el que estaba.
- **Fecha de cuarentena.** Indica la fecha y hora en la que el fichero se agregó o movió a la sección de cuarentena.
- **Fecha de envío a Panda.** Indica la fecha y hora en la que el fichero que está en cuarentena se envió a Panda Software, para ser investigado.
- **Estado.** Muestra información sobre el "estado clínico" del fichero. Éste puede estar desinfectado, o no estar infectado. También se puede desconocer su estado actual si no se ha realizado sobre él ninguna operación.
- **Sugerencias.** Esta columna muestra una indicación sobre las acciones que el antivirus sugiere realizar sobre el fichero en cuarentena.

Sobre cada uno de los ficheros que se encuentran en el **Hospital**, es posible realizar varias acciones. Puedes consultar las acciones a realizar con dichos ficheros, en la sección Acciones Sobre los Ficheros en Cuarentena, de esta misma ayuda.

Acciones Sobre los Ficheros en Cuarentena

En el listado de ficheros en Cuarentena, es posible realizar multiselecciones. Es decir, es posible marcar varios de los ficheros que aparecen en el listado, al mismo tiempo, para realizar operaciones sobre éstos. Para seleccionar un fichero, pincha sobre él con el ratón. Si deseas seleccionar ficheros consecutivos, pincha en el primero, pulsa la tecla *SHIFT* y pincha en el último de ellos. Si lo que deseas es marcar ficheros alternativos en la lista, pincha sobre uno de ellos y después pulsa la tecla *CTRL*. Mientras la mantienes pulsada, vete pinchando sobre todos los ficheros que deseas marcar.

Una vez hayas marcado todos los ficheros deseados de la cuarentena, indica la acción que deseas realizar sobre cada uno de ellos. Cuando hay varios ficheros marcados, las acciones se aplican a todos éstos. Las acciones a realizar, pueden seleccionarse a través del panel de control **Cuarentena**, o a través del menú contextual (pulsando con el botón derecho del ratón sobre los ficheros seleccionados). Veamos las acciones que se pueden realizar sobre estos ficheros:

- **Desinfectar y restaurar.** Los ficheros que se encuentran en cuarentena y están seleccionados serán analizados. Si éstos no contienen virus, o no se consideran sospechosos, se restaurarán en su ubicación original.

  Esta acción también se puede realizar desde el menú contextual (pulsando con el botón derecho del ratón sobre la selección de ficheros) y seleccionando la opción **Desinfectar y restaurar**, o pulsando la tecla de función *F8*.

  Nota: si se analiza un fichero de la cuarentena y no se encuentra infectado, éste se elimina automáticamente de la sección de **Cuarentena** y se coloca de nuevo en su ubicación original. Aparecerá un cuadro de diálogo a través del cual se nos pide confirmación para restaurarlo en su ubicación original.

- **Actualizar.** Esta acción sólo se puede llevar a cabo a través del menú contextual, o pulsando la tecla de función *F5*. Para realizarla mediante el menú contextual, pulsa con el botón derecho del ratón sobre la lista de ficheros y selecciona la opción **Actualizar**. Inmediatamente se actualiza la información correspondiente a los fichero que se encuentran en el panel de **Cuarentena** (*Nombre*, *Ubicación original*, *Fecha de cuarentena*, *Fecha de envío a Panda*, *Estado* y *Sugerencias*), si ésta hubiese cambiado.

- **Mostrar información.** Esta opción sólo está accesible desde el menú contextual. Selecciona uno de los ficheros existentes en el panel de **Cuarentena** (esta opción no estará activa cuando se hayan seleccionado varios ficheros) y consulta información sobre el fichero seleccionado (se indicará si éste contiene, o no, virus).

- **Eliminar archivo.** Borra los ficheros seleccionados de la cuarentena y de su ubicación original, definitivamente. Antes de hacerlo, se solicita confirmación para realizar la acción, ya que éstos no se podrán recuperar. Esta acción también se puede llevar a cabo a través del menú contextual, seleccionando la opción **Eliminar**.

- **Enviar a Panda.** Permite enviar los ficheros sospechosos que se encuentran en cuarentena y hayamos seleccionado, a Panda Software, para su análisis y estudio. Si el fichero seleccionado en la lista de cuarentena no se considera sospechoso, será restaurado en su ubicación original. Además, no será posible realizar un envío de ficheros sospechosos o en cuarentena, si el antivirus

no está actualizado (si la versión del archivo de identificadores de virus, no es reciente). Esta operación también puede realizarse seleccionando la opción **Enviar** del menú contextual.

- **Añadir archivo.** Esta operación solamente se puede realizar desde el Panel de control **Cuarentena**, no desde el menú contextual, o mediante ninguna tecla de función. Permite incluir los ficheros que se deseen en la cuarentena del antivirus. Recuerda que, en tal caso, desaparecerán de su ubicación original (son movidos al directorio en el que el antivirus mantiene a los ficheros en cuarentena, desapareciendo del directorio en el que se encontraban).

  Esto muestra un cuadro de diálogo. Mediante él, colóquese en la unidad de disco donde está el fichero que deseas agregar a la cuarentena, selecciona el directorio y camino completo en el que se encuentra ese fichero y finalmente selecciónalo. Después, pulsa el botón **Abrir** o haz doble clic sobre el fichero en cuestión. Automáticamente, aparecerá en la lista de ficheros en cuarentena.

- **Ayuda sobre hospital.** Selecciona esta opción en el panel **Cuarentena** (no disponible a través del menú contextual) y obtendrás más información sobre el funcionamiento y la utilidad de la cuarentena.

¿Qué son los Servicios y Cómo Puedo Utilizarlos?

Nota: antes de poder utilizar correctamente todos los servicios que incluye tu Panda Antivirus Platinum, debes registrarse como usuario, para obtener tu nombre de *usuario* y tu *contraseña*. Sólo estos datos te permitirán utilizar los servicios. Si deseas obtener más información sobre este registro, consulta el apartado Registro online de esta ayuda, o accede a la página de Registro online en la Web de Panda Software, para realizarlo. También puedes registrarte realizar tu registro online pulsando sobre la dirección Web que aparece en la sección inferior de la pantalla de servicios.

Panda Antivirus Platinum incluye varios de los servicios más demandados habitualmente por los usuarios (domésticos y corporativos). Estos servicios complementan las excelentes capacidades y ventajas del antivirus, haciendo de Panda Antivirus Platinum un **¡antivirus vivo!**. Con esta combinación, tu Panda Antivirus Platinum se convierte en una de las herramientas más completas, potentes, versátiles y útiles. Un antivirus sin servicios es un antivirus muerto.

En Panda Software nos esforzamos al máximo para ofrecer unas soluciones antivirus insuperables, acompañadas de unos servicios excelentes. La combinación de una buena herramienta antivirus y unos excelentes servicios, es el objetivo principal de Panda Software.

¿Qué son los servicios?. Los servicios, por lo tanto, pueden entenderse como apoyos adicionales que permiten al usuario contar con más ayuda, capacidades y ventajas de las que le ofrece la herramienta antivirus por sí sola. En definitiva, mediante la utilización de los servicios, nunca estarás sólo. Siempre tendrás a su lado un grupo de expertos que te asesorarán, resolverán sus dudas, te guiarán y solucionarán tus problemas en lo referente a los virus.

¿Quién y Cuándo puede utilizar los servicios?. Durante el proceso de instalación del antivirus, tú mismo podrás realizar tu registro online, como usuario de Panda Antivirus Platinum. Tras realizar el registro, recibirás tu nombre de **Usuario** y tu **Contraseña**. Sólo a partir de ese momento, podrás disfrutar de los servicios que acompañan a Panda Antivirus Platinum, indicando estos datos, cuando te sean solicitados.-

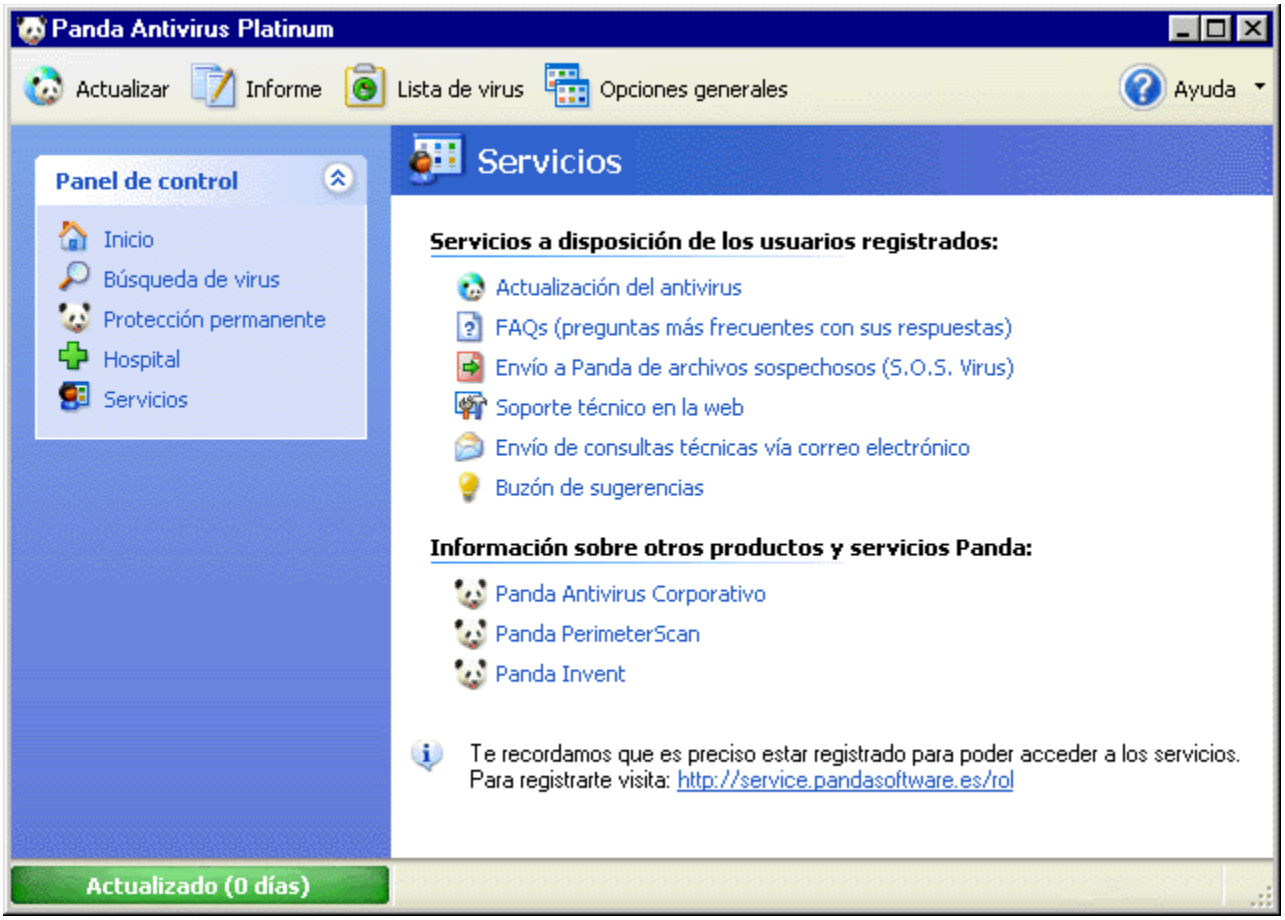
Registro online. Para poder utilizar todos los servicios que incorpora el antivirus, **DEBES REGISTRARTE PREVIAMENTE**. Esto quiere decir que, a partir de ese instante, serás oficialmente usuario de Panda Antivirus Platinum. Por lo tanto, recibirás tu nombre de *usuario* y tu *contraseña* de acceso, para poder utilizar todos los servicios que acompañan al antivirus

Nota: consulta la tarjeta de registro de Panda Antivirus Platinum, para saber cuáles son los servicios a los que tienes derecho, por cuanto tiempo y cuáles son los servicios que puedes contratar de forma adicional.

Para acceder a los servicios que incluye tu Panda Antivirus Platinum, selecciona la opción **Servicios**, en el **Panel de control**, dentro de la ventana del antivirus. Panda Antivirus Platinum incorpora un buen grupo de servicios que te ayudarán. Puedes consultar cada uno de ellos a través del apartado ¿Qué Servicios Incluye Panda Antivirus Platinum?, de esta ayuda.

¿Qué Servicios Incluye Panda Antivirus Platinum?

Para acceder a cada uno de los servicios que incluye Panda Antivirus Platinum, selecciona la opción **Servicios**, en el **Panel de control**, dentro de la ventana del antivirus. Esto muestra en el panel central la lista de los servicios disponibles, pudiendo acceder a cada uno de ellos directamente (pulsando sobre ellos)



- **Actualización del antivirus.** Este servicio permite realizar actualizaciones manuales del antivirus, activar o desactivar las actualizaciones automáticas del mismo y definir cada una de las características de cualquiera de ellas. Para obtener más información, puedes consultar el apartado ¿Qué es una Actualización?, de esta ayuda y realizar actualizaciones manuales a través de la página de actualizaciones de Panda Software.
- **FAQs (preguntas más frecuentes con sus respuestas).** Son preguntas que otras personas nos han planteado con anterioridad. Junto a cada una de ellas encontrarás la respuesta correspondiente. Esto puede ayudarte a solucionar las dudas que te plantees. Para acceder a ella, selecciona la opción **Servicios** en el **Panel de control**, dentro de la ventana del antivirus y pincha la opción **FAQs (preguntas más frecuentes con sus respuestas)**. Entonces se muestra un índice con todas ellas. Pulsa sobre la que más te interese y accederás a su respuesta. Para volver al índice o para volver al menú de **Servicios**, pulsa el botón **Atrás**, que aparece en la parte inferior de esta sección.
- **Envío a Panda de archivos sospechosos (S.O.S. Virus).** Si durante un análisis, alguno de los ficheros se considera sospechoso, podría encontrarse bajo los efectos de un nuevo virus. En tal

caso envíanoslo. ¡Panda Software, te entregará en poco tiempo y de forma gratuita una solución antivirus, o la certificación de que los ficheros se encuentran en perfectas condiciones!. Selecciónalos e indica a tu Panda Antivirus Platinum que los envíe al Laboratorio de Investigación de Panda Software. Nuestros expertos informáticos los estudiarán, detectarán el virus (si éste existe), lo eliminarán, y te enviarán la solución antivirus correspondiente. Si deseas obtener más información, consulta el apartado Envío a Panda de Ficheros Sospechosos (S.O.S. Virus), de esta ayuda.

- **Soporte técnico en la web.** Sin duda es muy importante contar con alguien que te ayude a solucionar inmediatamente cualquier incidencia con algún virus, o con tu programa antivirus. Panda Antivirus Platinum te permite el acceso directo al área de *Soporte Técnico*, en la Web de Panda Software (www.pandasoftware.es/soptecni/). Para ello, sólo debes abrir la ventana de tu antivirus, acceder al menú **Servicios** y seleccionar la opción **Soporte técnico en la web**.. Si deseas obtener más información, consulta el apartado Soporte técnico en la web, de esta ayuda.
- **Envío de consultas técnicas vía correo electrónico.** Tras haber consultado cada una de las FAQs que se incluyen en el antivirus, a través del servicio **FAQs (Preguntas más frecuentes con sus respuestas)**, habrás solucionado todas tus dudas. Si no fuese así, puedes enviarnos cualquier otra cuestión, mediante este servicio de soporte técnico, o envío de consultas técnicas por correo electrónico. Si deseas obtener más información, consulta el apartado Envío de consultas técnicas vía correo electrónico, de esta ayuda.
- **Buzón de sugerencias.** ¡Tu opinión es muy importante para nosotros!. Este servicio te permite estar en contacto directo con Panda Software, haciéndonos llegar cualquiera de tus ideas, comentarios o sugerencias para mejorar tu Panda Antivirus Platinum, los servicios que éste incluye, o cualquier otro factor. Si deseas obtener más información, consulta el apartado Buzón de sugerencias, de esta ayuda.

Desde esta sección de **Servicios** además, podrás acceder a información completa sobre **Otros de los productos y servicios Panda**.

Envío a Panda de Ficheros Sospechosos (S.O.S. Virus)

Este es uno de los servicios incluidos en Panda Antivirus Platinum. Para utilizarlo, previamente debes haberte registrado como usuario de Panda Software. Si ya te has registrado, podrás enviar a Panda Software los ficheros que el antivirus haya considerado como sospechosos, o aquellos sobre los que actualmente no exista posibilidad de desinfección (nuevos virus,… etc.).

Es conveniente tener controlados y aislar este tipo de ficheros de los demás. De este modo, si finalmente estuviesen infectados, evitaríamos que reprodujesen su infección o contagiasen al resto. Por este motivo, Panda Antivirus Platinum incluye el **Hospital**. Gracias a él, podrás mantener en cuarentena todos los ficheros sospechosos. Si deseas obtener más información sobre el Hospital y la Cuarentena, o sobre el modo de agregar ficheros a la cuarentena, te aconsejamos la lectura del apartado Hospital - Cuarentena, de esta ayuda.

También puedes enviarnos dichos ficheros sospechosos a Panda Software, para que los estudiemos y analicemos. En caso de que estuviesen infectados por algún nuevo virus, te enviaremos la correspondiente solución antivirus que permita su desinfección. Es conveniente actualizar el antivirus antes de enviarnos ficheros sospechosos.

¿Cómo puedes enviar los ficheros sospechosos a Panda Software?. Es muy sencillo. Sigue estos pasos:

1. Desde la ventana de Panda Antivirus Platinum, accede al menú **Hospital**, en el **Panel de control**.
2. Si ya existen ficheros que el antivirus ha considerado sospechosos, éstos aparecerán en la lista de ficheros en cuarentena. También encontrarás en dicha lista los que tú mismo hayas incluido en la **Cuarentena** del **Hospital**. Si ahora mismo deseases poner en cuarentena algún otro fichero, podrías hacerlo mediante la opción **Añadir archivo** del panel **Cuarentena**. Si deseas obtener más información, consulta el apartado Acciones sobre los ficheros en cuarentena, de esta ayuda.
3. Si deseas enviar a Panda Software alguno de los ficheros de la lista, selecciónalo o márcalo. Puedes seleccionar varios ficheros utilizando el ratón junto con las teclas *CTRL* y *SHIFT*.
4. Pincha la opción **Enviar a Panda**, en el panel **Cuarentena**. También puedes hacerlo a través de la opción **Enviar** del menú contextual (botón derecho del ratón sobre los ficheros seleccionados).
5. El fichero es inmediatamente analizado. Tanto si está infectado, como si no lo está se te indicará a través de un cuadro de diálogo y se te pedirá confirmación para continuar con el envío.
6. Lee atentamente los comentarios que se muestran y pulsa el botón **Siguiente**.
7. En el recuadro **Indica tu dirección de correo electrónico**, escribe tu correo electrónico y asegúrate de que éste es el correcto. En la sección **Descripción del problema**, indícanos qué es lo que ha sucedido, cómo se ha realizado el análisis, qué ficheros se han renombrado, etc. Explícanos, de forma muy CLARA y CONCRETA, lo ocurrido. Después de hacerlo, pulsa el botón **Siguiente**. Si deseas volver al paso previo, puedes pulsar el botón **Anterior**. Si pulsas el botón **Cancelar**, volverás al menú de servicios. Pulsando sobre la opción **Aviso legal**, podrás leer una nota sobre la legalidad y la protección de datos confidenciales. Pulsa el botón **Siguiente**, para continuar.
8. Se mostrará la lista con los ficheros seleccionados. Si no deseas enviar alguno de los ficheros de la lista, selecciónalo en ella y pulsa el botón **Eliminar archivos**.
9. Podrás realizar selecciones múltiples de ficheros (seleccionar al mismo tiempo varios de ellos), utilizando el ratón junto con la pulsación de las teclas *SHIFT* (selección de ficheros adyacentes o

contiguos), o `CTRL` (selección de ficheros alternos). Cuando hayas finalizado la selección de los ficheros que deseas enviarnos, pulsa el botón **Siguiente**, para continuar. En ese momento, Panda Antivirus Platinum comprimirá los ficheros que quieres enviarnos.

10. A continuación se mostrará una pantalla en la que se indica el tamaño del mensaje que se va a enviar. Tienes la posibilidad de enviarlo pulsando el botón **Enviar**, o volver al paso **Anterior**.

FAQs (Preguntas Más Frecuentes Con Sus Respuestas)

A través de esta sección puedes encontrar las respuestas a muchas de las dudas que te surgen con respecto al funcionamiento, configuración, instalación y desinstalación del antivirus. Del mismo modo, encontrarás respuestas a tus dudas sobre los virus. Si deseas consultar la respuesta a alguna de las preguntas que aparecen en esta lista, pincha sobre ella.

Nota: si deseas imprimir TODAS las FAQs (preguntas más frecuentes con sus respuestas), pulsa el botón Imprimir **TODAS las FAQs** (bajo estas líneas), o pulsa **aquí**. Sólo disponible para la ayuda en formato HLP.

{button Imprimir TODAS las FAQs,IF(InitMPrint(),`MPrintId(`320'):MPrintId(`355'):MPrintId(`360'):MPrintId(`365'):MPrintId(`370'):MPrintId(`375'):MPrintId(`380'):MPrintId(`385'):MPrintId(`390'):MPrintId(`395'):MPrintId(`400'):MPrintId(`405'):MPrintId(`410'):MPrintId(`415'):MPrintId(`420'):MPrintId(`425'):MPrintId(`430'):MPrintId(`435'):MPrintId(`440'):MPrintId(`445'):MPrintId(`450'):MPrintId(`455'):MPrintId(`460'):MPrintId(`465'):MPrintId(`470'):MPrintId(`475'):MPrintId(`480'):MPrintId(`485'):MPrintId(`490'):MPrintId(`495'):MPrintId(`500'):MPrintId(`505'):MPrintId(`510'):MPrintId(`515'):MPrintId(`520'):MPrintId(`521'):MPrintId(`625'):EndMPrint()')}

Envío de Consultas Técnicas Vía Correo Electrónico

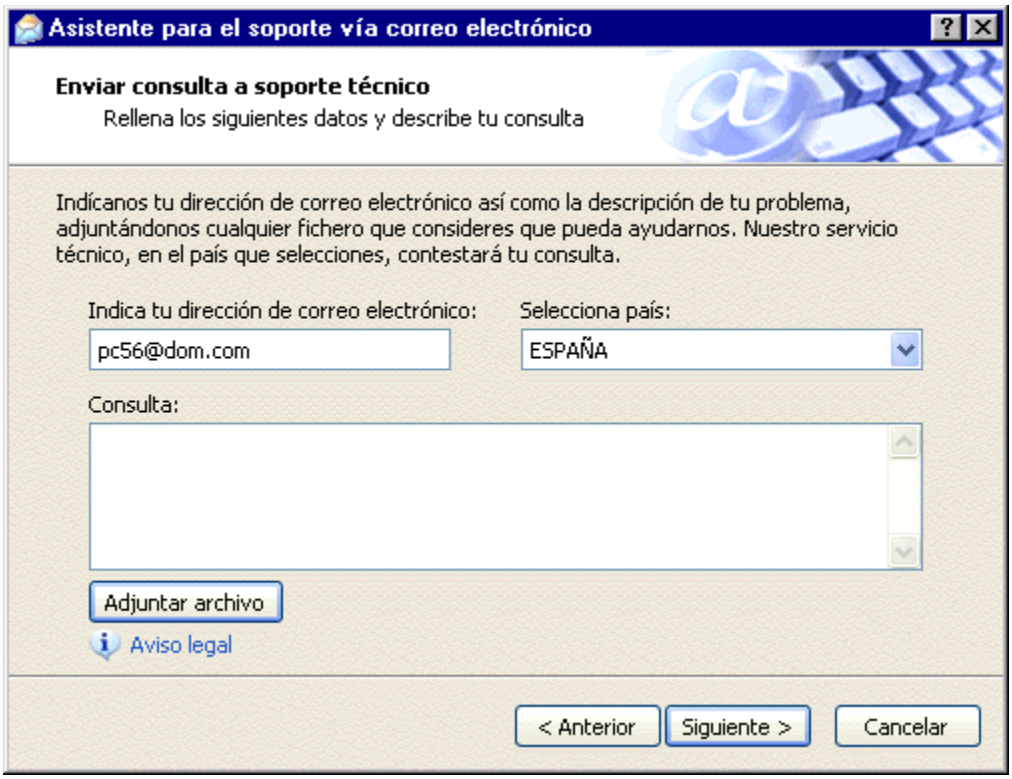
Este es uno de los servicios incluidos en Panda Antivirus Platinum. Para utilizarlo, previamente debes haberte registrado como usuario de Panda Software. Si ya te has registrado, selecciona la opción **Servicios** en el **Panel de control** y pulsa sobre la opción **Envío de consultas técnicas vía correo electrónico**.

Entonces, sigue estos pasos:

1. Desde la ventana de Panda Antivirus Platinum, acceda al menú **Servicios**, en el **Panel de control**.
2. Selecciona la opción **Envío de consultas técnicas vía correo electrónico**. Entonces, aparece un asistente que te guiará paso a paso, para que puedas enviar tu consulta a Panda Software.

   Si cuentas con la versión Beta de Panda Antivirus Platinum, se mostrará un cuadro de diálogo con una dirección Web (www.pandasoftware.es/beta). Pincha sobre ella para acceder a la página Web correspondiente al programa Beta del antivirus.

3. Si cuentas con una versión comercial que no sea Beta, se mostrará la primera pantalla del asistente, donde se comenta la función del mismo. Es aconsejable consultar previamente las FAQs, antes de realizar el envío de una consulta. Puede que la solución a la misma se encuentre en ellas. Para hacerlo, pincha sobre la opción **FAQs (Preguntas más frecuentes con sus respuestas)**.
4. Si has revisado las FAQs y no has encontrado una respuesta que se adapte a tus necesidades, pulsa el botón **Siguiente**.
5. En el recuadro **Indica tu dirección de correo electrónico**, escribe tu correo electrónico y asegúrate de que éste es el correcto. A continuación, selecciona el país al que deseas enviar tu consulta. En la sección **Consulta**, indícanos o explícanos de forma muy CLARA y CONCRETA, tu problema o duda.



Por otra parte, el botón **Adjuntar Archivo** te permite seleccionar cualquier fichero que consideres que pueda ayudarnos a solucionar tu problema. Después de hacerlo, pulsa el botón **Siguiente**. Si deseas volver al paso previo, puedes pulsar el botón **Anterior**. Pulsando sobre la opción **Aviso legal**, podrás leer una nota sobre la legalidad y la protección de datos confidenciales. Pulsa el botón **Siguiente**, para continuar.

6. Aparece un cuadro de diálogo en el que se informa del tamaño del mensaje a enviar con su consulta. Pulsa sobre el botón **Enviar**, para que recibamos las dudas que nos has comentado en el apartado **Consulta**. Al finalizar se mostrará un mensaje, indicando cómo ha transcurrido el envío. Para regresar al menú de servicios, pulsa el botón **Volver**.

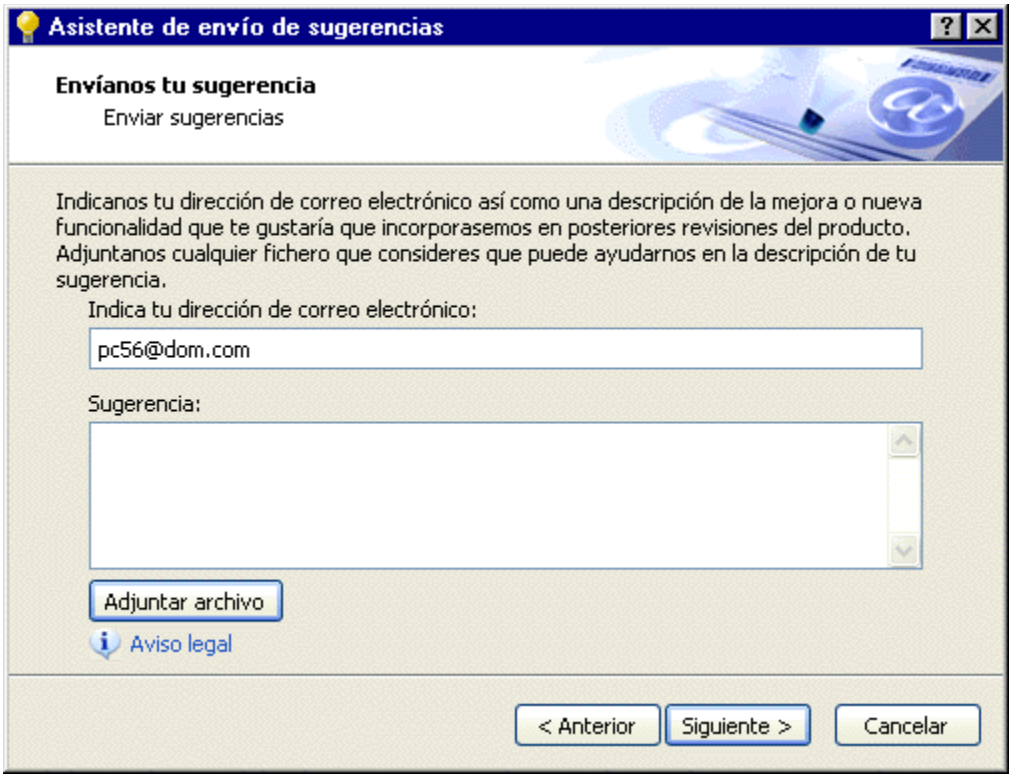
En cualquier momento podrás pulsar el botón **Cancelar**, para finalizar o detener el proceso de envío de consultas.

Buzón de Sugerencias

Este es uno de los servicios incluidos en Panda Antivirus Platinum. Para utilizarlo, previamente debes haberte registrado como usuario de Panda Software. Si ya te has registrado, selecciona la opción **Servicios** en el **Panel de control** y pulsa sobre la opción **Buzón de sugerencias**.

Para la utilización de este servicio, sigue estos pasos:

1. Desde la ventana de Panda Antivirus Platinum, accede al menú **Servicios**, en el **Panel de control**.
2. Selecciona la opción **Buzón de sugerencias**.
3. En la primera pantalla del asistente, se comenta la función del mismo. Es aconsejable consultar las FAQs, antes de realizar el envío de una sugerencia. Para hacerlo, pincha sobre la opción **FAQs (Preguntas más frecuentes con sus respuestas)**.
4. Si has revisado las FAQs y no has encontrado una respuesta que se adapte a tus necesidades, pulsa el botón **Siguiente**.
5. En el recuadro **Indica tu dirección de correo electrónico**, escribe tu correo electrónico y asegúrate de que éste es el correcto. En la sección **Sugerencia**, indícanos tus comentarios o ideas para mejorar tanto el antivirus, como los servicios que éste incluye. Todas ellas serán tenidas en cuenta y nos ayudarán a mejorar. Explica cada uno de tus comentarios de forma muy CLARA y CONCRETA.



El botón **Adjuntar Archivo** te permite seleccionar el fichero que deseas enviarnos en caso de que lo estimes oportuno. Después de hacerlo, pulsa el botón **Siguiente**. Si deseas volver al paso previo, puedes pulsar el botón **Anterior**. Pulsando sobre la opción **Aviso legal**, podrás leer una nota sobre la

legalidad y la protección de datos confidenciales. Pulsa el botón **Siguiente**, para continuar.

6. Pulsa sobre el botón **Enviar**, para que recibamos todos los comentarios que nos has incluido en el apartado **Sugerencia**.
7. Al finalizar se mostrará un mensaje, indicando cómo ha transcurrido el envío. Para regresar al menú de servicios, pulsa el botón **Finalizar**.

En cualquier momento podrás pulsar el botón **Cancelar**, para finalizar o detener el proceso de envío de sugerencias.

Información Sobre Otros Productos y Servicios Panda

Aunque no se trata de un servicio como tal, es importante estar informado sobre otros productos y servicios antivirus, de seguridad informática y de inventariado automático de equipos y redes informáticas.

Panda Software cuenta con varios productos y servicios con esta finalidad. Para acceder a esta información sólo tienes que seleccionar la opción **Servicios** en el **Panel de control**. En la sección inferior del panel central aparece un apartado con el título **Información sobre otros productos y servicios Panda**.

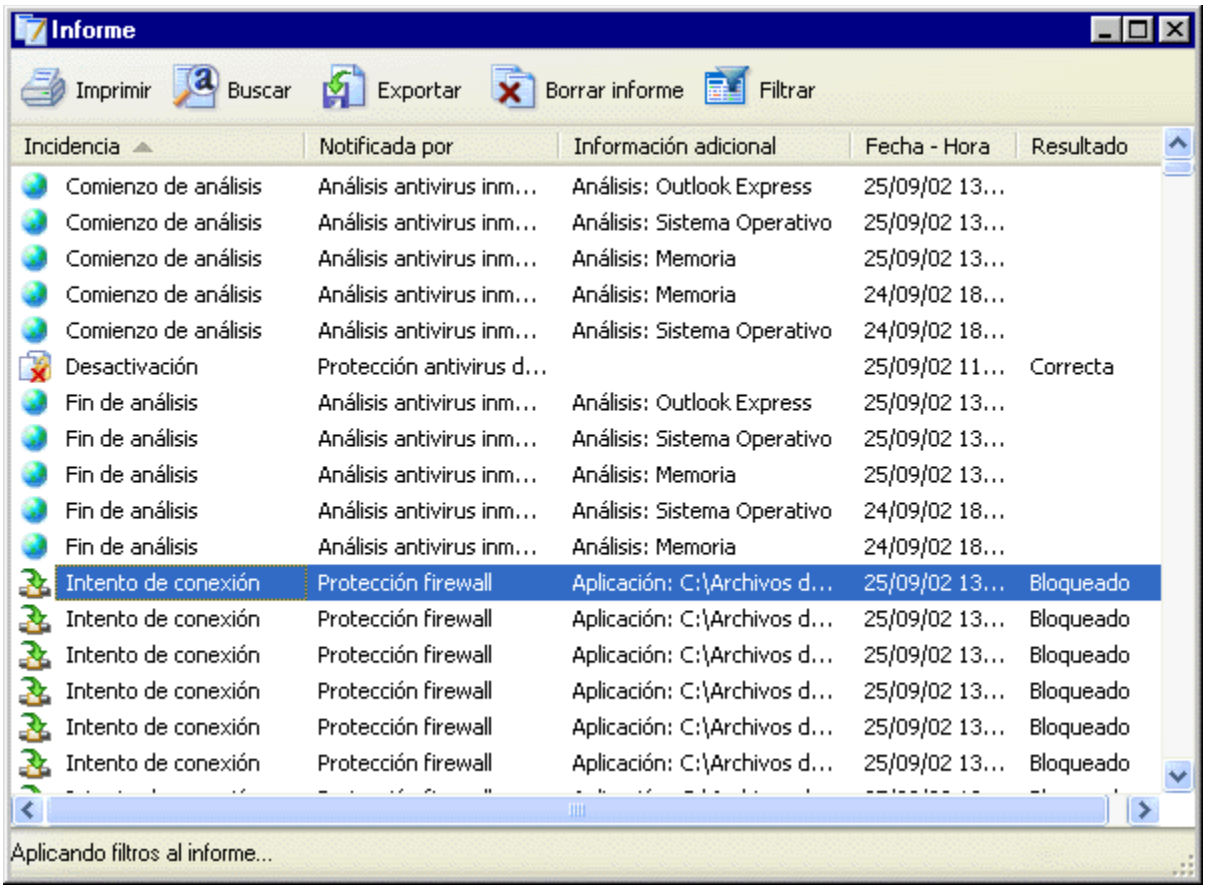
Esta sección se subdivide a su vez en varios apartados en los que podrás encontrar información sobre el producto que selecciones. Esto será posible mediante un acceso a las fichas de cada uno de los productos, en la Web de Panda Software (www.pandasoftware.es).

El Informe de los Análisis y de la Protección Permanente (Antivirus y Firewall)

El informe recoge toda la actividad del antivirus correspondiente a los análisis (inmediatos y programados), así como a la protección permanente (Antivirus -archivos y correo- y Firewall). Su principal función es servir de histórico de los análisis, así como servir de registro de todas las incidencias ocurridas con la protección permanente y el fiewall. El resultado de un análisis, se puede consultar de dos modos:

- Justo después de finalizar el análisis. Si en el momento en el que finaliza éste, se pulsa el botón **Informe** que aparece, se accederá a la ventana del informe completo.
- En cualquier otro momento. El informe se puede mostrar en cualquier instante, pulsando el botón **Informe** de la barra de herramientas (en la ventana del antivirus). Se mostrará el informe de todas las incidencias, siempre que no se haya eliminado o borrado el contenido del mismo.

Cada una de las incidencias del informe se presenta en un listado, con cada uno de los campos del mismo en una columna. Éstos son los siguientes:



Incidencia: indica la acción que se ha llevado a cabo durante el análisis, o durante el periodo de tiempo en el que ha estado activa alguna de las protecciones permanentes (antivirus y/o firewall).

Notificada por: este campo indica qué tipo de análisis (inmediato, programado), protección permanente, u operación (actualización, etc) ha sido quien ha originado la entrada de la incidencia correspondiente en

el informe.

Información adicional: indica el directorio y ruta (ubicación) en la que se encuentra el fichero que ha provocado la incidencia (en el caso de los análisis del antivirus), o el tipo (nombre) del análisis que ha provocado dicha incidencia.

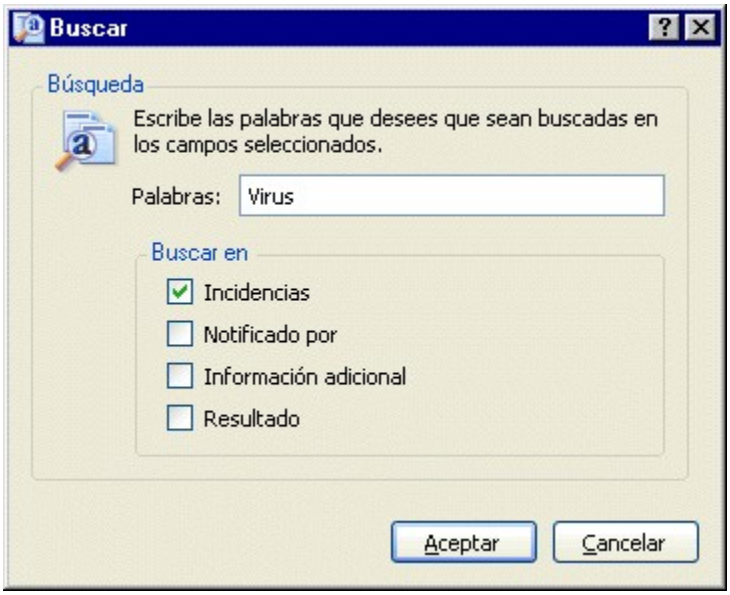
Fecha-hora: registra la fecha y la hora en la que se ha producido la incidencia.

Resultado: muestra la acción que se llevó a cabo en la incidencia en cuestión.

La ventana del informe, contiene una barra de botones o herramientas en la parte superior. A través de los botones que se encuentran en ella, es posible realizar determinadas acciones. Éstas son las siguientes:

Imprimir: es posible realizar la impresión del informe, indicando el nombre de la impresora así como el intervalo y el número de copias deseado.

Buscar: permite realizar búsquedas en el informe. Al acceder a ella, se requiere la introducción de la palabra o **Palabras** de búsqueda y el lugar (campo o columna en el informe) en el que ésta se debe buscar: **Incidencias**, **Notificado por**, **Información adicional**, o **Resultado**. Se pueden seleccionar todas ellas. Después de indicar estos datos, pulse el botón **Aceptar**.

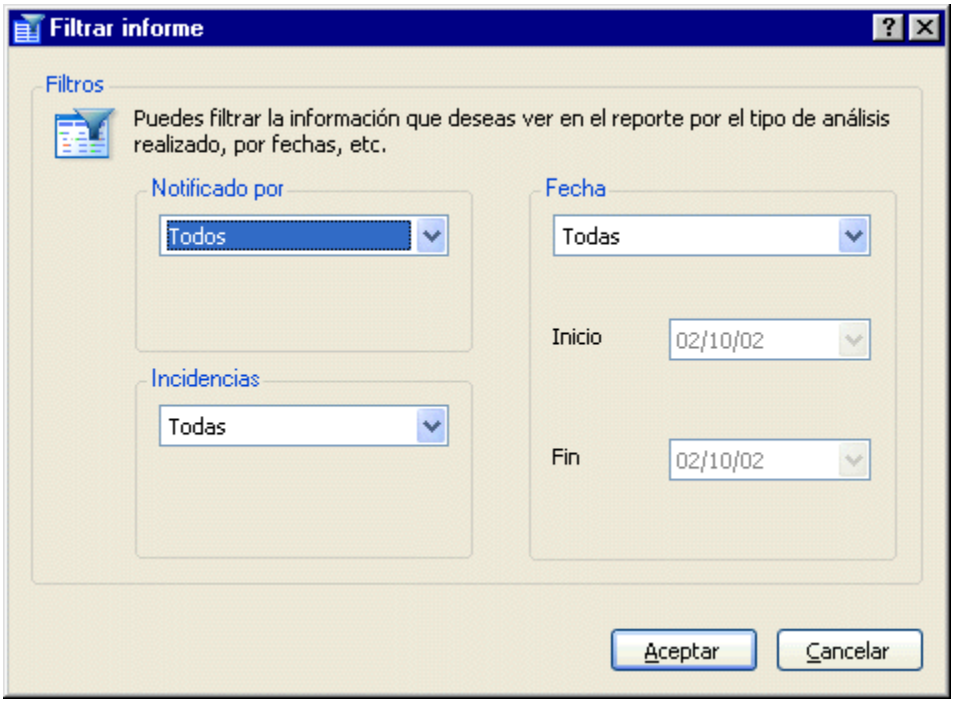


Exportar: gracias a esta utilidad, el informe se podrá guardar en un fichero de texto (*TXT*, en formato ASCII), para su almacenamiento y posterior consulta o traslado a otro ordenador. Se debe indicar en nombre del fichero, así como la unidad de disco y el directorio en el que se almacenará.

Borrar informe: borra el contenido del informe (reporte) definitivamente. Antes de eliminarlo, se pide confirmación para hacerlo.

Filtrar: su utilidad es la de presentar la información de forma reducida. Haciendo uso de los posibles

filtros, se indicará la presentación de una información u otra:

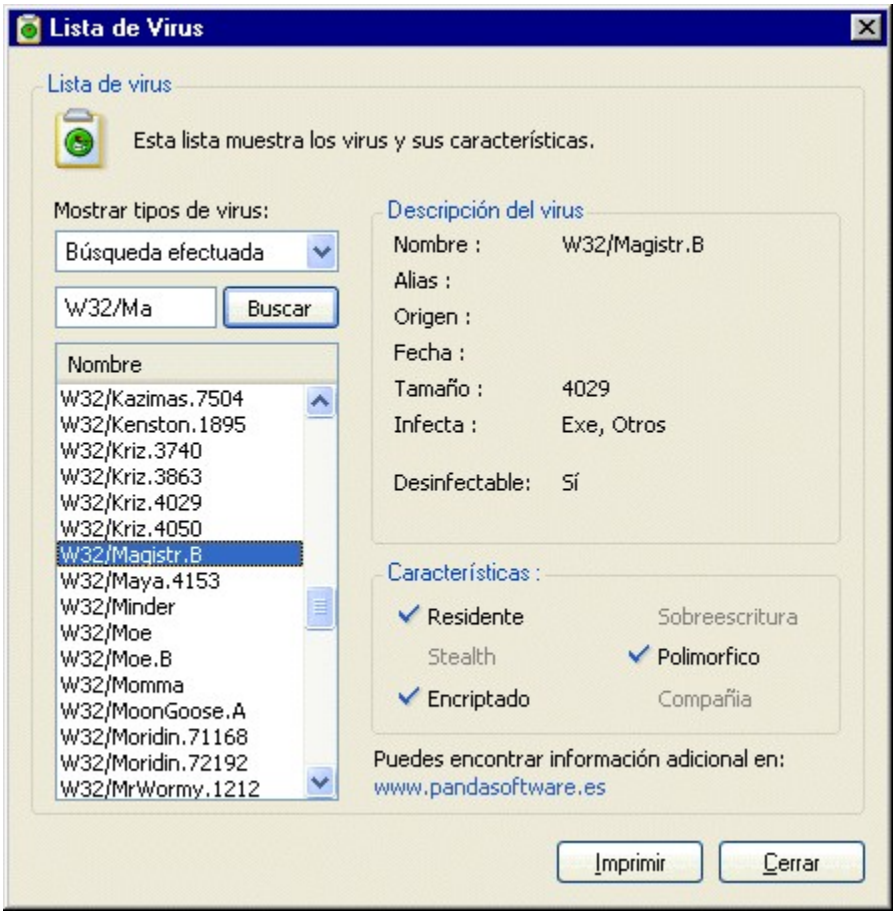


- **Notificado por:** mediante esta lista desplegable será posible presentar exclusivamente las incidencias en función del tipo de análisis o tipo de protección permanente en el que sucedieron. También es posible filtrar dicho informe teniendo en cuenta que las incidencias pueden deberse a las actualizaciones.
- **Incidencias:** en esta caso el filtrado de la información, se refiere al suceso o situación que se produjo.
- **Fecha:** permite determinar el criterio de comparación (**Todas**, **Antes o igual a...**, **Después o igual a...**, **Entre**), a la hora de realizar el filtrado por fechas entre los campos **Fecha Inicio** y **Fecha Fin**.

Además, es posible ordenar el listado del informe (de forma ascendente o descendente) por cualquiera de sus columnas. Para ello, solamente se debes pulsar sobre el título de la columna.

La Lista de Virus (Informaciones)

Mediante el botón **Lista de virus** situado en la barra de botones o herramientas de Panda Antivirus Platinum, se puede acceder a la lista de virus que detecta el antivirus. Se puede obtener información detallada sobre cada virus de la lista seleccionándolo.



Mediante la lista desplegable que se encuentra dentro del apartado **Mostrar tipos de virus**, se puede escoger entre ver **Todos los Virus**, ver sólo aquellos **Virus de Programa**, ver aquellos **Virus de Boot**, ver exclusivamente los llamados **Virus de Macro**, ver una lista con los **Virus más comunes**, o realizar una **Búsqueda por contenido**. En función de la opción que se escoja, se mostrarán unos u otros virus en la lista.

Se puede indicar también el nombre de un virus dentro de la sección **Buscar Virus** para encontrar así un virus concreto con mayor facilidad. Con ese mismo fin, la lista de virus se presenta ordenada alfabéticamente.

Seleccionado cualquier virus de la lista, se verá información detallada sobre el mismo en el apartado **Descripción del virus**. Entre los datos que se presentan están: **Nombre**, **Alias**, **Origen**, **Fecha** (en la que se detectó el virus), **Tamaño** (del virus) y las áreas que **Infecta** y si es **Desinfectable**. Además, como información adicional, se indica si el virus cuenta con características concretas. Entre ellas están:

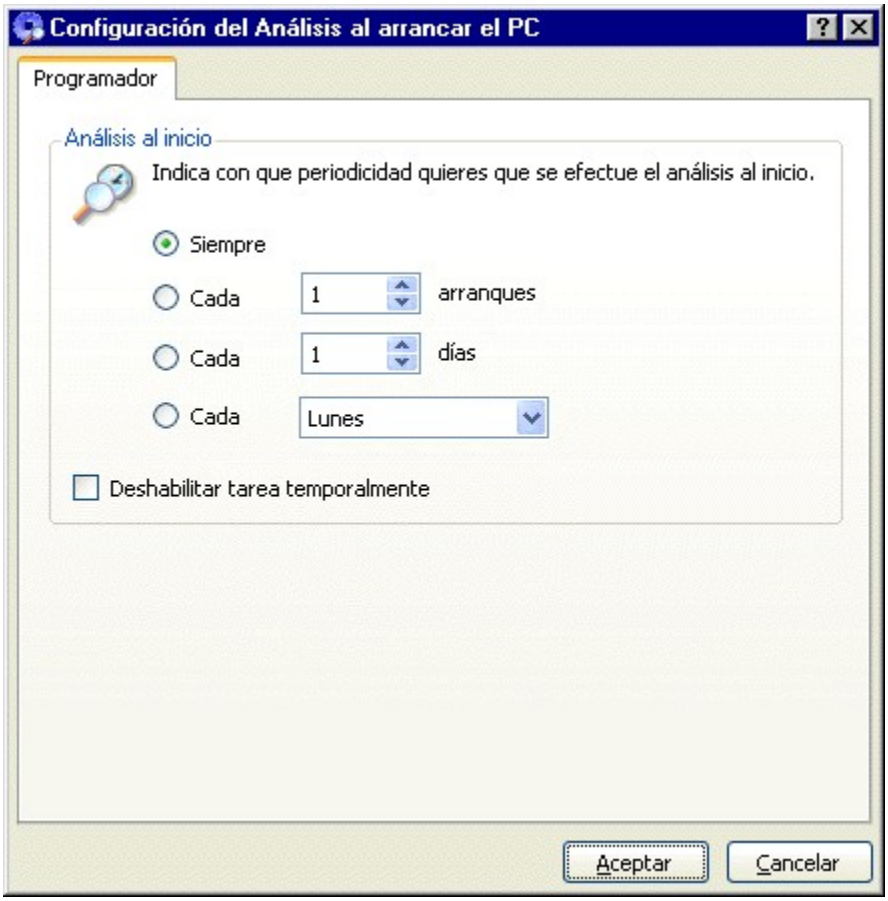
- **Residente:** cuando se ejecuta, el virus reserva una pequeña parte de la memoria y se instala en ella para ir contagiándose desde ahí.
- **Stealth:** es una técnica que usan algunos de los virus residentes. Esta técnica consiste en camuflar los cambios que el virus hace sobre los ficheros que infecta. 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 o codificarse a sí mismos. Aquellos que además lo hacen de manera diferente cada vez que infectan un fichero, son virus polimórficos.
- **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.
- **Compañía:** los virus de compañía son aquellos que, para contaminar un fichero *EXE* crean un fichero *COM* con igual nombre y con el atributo de oculto activado. El virus reside en el mencionado fichero *COM*. Si existen dos ficheros con igual nombre y con extensiones *EXE* y *COM*, el sistema operativo MS-DOS ejecuta primero el fichero con extensión *COM*. De esto se valen este tipo de virus. De esta forma, al intentar ejecutar un programa (fichero *EXE*) en realidad se ejecuta el virus (fichero *COM*) que se cargará en memoria y después, habitualmente, ejecutará el fichero *EXE* para que el usuario no sospeche nada.

El botón **Imprimir** permite obtener una copia impresa de los datos del virus cuya información se esté visualizando.

Si deseas consultar información sobre virus en general, o sobre algún virus en particular, puedes hacerlo a través de la **Enciclopedia de Virus** (www.pandasoftware.es/enciclopedia), en la Web de Panda Software.

Programación de Análisis Programados Predefinidos (Inicio del Sistema y de Windows)

Los análisis programados predefinidos de antemano (definidos en el antivirus por defecto), son los análisis al *inicio del sistema* -sólo en equipos con Windows 98/95- y al *inicio de Windows*. Su periodicidad o programación (definición de cuándo deben ponerse en marcha) se realiza a través de la pestaña **Programador** correspondiente a la configuración (véase el apartado Configuración de los Análisis - Ficha Programador, de esta ayuda).



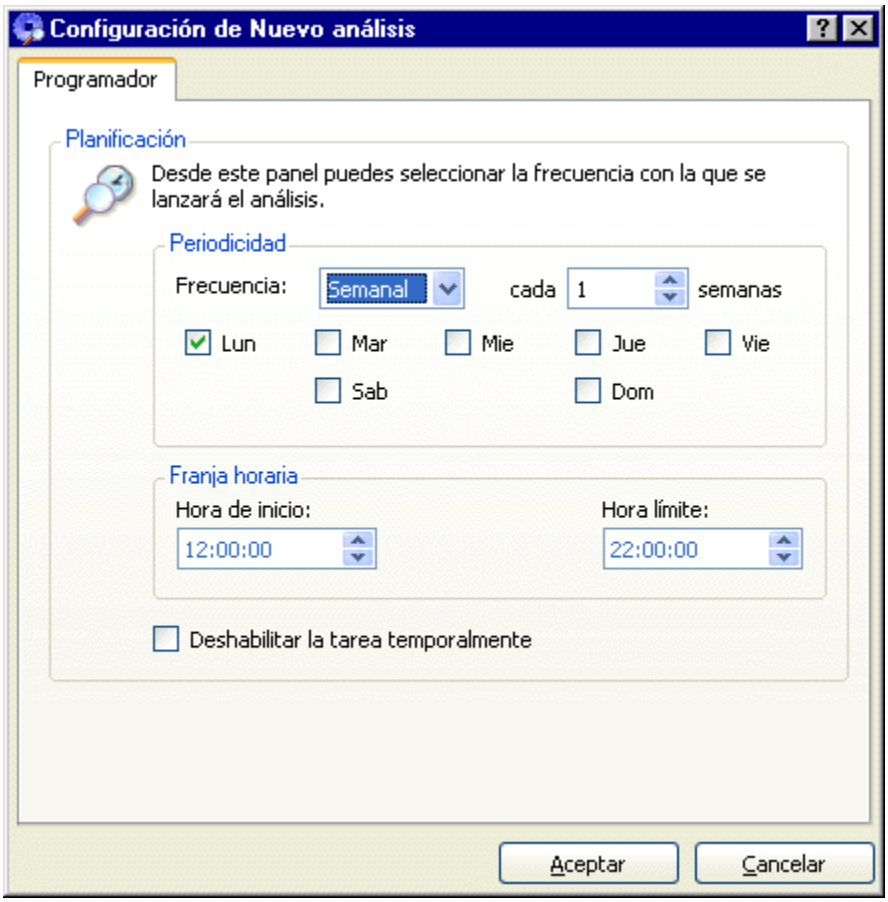
Dentro de esta pestaña del **Programador** se pueden programar los análisis predefinidos en el inicio (del sistema y de Windows) para que estos análisis predefinidos se lleven a cabo sólo en determinadas ocasiones. Las opciones disponibles son:

- **Siempre:** el análisis en el inicio se llevará a cabo en cada arranque del ordenador, o en cada inicio de Windows (dependiendo del tipo de análisis programado al inicio que hayamos seleccionado).
- **Cada "n" arranques:** el análisis en el inicio (del sistema, o de Windows) se ejecutará de manera regular pasados los arranques o inicios de Windows que se indiquen.
- **Cada "n" días:** el análisis en el inicio (del sistema o de Windows) se realizará de forma periódica de acuerdo a los días indicados.
- **Cada "día de la semana":** el análisis en el inicio (del sistema o de Windows) se ejecutará únicamente en el día de la semana indicado.

Deshabilitar tarea temporalmente. Si marcas esta casilla, el análisis programado no se realizará hasta que se vuelva a desmarcar.

Programación de Análisis Programados Creados por los Usuarios

Los análisis programados que crean los usuarios (**Nuevo análisis**), son diferentes en el tratamiento de su periodicidad a los análisis programados definidos de antemano. Éstos pueden ser creados y eliminados por los usuarios, cuando lo estimen oportuno. Su periodicidad o programación (definición de cuándo deben ponerse en marcha) se realiza a través de la pestaña **Programador** correspondiente a la configuración (véase el apartado Configuración de los Análisis - Ficha Programador, de esta ayuda).



Frecuencia

Mediante esta lista desplegable, se puede indicar cuándo se ejecutará el análisis programado. Los análisis programados se pueden ejecutar una única vez, cada cierto número de horas, de días o semanas o incluso ciertos días concretos de cada mes. Las opciones que se pueden seleccionar en la lista desplegable de **Frecuencia**, son las siguientes: **Una vez**, **Horario**, **Diario**, **Semanal**, **Mensual** y **Anual**. Esto significa que podremos escoger si se desea que se analice una única vez, cada cierto número de horas, días o semanas, unos ciertos días concretos de cada mes o un día concreto al año. Dependiendo de la frecuencia de análisis seleccionada en la lista desplegable, se solicitará la introducción de unos datos u otros en la sección central de la pantalla:

- **Día que se lanzará el análisis:** al seleccionar **Una vez** en la lista **Frecuencia**, se podrá seleccionar la fecha, mediante un calendario.
- **Intervalo de horas:** al seleccionar **Horario** en la lista **Frecuencia**, se podrá seleccionar cada

cuantas horas se debe iniciar el análisis.

- **Intervalo de días:** al seleccionar **Diario** en la lista **Frecuencia**, se podrá seleccionar cada cuantos días se debe iniciar el análisis.
- **Programación semanal:** al seleccionar **Semanal** en la lista **Frecuencia**, se podrá seleccionar cada cuantas semanas se debe iniciar el análisis y qué día de la semana (Lunes, Martes,…).
- **Programación mensual:** al seleccionar **Mensual** en la lista **Frecuencia**, se podrá seleccionar el número de orden del día (dentro del mes) en el que debe activarse el análisis (por ejemplo: todos los 17 de cada mes), o que éste se produzca el primero, segundo, tercero, cuarto o quinto día de cada mes (por ejemplo: el cuarto jueves de cada mes).
- **Día que se lanzará el análisis:** al seleccionar **Anual** en la lista **Frecuencia**, se debe indicar el número del día y del mes en el que el análisis programado debe ejecutarse.

Franja horaria

Existen además, otros datos que es necesario introducir en la configuración de la programación de un análisis programado definido o creado por el usuario. Éstos son los siguientes:

- **Hora de inicio:** indica la hora a la que comenzará el análisis.
- **Hora límite:** indica la hora límite hasta la que puede durar el análisis. Si llegada esta hora el análisis no ha finalizado, se cancelará la operación.

Deshabilitar la tarea temporalmente. Si marcas esta casilla, el análisis programado no se realizará hasta que se vuelva a desmarcar.

FAQ 1: Tengo Instalado Otro Antivirus, ¿Puedo Instalar Panda Antivirus Platinum?

Si el antivirus que tienes instalado en tu ordenador es Panda Antivirus Platinum, el proceso de instalación lo detectará. En tal caso, permitirá actualizarlo automáticamente (**Reparar**), o desinstalarlo (**Eliminar**).

En cualquier otro caso, si ya tienes instalado cualquier otro antivirus, es necesario que desinstales completamente dicho antivirus e instales posteriormente Panda Antivirus Platinum. Esto es debido a que las protecciones permanentes (residentes -de archivos y de correo-) de distintos antivirus podrían provocar conflictos entre ellas.

FAQ 2: ¿Por Qué No se Ejecuta Directamente el Proceso de Instalación al Insertar el CD-ROM de Panda Antivirus Platinum?

Es posible que la unidad de disco en la que has insertado el CD-ROM de Panda Antivirus Platinum no sea la correcta, o que no funciona correctamente. Compruébalo e introduce el CD-ROM en la unidad lectora correcta.

También es posible que tu ordenador tenga desactivada la función de ejecución automática. Si es así y el CD-ROM no muestra automátcamente el menú de opciones, ejecuta el fichero `SETUP.EXE`. Puedes ejecutarlo a través del *Explorador de Archivos de Windows*, o desde el botón **Inicio - Ejecutar**. Este fichero se encuentra en el directorio o carpeta `Platinum`.

Si deseas obtener información más ampliada, consulta el apartado, **Instalación de Panda Antivirus Platinum**, en la ayuda.

FAQ 3: ¿Cómo Ejecuto Manualmente el Proceso de Instalación?

Si insertas el CD-ROM de Panda Antivirus Platinum en el lector de CD, el proceso de instalación comenzará automáticamente, Si no es así, puedes ejecutarlo manualmente de alguno de los siguientes modos:

Mediante el *Explorador de Archivos de Windows*

1. Abre el *Explorador de Archivos de Windows*.
2. Selecciona la unidad de CD, donde has insertado el CD-ROM de Panda Antivirus Platinum (D:, por defecto).
3. Ejecuta el fichero *SETUP.EXE*, haciendo doble clic sobre él. Este fichero corresponde el programa que permite instalar el antivirus.

A través del botón Inicio de Windows

1. Pulsa el botón **Inicio** en la *Barra de tareas de Windows*.
2. Selecciona la opción **Ejecutar**.
3. Escribe la ruta y nombre de fichero que deseas ejecutar, o pulsa el botón **Examinar…**, para indicarlo. El fichero que debes ejecutar se encuentra en el CD-ROM de Panda Antivirus Platinum y su nombre es *SETUP.EXE*.
4. Cuando hayas indicado cuál es el fichero a ejecutar, pulsa el botón **Aceptar**.

Si has descargado tu Panda Antivirus Platinum desde Internet

1. Ejecuta el fichero que has descargado, haciendo dobre clic sobre él.
2. Esto comienza un proceso automático de instalación. Sigue los pasos que se te indican en él.

FAQ 4: ¿Qué Ocurre si Ya Tengo Instalado Panda Antivirus Platinum en mi Ordenador?

Si se trata de la misma versión, cuando ejecute el instalador, podrás **Reparar** o **Eliminar**. Esto quiere decir que se podrán restaurar los ficheros existentes de la instalación anterior (actualizarlos -**Reparar**-), o desinstalar el antivirus (borrarlo -**Eliminar**-). En cualquier otro caso, la instalación finalizará.

Si deseas obtener información más ampliada, consulta el apartado, Instalación de Panda Antivirus Platinum, en la ayuda.

FAQ 5: ¿Qué Idioma Debo Seleccionar al Comienzo de la Instalación?

Por defecto, se habrá seleccionado y podrás instalar el antivirus en el idioma de tu ordenador. Éste es el idioma en el que se realizará la instalación, si así lo deseas, y aquel en el que se instalará y funcionará Panda Antivirus Platinum en tu ordenador.

Al comenzar el proceso de instalación del antivirus, se detectará el idioma de tu ordenador. El proceso de instalación se realizará en dicho idioma, si tú no indicas lo contrario, y Panda Antivirus Platinum se instalará y funcionará en dicho idioma.

Si deseas obtener información sobre los pasos del proceso de instalación, consulta el apartado, Instalación de Panda Antivirus Platinum, en la ayuda.

FAQ 6: ¿Qué Ocurre si No Acepto el Acuerdo de Licencia?

Si no aceptas el Acuerdo de Licencia (es decir, si no pulsas el botón **Sí**) que aparece durante el proceso de instalación, el asistente finalizará y el antivirus no se instalará en tu ordenador.

FAQ 7: ¿Tengo que Realizar un Análisis de la Memoria y/o del Disco Duro Antes de Comenzar la Instalación?

Aunque no es necesario, sí es conveniente que lo hagas cuando así se indica durante el proceso de instalación. De esta forma estarás seguro de que no existe ningún virus, antes de continuar con la instalación del antivirus.

Si deseas obtener información sobre los pasos del proceso de instalación, consulta el apartado, Instalación de Panda Antivirus Platinum, en la ayuda.

FAQ 8: ¿Qué Ocurre si Realizo un Análisis Antes de la Instalación y se Detectan Virus?.

Si durante el proceso de instalación has indicado que se realice un análisis (marcando las casillas correspondientes al análisis de la memoria y/o del disco duro) y se detecta algún virus en el disco duro, podrás eliminarlo.

Si los virus se detectan en memoria, inserta el primer disquete de arranque o de rescate (libre de virus) en la disquetera y reinicia el ordenador. Después de hacerlo, comenzará un proceso automático. Entonces, sigue cada uno de los pasos que se te indiquen.

FAQ 9: ¿En Qué Directorio o Carpeta Debo Instalar el Antivirus?

Se aconseja elegir el directorio propuesto por defecto, durante el proceso de instalación.

No obstante, puedes hacerlo en otro directorio diferente, pero éste NO DEBE SER: ni el de directorio de Windows, ni el directorio *Archivos de Programa*, ni el de sistema, ni el directorio raíz del disco duro.

FAQ 10: ¿Qué Es el Análisis al Inicio del Sistema?

Si tienes activo el análisis al inicio del sistema, Panda Antivirus Platinum, analizará tu ordenador siempre que lo enciendas (sólo en ordenadores con Windows 98, o Windows 95).

FAQ 11: ¿Es Necesario Crear los Discos de Rescate?

Aunque no es necesario, si es MUY RECOMENDABLE.

De todas formas, si no los creas durante el proceso de instalación, siempre puedes crearlos en otro momento. Si no has creado los discos de rescate durante el proceso de instalación del antivirus, podrás crearlos posteriormente, del siguiente modo:

Desde los avisos en la ventana del antivirus

Si todavía nos has creado los discos de rescate, tu Panda Antivirus Platinum te mostará un aviso. Si accedes a la sección **Inicio** en la ventana del antivirus, verás que existe un área en la sección inferior, con el título **Avisos:**. Si aun no has creado estos discos, aparacerá el siguiente texto de aviso o sugerencia: ***Todavía no has creado los discos de recate. ¡Hazlo ahora!***. Pulsa sobre este texto, para crear los discos de rescate.

Desde el botón Inicio de Windows

También podrás crear los discos de rescate desde la opción que se encuentra accesible a través del botón **Inicio** de Windows. En tal caso, pincha sobre el botón **Inicio**. Entonces selecciona **Programas**. Pincha sobre el grupo Panda Antivirus Platinum. Finalmente selecciona la opción **Discos de rescate**.

FAQ 12: ¿Qué Son los Discos de Rescate?

Son varios disquetes que puedes generar durante el proceso de instalación de tu Panda Antivirus Platinum. También puedes proceder a su generación posteriormente, a través del botón Inicio de Windows, o desde los avisos en el área de inicio de Panda Antivirus Platinum (sección **Avisos**).

Los **Discos de Rescate** permiten iniciar un ordenador y además contienen el antivirus en línea de comandos (*PAVCL*). Arranca tu ordenador con el primero de los **Discos de Rescate** introducido en la disquetera. Se irá solicitando automáticamente la introducción de cada uno de los **Discos de Rescate** correspondientes. Sigue las instrucciones que se te indiquen.

Si deseas ampliar información sobre estos discos, consulta el apartado Discos de Rescate, en la ayuda.

FAQ 13: ¿Qué es el Registro OnLine y Por Qué Debo Registrarme?

Sólo cuando te has registrado, puedes utilizar los servicios incluidos en tu Panda Antivirus Platinum.

Por lo tanto, debes realizar este proceso para disfrutar de todos los servicios que acompañan a tu Panda Antivirus Platinum. Esto te conectará a la página de registro, en la Web de Panda Software.

Allí deberás rellenar un formulario, en el que se solicitará el código de activación correspondiente al antivirus y otra serie de datos. En cuanto lo hayas hecho, recibirás tu nombre de **usuario** y tu **contraseña**. Con ellos podrás utilizar correctamente los servicios de tu Panda Antivirus Platinum.

El registro online puede realizarse durante el proceso de instalación, o en cualquier otro momento después de haber instalado el antivirus. Si no te registras, no podrás utilizar los servicios incluidos en su Panda Antivirus Platinum.

FAQ 14: Al Finalizar la Instalación, ¿Debo Reiniciar mi Ordenador?

Si durante el proceso de instalación NO has instalado o activado el firewall de Panda Antivirus Platinum, NO es necesario que reinicies el ordenador. Además, no se te solicitará confirmación para ello.

Sólo en el caso de que hayas instalado / activado el firewall de Panda Antivirus Platinum (durante la instalación, o en otro momento), se te solicitará el reinicio de tu ordenador. El firewall estará instalado, pero sólo entrará en funcionamiento cuando hayas reiniciado tu equipo, una vez que el firewall haya sido instalado / activado..

Si durante el proceso de instalación no has instalado / activado el firewall, estarás protegido a través de la protección permanente antivirus (de archivos y de correo), pero no de los accesos no autorizados a tu ordenador -a través de la red-.

Sólo será conveniente reiniciar el sistema en algunas ocasiones (cuando hayas instalado / activado el firewall que acompaña a Panda Antivirus Platinum). En tal caso, el proceso de instalación / activación te pedirá confirmación para hacerlo de forma automática.

Nota: recuerda que, si has instalado el firewall, éste sólo comenzará a funcionar cuando hayas reiniciado tu ordenador.

FAQ 15: ¿Cómo Realizo un Análisis Predefinido?

Al seleccionar la opción **Análisis exhaustivo** en el **Panel de control** -dentro de la ventana del antivirus-, aparece una lista con todos los posibles análisis predefinidos (inmediatos y programados) y los elementos que pueden analizarse de forma independiente. Además, también puedes crear nuevos análisis (inmediatos y programados).

Para realizar cualquiera de los análisis ya predefinidos, márcalos y pulsa la opción **Analizar**. También puedes pulsar sobre él con el botón derecho del ratón y seleccionar la opción **Analizar**, o pulsar la tecla de función *F8*.

Si deseas obtener más información sobre los análisis, consulta el apartado ¿Cómo realizar un análisis (Inmediato o Programado)?, en la ayuda.

FAQ 16: ¿Cómo Sé Cuáles son los Elementos que Analizará un Determinado Análisis Predefinido?

Cuando seleccionas un análisis predefinido (o también alguno creado por cualquier usuario), ya sea éste inmediato o programado, el antivirus muestra información sobre él.

Estos datos aparecerán a la derecha del panel central como una sección o columna con el título **Elementos**. En dicha columna se enumeran todos los elementos que dicho análisis chequeará en busca de virus cuando sea puesto en marcha.

FAQ 17: ¿Puedo Crear un Nuevo Análisis?, ¿Cómo?

Sí, es muy sencillo. Sigue estos pasos:

1. Selecciona la opción **Análisis exhaustivo**, en el **Panel de control** (dentro de la ventana del antivirus).
2. Dentro del panel **Tareas de análisis**, selecciona la opción **Crear nuevo análisis**. También puedes pulsar con el botón derecho del ratón sobre uno de los análisis o elementos existentes en la lista y seleccionar la opción **Nuevo análisis**.
3. Esto mostrará un asistente para la creación de un nuevo análisis. Sigue los pasos del mismo.

Puedes consultar más información en el apartado ¿Cómo crear un nuevo análisis? (Inmediato / Programado), de la ayuda.

FAQ 18: ¿Puedo Borrar o Eliminar un Análisis que he Creado?

Sí, pero solamente los que se han creado, no los que vienen predefinidos por el antivirus. Eliminar uno de los análisis que el usuario ha creado, es muy sencillo. Sigue estos pasos:

1. En la lista de análisis y elementos a analizar, selecciona el nombre del análisis que deseas eliminar.
2. En el panel **Tareas de análisis**, seleccione opción **Eliminar análisis**.
3. Se pide confirmación para borrar dicho análisis. Pulse el botón **Sí**.

El análisis desaparecerá de la lista de análisis.

Puedes consultar más información en el apartado ¿Cómo borrar o eliminar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 19: ¿Cómo Puedo Analizar una sola Carpeta o un sólo Fichero?

Panda Antivirus Platinum te permite analizar una sola carpeta o un sólo fichero de forma individual o independiente, de dos formas:

Mediante el análisis contextual en el *Explorador de Archivos de Windows*

1. Accede al *Explorador de Archivos de Windows*, a través del botón **Inicio** de Windows, o a través de alguno de los accesos directos que tengas a él.
2. Selecciona el fichero o carpeta (o varios de ellos) que deseas analizar.
3. Pulsa sobre el/los ficheros o carpetas seleccionados con el botón derecho del ratón (menú contextual).
4. Selecciona la opción **Analizar con antivirus Platinum**.
5. Se ejecuta el análisis del elemento (fichero o carpeta que hayas seleccionado). Esto es lo que se denomina *análisis contextual*.

Desde la ventana de Panda Antivirus Platinum

1. Estando en la ventana del antivirus, selecciona la opción **Análisis exhaustivo**, del **Panel de control**.
2. Tanto si deseas analizar un determinado directorio (carpeta), como si lo que deseas es analizar un determinado fichero (archivo), debes localizarlo. Para hacerlo, sigue estos pasos:

    - Despliega la sección **Analizar otros elementos**, pulsando el signo + que se encuentra a su izquierda.
    - Selecciona la unidad de disco en la que se encuentra la carpeta o fichero a analizar (por ejemplo, Disco local C:).
    - Abre su estructura de directorios, pulsando el signo + que aparece a su izquierda.
    - Desciende por la rama o ruta de directorios en cuestión, hasta llegar al directorio o fichero que deseas analizar. Utiliza para ello, el signo + que encontrarás a la izquierda de todos los directorios.

3. Cuando hayas llegado al directorio (carpeta) o fichero final que deseas analizar, pincha sobre él con el botón derecho del ratón (menú contextual).
4. Selecciona la opción **Analizar** y el elemento seleccionado (carpeta o fichero) será analizado.

Puedes obtener más información sobre el análisis de elementos independientes, en el apartado ¿Cómo realizar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 20: ¿Cómo Puedo Hacer un Análisis de Todo el Sistema?

El análisis de Todo el Sistema, implica el análisis de todos y cada uno de los elementos (memoria, discos, correo,…) de tu ordenador que podrían contener virus. Para realizar el análisis de todo el sistema sigue estos pasos:

1. En la ventana del antivirus, selecciona la opción **Análisis exhaustivo**, dentro del **Panel de control**.
2. Dentro de los Análisis inmediatos, selecciona la opción **Analizar todo el sistema**. A la derecha se mostrarán todos los elementos que serán analizados.
3. En el panel de **Tareas de análisis**, selecciona la opción **Analizar**. También puedes pulsar con el botón derecho del ratón sobre la opción **Analizar todo el sistema** y seleccionar la opción **Analizar**.

Puedes obtener más información consultando el apartado ¿Cómo realizar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 21: ¿Qué Significa Analizar el Sistema Operativo?

Algunos virus, además de realizar sus acciones habituales, realizan ciertas modificaciones o alteraciones en el Sistema Operativo. Éstas suelen centrarse en la configuración del sistema, cambios en el *Registro de Windows* y en otros ficheros, etc.

Cada una de ellas produce efectos secundarios que, tras la detección y desinfección del virus con otros programas antivirus, no desaparecen (ya que la desinfección no implica la correcta reconfiguración del sistema).

Sin embargo, tu Panda Antivirus Platinum, ¡NO SOLAMENTE DETECTA Y DESINFECTA!. Además, ¡RESTAURA LA CONFIGURACIÓN ORIGINAL DEL SISTEMA OPERATIVO!, si ésta se vió afectada por algún virus de este tipo.

Para conseguir eliminar los posibles cambios realizados por este tipo de virus en la configuración, haz lo siguiente:

1. En la ventana del antivirus selecciona la opción **Análisis exhaustivo**, del **Panel de control**.
2. Dentro de los **Análisis inmediatos**, despliega la lista **Analizar otros elementos**, pulsando el signo + que se encuentra a la izquierda.
3. Selecciona la opción **Sistema Operativo** que aparecerá en primer lugar.
4. En el panel de **Tareas de análisis**, selecciona la opción **Analizar**. También puedes pulsar con el botón derecho del ratón sobre la opción **Sistema Operativo** y seleccionar la opción **Analizar**.

Puedes obtener más información consultando el apartado ¿Cómo realizar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 22: Quiero Información sobre un Virus: ¿Dónde la Obtengo?

Los informes muestran los nombres de los virus detectados. Además, tu Panda Antivirus Platinum cuenta con información sobre las características más destacadas de cada uno de ellos. Para consultarla, haz lo siguiente:

1. En la ventana del antivirus, pulsa el botón **Lista de virus**, que se encuentra en la barra de herramientas.
2. Dentro del recuadro **Buscar Virus**, escribe el nombre del virus del que deseas obtener información. La lista de virus se colocará automáticamente en él.
3. Selecciónalo con el puntero del ratón. Entonces, se mostrará una ficha de información básica sobre ese virus (Nombre, Alias, Origen, Fecha, Tamaño,…).

Además, si deseas consultar información más ampliada sobre él, puedes encontrarla en la Enciclopedia de Virus, en la Web de Panda Software (www.pandasoftware.es/enciclopedia).

FAQ 23: ¿Qué Hago si un Fichero se Considera Sospechoso?

Como medida preventiva, y en previsión de que realmente se encuentre infectado, podrás ponerlo en cuarentena. Esto quiere decir que no podrá ser utilizado y otros ficheros no tendrán relación con él. Con ello evitarás que, si finalmente se encuentra infectado, éste extienda su infección.

Para poner un fichero en cuarentena, debes utilizar el Hospital de ficheros, incluido en Panda Antivirus Platinum. Para hacerlo, sigue estos pasos:

1. En la ventana del antivirus, selecciona la opción **Hospital** del **Panel de control**.
2. Si quieres añadir un determinado fichero a la cuarentena, pincha sobre la opción **Añadir archivo**, en el panel **Cuarentena**.
3. Aparece un cuadro de diálogo a través del cual debes seleccionar el fichero que quieres poner en cuarentena. Selecciónalo y pulsa el botón **Abrir**.
4. Se muestra un aviso en el que se indica que el fichero que vas a poner en cuarentena, desaparecerá de su ubicación original, moviéndose a la carpeta de ficheros en cuarentena. Si estas convencido de ello, pulsa el botón **Sí**.
5. El fichero seleccionado se incluirá en la lista de ficheros en cuarentena.

Nota: recuerda que si agregas un fichero a la cuarentena, éste se moverá desde su ubicación original a la correspondiente en la cuarentena. Esto significa que desaparecerá del directorio en el que se encontraba (no se ha borrado). Por lo tanto, es posible que algunas aplicaciones que lo utilizaban, no funcionen, o no lo hagan correctamente.

Además, una vez el fichero está en cuarentena, podrás realizar determinadas operaciones con él: desinfectarlo, enviarlo a Panda Software para su estudio, eliminarlo (borrarlo definitivamente de todas partes), o mostrar información sobre él.

Puedes enviar al Laboratorio de Virus de Panda Software, los ficheros que se encuentren en cuarentena. para que los analicemos y estudiemos. ¡Te entregaremos la solución antivirus correspondiente, o la certificación de que los ficheros no se encuentran infectados!. Hazlo del siguiente modo:

1. En la ventana del antivirus, selecciona la opción **Hospital**, del **Panel de control**.
2. Selecciona el fichero de la cuarentena que deseas enviarnos.
3. Selecciona la opción **Enviar a Panda**, en el panel **Cuarentena**. También puedes pulsar con el botón derecho del ratón sobre él y seleccionar la opción Enviar.

Otra forma mediante la cual es posible poner en cuarentena ficheros sospechosos, e indirectamente enviarlos a Panda Software para su estudio, es a través de los análisis. En el momento en el que se realiza un determinado análisis, es posible que se detecte algún fichero sospechoso. Si las acciones del análisis en cuestión están configuradas para que se muevan los ficheros a la cuarentena, dichos ficheros también serán aislados de los demás, moviéndolos a la Cuarentena.

Puedes obtener más información consultando el apartado Hospital, de la ayuda.

FAQ 24: ¿Cómo Puedo Enviar un Archivo a Panda?

Gracias a tu Panda Antivirus Platinum, ¡es muy sencillo!, él se encarga de realizar el envío. Puedes hacerlo de dos formas:

Desde la cuarentena del Hospital

1. En la ventana del antivirus, selecciona la opción **Hospital**, del **Panel de control**.
2. Selecciona entonces los ficheros en cuarentena que deseas enviarnos a Panda Software para que los estudiemos y analicemos.
3. En el panel **Cuarentena**, selecciona la opción **Enviar a Panda**. También puedes realizar esta operación, seleccionando la opción **Enviar** del menú contextual (botón derecho del ratón sobre los ficheros marcados).
4. Cada uno de los ficheros seleccionados, será analizado y si no se encuentra infectado, se mostrará un mensaje indicándolo. En dicho mensaje se pedirá además confirmación para enviarlo. Pulsa el botón **Sí**, para confirmar el envío.
5. Comienza el asistente para el envío de ficheros sospechosos, indicándo que debe existir una conexión abierta a Internet. Pulsa el botón **Siguiente**.
6. En la sección **Indica tu dirección de correo electrónico**, escribe correctamente tu e-mail. En la sección **Descripción del problema**, indícanos CLARA y COMPLETAMENTE cuál es el problema que tienes con estos ficheros y en qué circunstacias se ha dado ese problema. Después pulsa el botón **Siguiente**.
7. Se muestra la lista de ficheros que habías seleccionado. Todos ellos serán enviados a Panda Software para su estudio. En este paso, puedes quitar de la lista cualquiera de los ficheros, para que no sean enviados. Esto lo puedes hacer, seleccionándolos y pulsando el botón **Eliminar archivos**. Cuando tengas la lista de ficheros que deseas enviar, pulsa el botón **Siguiente**.
8. Se mostrará el tamaño del mensaje que se ve e enviar. Para que los ficheros seleccionados sean enviados a Panda Software, pulsa el botón **Enviar**. Puedes impedir el envío, pulsando el botón **Cancelar**.

Desde el panel de control

1. En la ventana del antivirus, selecciona la opción **Servicios**, del **Panel de control**.
2. Selecciona entonces la opción **Envío a Panda de archivos sospechosos (S.O.S. Virus)**.
3. Esto te mostrará las instrucciones que te permitirán el envío de ficheros sospechosos a Panda Software.
4. Sigue las instrucciones que allí se te indican.

FAQ 25: He Desinfectado un Virus, ¿Por Qué Sigue Apareciendo su Nombre en el Informe?

Al finalizar cualquier análisis, tu Panda Antivirus Platinum muestra un resumen de lo ocurrido durante el mismo. Desde éste, puedes pulsar la opción **Informe**, para ver las incidencias que hayan podido tener lugar en él.

Además, Panda Antivirus Platinum guarda un registro en el que almacena las incidencias ocurridas en TODOS los análisis que se han ido realizando. Esto es lo que se denomina, Informe de todos los análisis realizados. Para consultarlo al completo, debes pulsar el botón **Informe** que se encuentra en la barra de herramientas, dentro de la ventana del antivirus. Esto mostrará todas las incidencias de los análisis realizados (Comienzo, Finalizado, nombres de los virus detectados, etc).

Puede ser que, en uno de dichos análisis (o en varios de ellos) se haya detectado un virus o más. Éste habrá sido desinfectado y eliminado por Panda Antivirus Platinum. El que se haya detectado y eliminado, no implica que no se muestre la información de dicha incidencia en el informe. De todas formas, si deseas que no se muestre dicha incidencia, no tienes más que pulsar el botón **Borrar informe**. Con ello consigues que todo el contenido del informe se elimine. A partir de ese instante, éste sólo mostrará las incidencias que tengan lugar en los siguientes análisis que realices. Por lo tanto el nombre de dicho virus, desaparecerá del informe.

Puedes obtener más información consultando el apartado El informe de los análisis, de la ayuda.

FAQ 26: ¿Qué Ocurre si Desactivo la Protección Permanente?

La protección permanente antivirus (de archivos y correo), te protege en todo momento (siempre que la mantengas activa). Analiza continuamente todos los ficheros implicados en las operaciones que se realizan (del sistema y tuyas) y los que se transmiten a través de correo electrónico. Es MUY ACONSEJABLE tenerla activa. Si desactivas ambas protecciones, o alguna de ellas, no estarás protegido. Por defecto (tras instalar el antivirus), la protección permanente antivirus de archivos y de correo está activa.

Además (siempre que hayas instalado y activado el firewall), cuentas con otro tipo de protección permanente muy interesante: la del firewall. Este tipo de protección actúa como un *muro de fuego* o *cortafuegos* entre tu ordenador y el exterior. Se trata de una barrera o protección adicional al antivirus que permite a un sistema mantener a salvo la información (de entrada y salida) cuando el ordenador accede a otras redes -como Internet-.

Desde el menú **Inicio**, del **Panel de control** podrás consultar si dichas protecciones se encuentran activas o inactivas, consultando la sección **Estado de la protección permanente**. Además, el icono del antivirus en la *Barra de tareas de Windows*, tendrá color si alguna de las protecciones permanentes (Antivirus -de archivos o de correo- y/o Firewall) está activa. Estará gris si ninguna de estas protecciones está activa.

Puedes activar y desactivar la protección permanente antivirus (de archivos o de correo) y firewall, a través del menú **Protección permanente**, en el **Panel de control** de la ventana del antivirus. Desde allí, podrás pinchar sobre las opciones **Desactivar** / **Activar**, en cada uno de los paneles correspondientes: Protección **Antivirus** y protección **Firewall**.

Puedes obtener más información consultando el apartado Análisis permanente o protección permanente (Antivirus -archivos y correo- y Firewall), de la ayuda.

FAQ 27: ¿Cómo Sé que el Antivirus está Actualizado?

Las actualizaciones de tu Panda Antivirus Platinum consisten en la actualización del denominado Archivo de Identificadores de Virus (el encargado de detectar los virus - cada día surgen más de 20) y del propio programa antivirus.

Éstas se pueden realizar diariamente, de forma automática o manual. Si has configurado tu antivirus para que él mismo se actualice cuando lo necesite (actualización automática), estarás siempre actualizado. Tu Panda Antivirus Platinum se actualizará cuando detecte una conexión abierta a Internet y detecte la necesidad de actualizarse.

Para conocer el grado de actualización del antivirus, sólo debes observar la **Fecha del archivo de identificadores de virus**. Para conocer dicho dato, selecciona el menú **Inicio**, en el **Panel de control**, dentro de la ventana del antivirus. Esta información se muestra al comienzo de la sección **Estado del programa**.

Además, esta información se muestra de forma gráfica en la propia ventana del antivirus. La barra de estado muestra (en la sección izquierda -justo debajo del Panel de control-), una barra de progreso. Esta estará coloreada completamente en verde si el antivirus se encuentra completamente actualizado. Además, si pulsas con el puntero del ratón sobre ella, aparece un cuadro de diálogo donde se te amplía la información. Desde dicho cuadro de diálogo, puedes actualizar tu Panda Antivirus Platinum, mediante la opción **Pulsa aquí**.

Por otra parte, podrás conocer el grado de actualización de tu Panda Antivirus Platinum, a través del icono correspondiente a la protección permanente (el icono del oso Panda) que aparece en la *Barra de tareas de Windows* (junto al reloj del sistema). Si dicho icono aparece (la protección permanente se encuentra cargada y activa) y colocas el puntero del ratón sobre él, se te indicará le fecha en la que se actualizó el antivirus por última vez.

Puedes obtener más información consultando el apartado ¿Qué es una Actualización?, de la ayuda.

FAQ 28: ¿Cómo Configuro la Actualización del Antivirus?

Es posible indicar el funcionamiento de las actualizaciones en Panda Antivirus Platinum. Para definir las características de la actualización, haz lo siguiente:

1. Dentro de la barra de herramientas que se encuentra en la sección superior de la ventana del antivirus, pulsa el botón **Opciones generales**.
2. En el cuadro de diálogo que aparece, accede a la ficha **Actualización**, pulsando sobre su nombre de etiqueta.
3. Puedes indicarle al antivirus que debe actualizarse automáticamente y cómo debe hacerlo. Esto es posible gracias a las siguientes casillas de verificación:

    - **Activar actualizaciones automáticas**. Si marcas esta casilla, el antivirus se actualizará por sí sólo, de forma automática (siempre que la actualización sea necesaria y se encuentra abierta una conexión a Internet).
    - **Notificarme al realizar una actualización automática**. Cuando el antivirus finalice su actualización automática, te lo indicará a través de un mensaje en pantalla.

4. La actualización es uno de los servicios incluidos en Panda Antivirus Platinum, por lo tanto es necesario estar registrado como usuario para poder utilizar dicho servicio. En la sección **Contraseña**, debes incluir tu nombre de **Usuario** y la **Contraseña** que se te asignó al registrarse (los que recibiste desde Panda Software, después de haberte registrado).
5. Es necesario indicar el lugar desde el cual el antivirus debe recoger los ficheros necesarios para actualizarse, entre dos posibilidades: **Internet**, o **Diskette, CD ROM ó Red Local**. Si te actualizas a través de Internet utilizando un módem para conectarte, no marques la casilla **Acceso a través de Proxy**. Si accedes a Internet a través de una red de ordenadores, mediante un servidor proxy, debes marcarla y determinar las características de acceso, mediante el botón **Configurar…** (**Dirección IP** y **Puerto** del proxy, así como **Nombre de usuario** y **Contraseña** que te permiten el acceso al proxy -no tienen nada que ver con el usuario y contraseña de registro-).

Cuando vayas a realizar una actualización manual (mediante el botón **Actualizar** en la barra de herramientas del antivirus), podrás configurar también las características de la actualización. Esto lo podrás hacer pinchando sobre la opción **Configurar actualizaciones** que aparece en la primera ventana del asistene de actualización.

Puedes obtener más información consultando el apartado Configuración general del antivirus - actualización, de la ayuda.

FAQ 29: El Antivirus, ¿Se Actualiza Automáticamente o Debo Realizar Actualizaciones Manuales?

Tu Panda Antivirus Platinum permite las dos posibilidades.

Para la realización de una actualización manual, sigue estos pasos:

1. Pulsa el botón **Actualizar**, en la barra de herramientas del antivirus.
2. Si deseas determinar las características que debe tener la actualización, pulsa sobre la opción **Configurar actualizaciones**, que se mostrará en el primer paso del asistente de instalación. Puedes consultar más información en el apartado Configuración General del Antivirus - Actualización.
3. Pulsa el botón **Siguiente** y el antivirus se actualizará.

Nota: también puedes realizar una actualización, seleccionando la opción **Actualización del antivirus**, en el menú **Servicios**.

Para la realización de una actualización automática o determinar que ésta debe tener lugar, sigue estos pasos:

1. Dentro de la barra de herramientas que se encuentra en la sección superior de la ventana del antivirus, pulsa el botón **Opciones generales**.
2. En el cuadro de diálogo que se muestra, selecciona la ficha **Actualización**.
3. Para indicar que las actualizaciones deben realizarse de forma automática, marca la casilla **Activar actualizaciones automáticas**. Si además quieres ser informado/a cuando se haya realizado una de estas actualizaciones, marca la casilla **Notificarme al realizar una actualización automática**.

FAQ 30: ¿Cuál Es la Frecuencia Correcta de Actualización?

Las actualizaciones se pueden realizar a diario, ya que Panda Software pone a disposición de sus clientes un nuevo archivo de identificadores de virus todos los días. Lo más aconsejable sería realizar una actualización, al menos una vez a la semana.

No obstante, si esto te supone un trastorno, puedes delegar esta función a tu Panda Antivirus Platinum. De esta forma, él mismo realizará una actualización automática, por su cuenta, cuando así lo necesite y detecte una conexión abierta a Internet. De esta forma, no tendrás que estar pendiente de las actualizaciones.

FAQ 31: ¿Qué Es y Cómo Realizo un Análisis Predefinido o Predeterminado?

Los análisis predefinidos o predeterminados son todas aquellas ‘‘tareas’’ de análisis que ya están creadas de antemano en el antivirus. Éstas pueden ser inmediatas o programadas y nos facilitan el trabajo, permitiendo realizar análisis de muchos elementos, con realizar un solo clic de ratón.

Para realizar un análisis predeterminado, sigue estos pasos:

1. Dentro de la ventana del antivirus, selecciona la opción **Análisis exhaustivo**, en el **Panel de control**.
2. Encontrarás dos grandes apartados: **Análisis inmediatos** (dentro de él encontrarás también la sección **Analizar otros elementos**) y **Análisis programados**.
3. Dentro de cada una de ellas, se encuentran los análisis predefinidos. Éstos son los siguientes:

    - Para el caso de los análisis inmediatos: **Analizar todo el sistema**, **Analizar discos duros**, **Analizar todo el correo electrónico** y **Analizar la disquetera**. Además, dentro de la sección Analizar otros elementos, podrás indicar sobre que elementos concretos deseas realizar un análisis.
    - Para el caso de los análisis programados: **Análisis al inicio del sistema** -sólo en equipos con Windows 98/95- y **Análisis al inicio de Windows**.

4. Para realizar alguno de estos análisis predefinidos (todo el sistema, discos duros, todo el correo electrónico, disquetera, inicio del sistema, o inicio de Windows), selecciónalo.
5. Pincha sobre la opción **Analizar**, en el panel **Tareas de análisis**. También puedes pulsar sobre cualquiera de ellos con el botón derecho del ratón y seleccionar la opción **Analizar**, o pulsar la tecla de función *F8*

Puedes obtener más información consultando el apartado ¿Cómo realizar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 32: ¿Cómo Selecciono los Elementos que Deseo Analizar?

En ocasiones puede ser necesario analizar un determinado grupo de elementos. Si todos éstos no se encuentran incluidos en uno de los análisis inmediatos, podrían ser analizados de estas dos formas:

De forma independiente, uno por uno. En este caso los elementos serán analizados uno a uno de forma secuencial. Para analizar elementos independientes, sigue estos pasos:

1. En el árbol de elementos a analizar (dentro de la rama **Analizar otros elementos**), selecciona el primero de los elementos que deseas analizar.
2. Pulsa la opción **Analizar**, en el panel **Tareas de análisis**, o pulsar sobre dicho elemento con el botón derecho del ratón y seleccionar la opción **Analizar** del dicho menú contextual.
3. Deberías repetir los pasos 1 y 2, con cada uno de los elementos que quieres analizar.

Esta no parece ser la solución más acertada si lo que deseas es analizar un gran grupo de elementos. En tal caso, es más aconsejable utilizar la segunda posibilidad que mostramos a continuación

Creando un nuevo análisis que los agrupe a todos. Si creas un nuevo trabajo o tarea de análisis, podrás indicar todos y cada uno de los elementos que deseas analizar. Posteriormente, cuando indiques que se realice dicho análisis, serán analizados al mismo tiempo todos y cada uno de estos elementos. Además, como el análisis creado existirá hasta que lo elimines, podrás realizar dicho análisis todas las veces que así lo desees. Para crear un análisis con varios elementos a analizar, sigue estos pasos:

1. En el panel **Tareas de análisis**, selecciona la opción **Crear nuevo análisis**. Esto abre un asistente para la creación de análisis.
2. Pulsa el botón **Siguiente**.
3. Agrega a la lista los elementos que deseas analizar (uno a uno), pulsando el botón **Añadir**.
4. Selecciona uno de los elementos de la lista y pulsa el botón **Aceptar**.
5. Repite los pasos 4 y 5 hasta que hayas incluido en la lista todos los elementos que quieres sean analizados. Si deseas eliminar alguno de los elementos que ya has seleccionado, márcalo y pulsa el botón **Quitar**.
6. Pulsa el botón **Siguiente**.
7. Puedes indicar el comportamiento del análisis que estás creando, pulsando el botón **Configuración**. Además, en este paso, puedes indicar si el análisis debe ser inmediato o programado. Por defecto será inmediato, pero si deseas que sea programado, marca la casilla **Quiero que esta tarea se realice periódicamente**. En tal caso, se activará el botón **Planificación**. Si lo pulsas, podrás indicar la periodicidad del análisis programado (cuándo debe realizarse éste de forma automática).
8. Escribe el nombre que quieres dar a la tarea que acabas de crear, para que sea almacenado con dicho **Nombre de análisis**.
9. Pulsa el botón **Siguiente**.
10. Pulsa el botón **Finalizar**.

Puedes obtener más información consultando el apartado ¿Cómo crear un nuevo análisis? (Inmediato / Programado), de la ayuda.

FAQ 33: ¿Se Pueden Eliminar o Borrar los Análisis Existentes?, ¿Cómo?

Solamente se pueden eliminar o borrar los análisis o tareas de análisis que hayan creado los usuarios del antivirus. Es decir, los que no están creados por defecto y hayan sido creados utilizando la opción nuevo análisis.

Nunca se podrán borrar los análisis predefinidos o predeterminados (ni inmediatos: **todo el sistema**, **discos duros**, **todo el correo electrónico**, **disquetera**; ni los programados: **inicio del sistema** e **inicio de Windows**), ni los elementos (**Analizar otros elementos**) sobre los que se puede ejecutar un análisis inmediato en cualquier momento.

Para eliminar o borrar uno de los análisis que hayas creado, debes seguir estos pasos:

1. En la ventana del antivirus, selecciona el menú **Análisis exhaustivo**, dentro del **Panel de control**.
2. Selecciona el análisis que deseas eliminar. Si se trata de un análisis inmediato, se encontrará justo encima de la sección **Analizar otros elementos**. Si se trata de un análisis programado, se mostrará al final de los análisis programados.
3. Cuando lo hayas seleccionado, selecciona la opción **Eliminar análisis**, en el panel **Tareas de análisis**. También puedes pulsar con el botón derecho del ratón sobre dicho análisis y seleccionar la opción **Eliminar análisis**.

Puedes obtener más información consultando el apartado ¿Cómo borrar o eliminar un análisis? (Inmediato / Programado), de la ayuda.

FAQ 34: ¿Cómo Desinstalo Panda Antivirus Platinum?

Puedes realizar la desinstalación de tu Panda Antivirus Platinum de dos formas:

Desde el botón Inicio de Windows. Es la forma más aconsejable. Para hacerlo de este modo, sigue estos pasos:

1. Pulsa sobre el botón **Inicio** de Windows.
2. Selecciona **Programas**.
3. Selecciona el grupo de programas **Panda Antivirus Platinum**.
4. Dentro de él, selecciona la opción **Desinstalar - Reparar**.
5. Aparece un cuadro de diálogo en el que debes pulsar el botón **Eliminar**. En ese momento, comenzará la eliminación y desinstalación de Panda Antivirus Platinum.

Desde el Panel de Control de Windows. De forma adicional, el antivirus puede desinstalarse como cualquiera de los programas que se encuentran instalado en el ordenador. Aunque esta no es la forma más aconsejable de hacerlo, deberías seguir estos pasos:

1. Pulsa sobre el botón **Inicio** de Windows.
2. Selecciona **Configuración**.
3. Selecciona el grupo de programas **Panel de Control**.
4. Haz doble clic sobre el icono **Agregar o quitar programas**.
5. En la lista de programas instalados, selecciona **Panda Antivirus Platinum**.
6. Pulsa el botón **Agregar o quitar**. En ese momento, comenzará la eliminación y desinstalación de Panda Antivirus Platinum.

Configuración General del Antivirus - Actualización

Nota: para realizar actualizaciones del antivirus, debes haberte registrado previamente como usuario de Panda Antivirus Platinum. Solamente en este caso, podrás utilizar el servicio de actualizaciones. Si deseas consultar más información, accede a la sección Registro online de esta ayuda, o a la página Web de Registro online de Panda Software, para registrarte.

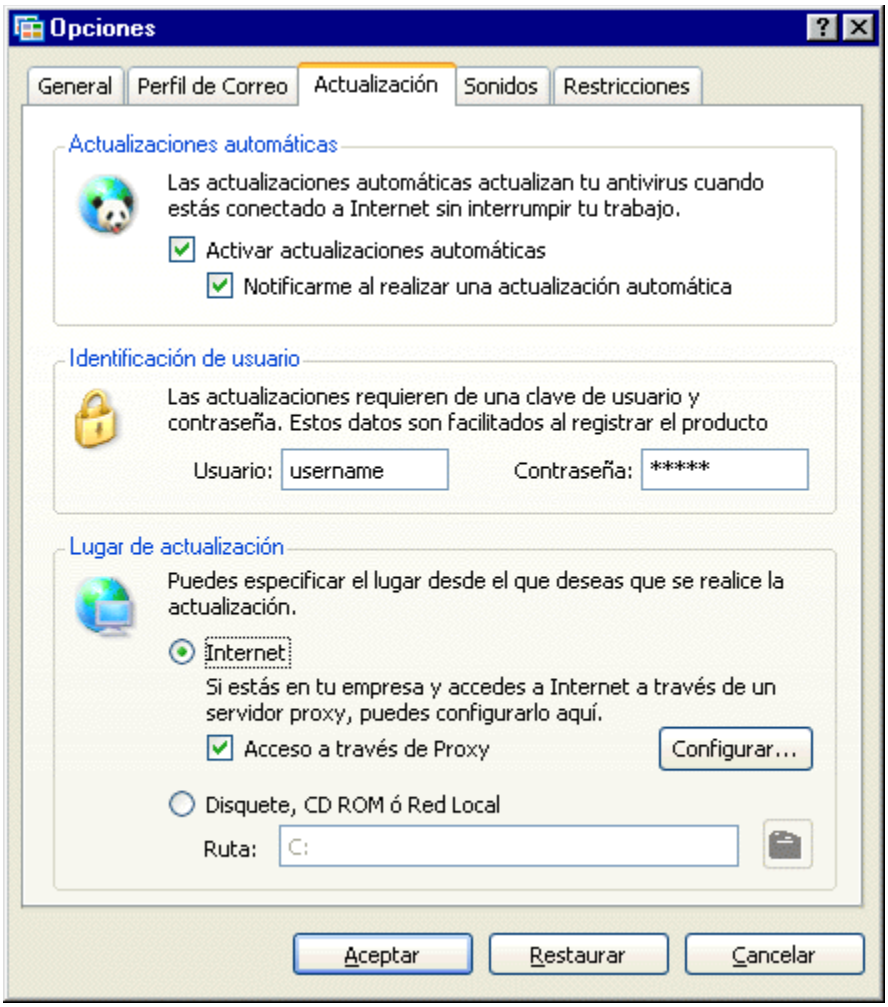
Para que un antivirus esté vivo, a la última, y sea capaz de detectar y eliminar todos los nuevos virus que van surgiendo a diario, debe estar completa y correctamente actualizado. Esto quiere decir que el fichero que permite al antivirus la detección de cada uno de los virus (*Archivo de Identificadores de Virus*, o *Fichero de Firmas de Virus*), debería ser el último que exista. Además, el propio programa antivirus puede contar con cambios sustanciales con el paso del tiempo, que también sería necesario actualizar.

Panda Software ofrece a sus clientes registrados la actualización DIARIA del archivo de identificadores de virus (Update), a través de Internet. Este fichero -que permite al antivirus identificar a cada uno de los virus-, puede encontrarse por lo tanto en diferentes ubicaciones (en un disquete, en un CD-ROM, en una red de ordenadores, o en Internet). Panda Software mediante su página de actualizaciones en la Web, permite que todos los clientes registrados pueden descargarse el archivo de identificadores de virus que se prepara TODOS LOS DÍAS. La dirección de la página de actualizaciones de Panda Software, es: www.pandasoftware.es/es/actualizaciones.asp.

Del mismo modo, el propio programa antivirus también se debe actualizar (Upgrade). Así lo hará cuando lo indiquemos, o cuando él mismo detecte esta necesidad. Este proceso también se realiza a través de la página de actualizaciones en la Web de Panda Software.

Por lo tanto, podrás indicar a tu Panda Antivirus Platinum desde dónde debe obtener el archivo de identificadores de virus: disquete, CD-ROM, Red de ordenadores (Red Local), o Internet. Además, también puedes indicarle que se actualice él por si mismo, sin que tengas que realizar ninguna operación (esto lo hará automática y transparentemente al usuario, cuando detecte una conexión abierta a Internet, sin interferir para nada en cualquier otra operación que se esté realizando).

Es posible configurar las siguientes características de actualización, pulsando el botón **Opciones generales** en la barra de herramientas del antivirus y seleccionando la ficha **Actualización**.



También es posible configurar o determinar las características de las actualizaciones, durante el proceso de actualización manual. En tal caso, si has comenzado una actualización manual pulsando el botón **Actualizar** en la barra de herramientas, selecciona la opción **Configurar actualizaciones**, del asistente.

Actualizaciones automáticas

Puedes actualizar tu Panda Antivirus Platinum, cuando lo desees y del modo que quieras. Además, éste también es capaz de actualizarse automáticamente por sí solo, cuando lo necesite y exista una conexión a Internet abierta. En tal caso, siempre que esté marcada la casilla **Activar actualizaciones automáticas** existente en esta sección, el antivirus se actualizará por su cuenta. Por defecto, Panda Antivirus Platinum se actualiza automáticamente.

Cuando Panda Antivirus Platinum detecta que hay abierta una conexión a Internet, se conecta automáticamente a la página de actualizaciones de Panda Software. Este proceso es transparente al usuario. Es decir, no serás consciente de que el antivirus se está actualizando y dicha actualización no consumirá recursos adicionales en el ordenador, ni afectará a otras tareas, aplicaciones, o procesos que se estén ejecutando. Puedes seguir trabajando del mismo modo, sin que se aprecien disminuciones en las capacidades del equipo. Cuando la actualización automática haya finalizado, el antivirus te lo indicará mediante un mensaje de aviso (si marcaste la casilla **Notificarme al realizar una actualización automática**, en la sección correspondiente de la configuración.

Identificación de usuario. Solamente podrás realizar actualizaciones (éste es uno de los servicios incluidos en Panda Antivirus Platinum), si previamente te has registrado como usuario (para obtener más información, consulta el apartado Registro online, en esta ayuda). Cuando te hayas registrado (utilizando tu correspondiente código de activación), recibirás desde Panda Software los datos que te identifican como usuario registrado de Panda Antivirus Platinum: un nombre de **Usuario** y una **Contraseña**. Estos datos son los que te permitirán utilizar todos los servicios incluidos en tu Panda Antivirus Platinum. En esta sección debes introducir dichos datos. En caso contrario, la actualización no será posible.

Lugar de actualización. Existen dos tipos de ubicaciones desde las cuales el antivirus puede actualizar el archivo de identificadores de virus (o fichero de firmas de virus, pav.sig):

- **Internet.** El archivo de identificadores de virus (fichero de firmas), será recogido de la página de actualizaciones en la Web de Panda Software. También se actualizará el propio programa antivirus, en caso de ser necesario.

  Para que sea posible llevar a cabo una actualización, es necesario contar con un nombre de **Usuario** y una **Contraseña**. Éstos serán los que se te habrán facilitado desde Panda Software, tras regístrarte como usuario de Panda Antivirus Platinum y habrás introducido en la sección anterior.

  Si te conectas a Internet a través de módem, NO marques la casilla **Acceso a través de Proxy**. Si te conectas a Internet a través de una red de ordenadores mediante un proxy, SÍ debes marcarla.

  Si utilizas un proxy para acceder a Internet, pulsa el botón **Configurar** para indicar los datos de acceso al proxy. Aunque el antivirus los detectará por defecto, podrás indicar la **Dirección IP** (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes en la red) y el número de **Puerto** (punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) que utilizas para acceder a Internet a través del proxy. Es aconsejable que consultes con el administrador de la red a la que estás conectado, antes de modificar dichos datos.

  Además, si es necesario, podrás introducir tu **Nombre de usuario** y **Contraseña** de acceso al proxy de la red. ¡¡ATENCIÓN!!, este **Nombre de usuario** y **Contraseña**, no son los datos correspondientes a tu registro como cliente de Panda Antivirus Platinum, sino los que te permiten el acceso a Internet a través del proxy de tu red de ordenadores (en el caso de que sea necesario). Consulta con el administrador de la red a la que estás conectado, si no conoces dichos datos.

- **Diskette, CD-ROM, o Red Local.** El archivo de identificadores de virus (fichero de firmas), se habrá colocado anteriormente en un disquete (puede tratarse de un disquete de actualización, o no), CD-ROM (puede tratarse de un CD de actualización, o no), o en un determinado directorio de una Unidad de red local. A través de la sección **Ruta** (pulsando el botón que aparece a la derecha para examinar, o escribiendo directamente el camino) se le indicará al antivirus el camino o path completo, para que lo recoja y actualice desde allí.

Si deseas obtener más información sobre las actualizaciones y la configuración del sistema de actualizaciones, consulta el apartado ¿Qué es una Actualización?, de esta ayuda.

Además, las actualizaciones que realiza el antivirus, son incrementales. Esto quiere decir que, en las actualizarse a través de Internet, sólo se descargarán los ficheros necesarios, o solamente secciones de éstos. El nuevo archivo de identificadores de virus (fichero de firmas, o pav.sig) sólo se descarga por completo cuando el actual (no actualizado), tiene más de 28 días. El antivirus es capaz de encontrar las diferencias entre el actual archivo de identificadores de virus y el nuevo. De este modo, el proceso de actualización es mucho más rápido ya que solamente deberá descargar las diferencias entre ambos. Por lo tanto, el sistema de actualizaciones incrementales, cumple dos objetivos fundamentales: reduce el tiempo de descarga, agilizando la actualización y libera al equipo de trabajo innecesario. Todo esto se traduce en una mayor velocidad y ligereza para el sistema.

Nota: puedes ampliar información sobre el sistema de actualizaciones de Panda Antivirus Platinum, consultando el apartado ¿Qué es una Actualización?, en esta misma ayuda.

FAQ 35: ¿Cómo Sé Cuál es la Versión de mi Panda Antivirus Platinum?

Para conocer cuál es la versión de tu Panda Antivirus Platinum, debes hacer lo siguiente:

1. En la ventana del antivirus, pulsa el botón **Ayuda** de la barra de herramientas.
2. Selecciona la opción **Acerca de Panda Antivirus**.
3. Esto mostrará un cuadro de diálogo. En el vértice superior derecho del mismo, aparece un número. Éste es quien nos indica la versión de Panda Antivirus Platinum que tenemos instalada.
4. Para cerrar dicho cuadro de diálogo, pulsa el botón **Aceptar**.

NOTA: Además, la *Barra de título* correspondiente a la ventana de Panda Antivirus Platinum, también muestra un número que se corresponde con la versión del antivirus.

Soporte Técnico en la Web

Sin duda es muy importante contar con alguien que te ayude a solucionar inmediatamente cualquier incidencia con algún virus, o con tu programa antivirus. Panda Antivirus Platinum te permite el acceso directo al área de Soporte Técnico, en la Web de Panda Software (www.pandasoftware.es/soptecni/). Para ello, sólo debes abrir la ventana de tu antivirus, acceder al menú **Servicios** y seleccionar la opción **Soporte técnico en la web**.

Dicho servicio abrirá tu navegador de Internet y te colocará en la página de soporte técnico. En ella encontrarás ayuda específica para los usuarios de Panda Antivirus Platinum. Además, podrás resolver cualquiera de tus problemas, obtener información sobre la desinfección de un determinado virus, acceder a las actualizaciones, pedir que se te reenvíe de nuevo tu nombre de **Usuario** y **Contraseña** (recordatorio de estos datos), etc.

¿Qué es un Firewall?

La traducción literal de la palabra firewall es *muro de fuego*. Cuando se habla de firewall también es común utilizar el término *cortafuegos*. En cualquier caso, el firewall es una barrera o protección que permite a un sistema mantener a salvo la información cuando el ordenador accede a otras redes -como Internet- o transmite información (que podría estar contaminada por virus, o que consiste en ataques de otros ordenadores o usuarios) a través de ellas.

Su máxima utilidad es la protección de los accesos (entradas y salidas) a través de la red donde está conectado el ordenador, o a través de Internet. El firewall consiste en el conjunto de software (programas) y/o hardware (elementos físicos, equipos, etc) que autoriza o deniega los accesos o el tráfico de información entre el ordenador y el mundo exterior.

¿Para qué sirve el firewall?

Mediante el firewall puedes indicar cuáles son los programas y servicios del sistema que no deben tener acceso a Internet o a la red a la que está conectado el ordenador, cuáles sí lo deben tener, cuáles son las direcciones IP (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes en una red) y los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) que se pueden utilizar para conectar con/desde otros ordenadores, indicar si tus carpetas compartidas en la red pueden ser accesibles o no, etc. Panda Antivirus Platinum incorpora un excelente software firewall, con el que podrás hacer todo esto.

Una buena combinación: antivirus + firewall

La combinación perfecta consiste en la instalación de un antivirus y de un firewall. Panda Antivirus Platinum es un magnífico antivirus que además incluye un firewall. Ambos trabajan de forma conjunta, sin interferir ninguno de ellos en el trabajo del otro, consiguiendo unas mejores cuotas de protección y de seguridad.

Sin embargo, debes tener en cuenta que la correcta utilización y configuración del firewall es muy importante. Con las restricciones o reglas de seguridad que establezcas en el firewall estarás aceptando o denegando el tráfico (entrada/salida) entre tu ordenador y el exterior (red local, Internet). Todo aquel tráfico aceptado puede incluir contenido perjudicial (un virus, o consistir en ataques realizados a tu ordenador desde otros ordenadores). En este caso -cuando las reglas establecidas en el firewall han permitido la transferencia o acceso-, el antivirus será el encargado de actuar detectando los posibles virus, gusanos, troyanos, etc.

Nota importante: a la hora de configurar y trabajar con el firewall, ten muy en cuenta que las reglas que apliques pueden afectar al funcionamiento de los programas y los recursos compartidos en la red con otros ordenadores. El impedir el acceso de ciertos programas a la red o no permitir el acceso a las carpetas compartidas, por ejemplo, conllevará que éstos no se podrán utilizar desde otros ordenadores conectados a la red.

En el mercado existen numerosos firewalls comerciales destinados a la protecciom de diferentes tipos de plataformas y sistemas operativos. Cada uno de ellos tiene sus propias características y objetivos. Sin embargo, es más aconsejable contar con un firewall incorporado en el antivirus que tengas instalado. A continuación, puedes consultar cada una de las características del firewall que Panda Antivirus Platinum incluye:

Funciones del Firewall

¿Cómo Instalar y Activar el Firewall de Panda Antivirus Platinum?
¿Cómo Configurar el Firewall de Panda Antivirus Platinum?
Ver la Actividad de la red a través del Firewall

Funciones del Firewall

Entre las principales características, o las principales funciones del firewall incluido en Panda Antivirus Platinum, se pueden destacar las siguientes

Accesos a la red y accesos a Internet

El firewall permite que indiques cuáles son los programas instalados en tu ordenador que pueden utilizar accesos a la red (o a Internet). En tal caso podrás establecer varios niveles de permiso para dichos accesos: **Permitida** (el programa podrá acceder sin restricción), **Denegada** (el programa no podrá acceder), o **Preguntar** (se te pregunta sobre la acción a realizar, cuando el programa intenta acceder a la red).

Protección de direcciones IP

Puedes indicar cuáles son las direcciones, o códigos numéricos que identifican exclusivamente a cada uno de los ordenadores integrantes de una red, con las que los programas pueden comunicarse.

Protección de puertos y protocolos de comunicaciones

Te permite indicar cuáles son los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) y los protocolos (conjuntos de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) que los programas instalados en tu ordenador podrán utilizar para conectarse a la red. Del mismo modo, también te permite indicar cuáles son los puertos de comunicaciones y los protocolos a través de los cuales se podrán utilizar desde la red los programas instalados en tu ordenador.

Protección de carpetas compartidas

En tu ordenador pueden existir carpetas o directorios compartidos (aquellos a los que se puede tener acceso desde otro ordenador de la red). El firewall te permite indicar si éstas deben estar accesibles a los demás usuarios de la red. Del mismo modo puedes permitir / denegar el acceso a las carpetas compartidas en otros ordenadores de la red desde el tuyo.

Protección de intrusos

En ocasiones tienen lugar intrusiones dentro del ordenador. Éstas pueden estar provocadas por otros usuarios que -de forma intencionada, o accidental- intentan acceder a tu ordenador y realizar operaciones en él (no siempre benignas). Concretamente, -cada día más, desgraciadamente- existen programas para tomar el control de los ordenadores atacados (troyanos). Mediante el firewall de Panda Antivirus Platinum, puedes detectar dichas intromisiones y ser informado de su existencia.

Bloqueos

Tu Panda Antivirus Platinum te permite bloquear los programas que has decidido no deben tener acceso a la red o a Internet. También bloquea los accesos que, desde otros ordenadores, se realizan para utilizar programas en tu ordenador.

Definición de Reglas

Todas las restricciones y la definición de la configuración o forma de trabajo del firewall se determina mediante el establecimiento de una serie de reglas (pautas de conducta) en él. Dichas reglas aunan todo lo comentado en los párrafos anteriores y permiten o deniegan los accesos correspondientes.

Nota importante: a la hora de configurar y trabajar con el firewall, ten muy en cuenta que las reglas que apliques pueden afectar al funcionamiento de los programas y los recursos compartidos en la red con otros ordenadores. El impedir el acceso de ciertos programas a la red o no permitir el acceso a las carpetas comparticas, por ejemplo, conllevará que éstos no se pueden utilizar desde otros ordenadores conectados a la red.

¿Cómo Configurar el Firewall de Panda Antivirus Platinum?

La configuración del firewall incluido en Panda Antivirus Platinum es muy sencilla. Sin embargo, ten muy en cuenta que cualquier cambio en las restricciones de acceso de tus programas, o de las carpetas que compartes en la red, las reglas que definas, etc pueden afectar a otros programas y al trabajo de otros usuarios conectados a dicha red.

Nota importante: a la hora de configurar y trabajar con el firewall, ten muy en cuenta que las reglas que apliques pueden afectar al funcionamiento de los programas y los recursos compartidos en la red con otros ordenadores. El impedir el acceso de ciertos programas a la red o no permitir el acceso a las carpetas comparticas, por ejemplo, conllevará que éstos no se pueden utilizar desde otros ordenadores conectados a la red.

El acceso al área de configuración del firewall puede realizarse de varios modos:

- Desde la opción **Protección permanente** que aparece en el **Panel de control**, dentro de la ventana del antivirus. Cuando hayas accedido a dicha área (seleccionado esta opción del panel), debes pulsar sobre la opción **Configurar** que se encuentra en el panel **Firewall**.
- Desde la opción **Inicio**, dentro de la ventana del antivirus. Cuando hayas accedido a dicha área (seleccionado esta opción del panel), debes pulsar pulsa sobre la opción **Configurar protección permanente**.
- Desde el icono de Panda Antivuirus Platinum en la *Barra de tareas de Windows*. Si alguna de las protecciones permanentes (Antivirus -de archivo o de correo-, o Firewall) se encuentra activa, se mostrará el icono de Panda Antivirus Platinum en la *Barra de tareas de Windows* (junto al reloj del sistema). Si pulsas con el puntero del ratón sobre dicho icono, accederás a la configuración de la protección permanente.

Si durante el proceso de instalación de tu Panda Antivirus Platinum activaste el firewall -si lo instalaste, marcando la casilla **Activar la protección permanente (recomendado)**-, o si ya lo has activado anteriormente, accederás directamente a su configuración.

Si aun no has instalado el firewall (la protección permanente de firewall), cuando accedas a su activación o a su configuración aparecerá un asistente. Dicho asistente te guiará siguiendo estos pasos:

1. Aparece una ventana de bienvenida al asistente. Pulsa el botón **Siguiente**, si deseas continuar con la configuración / instalación y activación del firewall.
2. Por defecto, aparece marcada la casilla **Activar la protección firewall (recomendado)**. Pulsa el botón **Siguiente**. Puedes obtener información sobre lo que es un firewall, pinchando sobre la opción **¿Qué es un firewall?**.
3. Selección de los adaptadores de red (tarjetas de red que tienes instaladas en tu ordenador, para que éste se conecte a una red de ordenadores). Existen dos posibilidades:

   Si tu ordenador sólo tiene una única conexión de red o un único acceso telefónico, debes indicar si está conectado a una red. En tal caso, marca la casilla **Este ordenador está conectado a una red local**.

   Si tu ordenador tiene configuradas varias conexiones de red y/o varios accesos telefónicos, se

mostrará un listado con todos ellos. En ella debes marcar las conexiones o accesos que deben ser utilizados para compartir ficheros e impresoras en la red. Se recomienda no marcar aquellos adaptadores que permiten la conexión directa a Internet (MODEM, xDSL, etc) .

Nota: si el sistema operativo de tu ordenador es Windows NT 4.0, no aparecerá esta lista de adaptadores de red. Las reglas avanzadas de seguridad no se aplicarán sobre un único adaptador, sino sobre todos los existentes. Por otra parte, las opciones de configuración de las carpetas compartidas (ficha **Seguridad**, en la configuración del firewall), no estarán activas.

En cualquier caso, pulsa el botón **Siguiente**.

4. Si no deseas ser informado cuando un programa común acceda a la red, marca la casilla **No preguntar cuando los programas comunes accedan a la red (recomendado)**. También puedes consultar la lista de los programas que son considerados como comunes en tu ordenador, pulsando el botón **Ver programas comunes de tu PC**. En cualquier caso, pulsa el botón **Siguiente**.
5. Con estos pasos, acabas de instalar y activar la protección permanente del firewall. Para que éste comience a funcionar, es necesario que reinicies tu ordenador. Sin embargo tienes dos posibilidades:

   Reiniciar Windows ahora. Si marcas esta casilla y pulsas el botón **Finalizar**, tu ordenador se reinicia. Cuando arranque, la protección firewall estará activa y en funcionamiento.

   Reiniciar más adelante. Si marcas esta casilla y pulsas el botón **Finalizar**, tu ordenador no se reinicia y la protección firewall queda inactiva (el firewall no te protege) hasta que reinicies tu ordenador en otro momento.

   Nota: recuerda que la protección del firewall estará inactiva (no entrará en funcionamiento) hasta que reinicies tu ordenador.

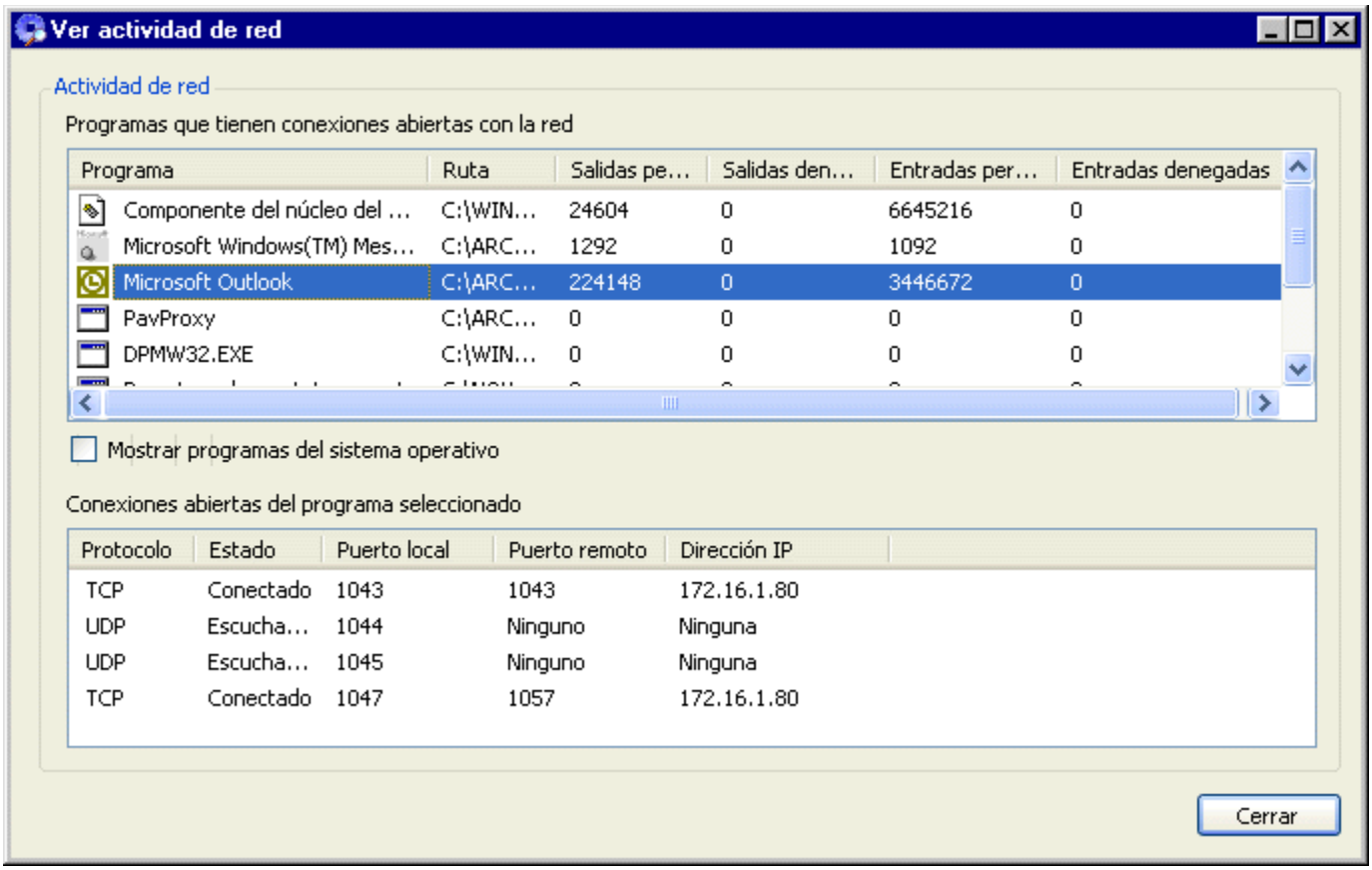
Si ya habías instalado el firewall anteriormente, se mostrará un cuadro de diálogo desde el cual puedes seleccionar la configuración del firewall, pulsando el correspondiente botón **Configurar** (el situado en la sección **Protección permanente firewall**). Esto abre la ventana de configuración del firewall, en la que se muestran varias fichas. Para conocer cada una de las posibilidades de configuración del firewall, consulta el apartado ¿Cómo Configurar un Análisis? (Inmediato / Programado / Permanente), de esta ayuda.

Nota: si durante el proceso de instalación de tu Panda Antivirus Platinum, no indicaste que debía instalarse / activarse el firewall, también podrás hacerlo desde el botón **Inicio** de Windows. En tal caso, pulsa el botón **Inicio**, selecciona el grupo **Programas**, selecciona **Panda Antivirus Platinum** y pulsa sobre la opción **Desinstalar - Reparar**. Esto muestra un cuadro de diálogo en el que debes pulsar el botón **Reparar**. Si aun no has instalado el firewall, podrás hacerlo en este momento.

Ver la Actividad de la Red a través del Firewall

Si deseas conocer la actividad del firewall en cualquier momento y el historial de las acciones que ha realizado, puedes hacerlo. Para ver este informe de actividad del firewall debes seleccionar el área **Protección permanente** que se encuentra en el **Panel de control**, dentro de la ventana de Panda Antivirus Platinum.

Una vez allí, selecciona la opción **Ver actividad de red** que se encuentra dentro del panel rotulado con el título **Firewall**. Esto muestra la siguiente información.



Los dos listados que aparecen, presentan la siguiente información:

Programas que tienen conexiones abiertas con la red. Dentro de la lista se enumeran aquellos programas que actualmente mantienen algún tipo de conexión con la red. Es decir, están accediendo a ella por algún motivo o están siendo utilizado por otros programas o usuarios conectados a la red. Los datos se presentan en varias columnas:

Programa (nombre del programa que está accediendo a la red), *Ruta* (directorio en el que se encuentra el programa), *Salidas permitidas* (número de accesos de salida que ha realizado el programa y que le han sido permitidas por el firewall), *Salidas denegadas* (número de accesos de salida que ha realizado el programa y que le han sido denegadas por el firewall), *Entradas permitidas* (número de accesos de entrada que ha realizado el programa y que le han sido permitidas por el firewall) y *Entradas denegadas* (número de accesos de entrada que ha realizado el programa y que le han sido denegadas por el firewall).

Marcando la casilla **Mostrar programas del sistema operativo**, esta lista incluirá además los programas correspondientes al sistema operativo que además están accediendo a la red por algún motivo.

Conexiones abiertas del programa seleccionado. Cuando selecciones uno de los programas de la lista superior (**Programas que tienen conexiones abiertas con la red**) esta segunda lista indicará que tipos de conexiones mantienen en este momento el programa seleccionado. Los datos se presentan en varias columnas:

Protocolo (tipo de protocolo a través del cual el programa se está comunicando con la red -un protocolo es un conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí-), *Estado* (indica en qué situación se encuentra el programa con respecto a la conexión: conectado, escuchando, etc), *Puerto local* (indica el puerto de comunicaciones de tu ordenador que el programa está utilizando para la conexión), *Puerto remoto* (indica el puerto de comunicaciones de otro ordenador de la red -al que está conectado- que el programa está utilizando para la conexión) y *Dirección IP* (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes en una red).

¿Cómo Instalar o Activar el Firewall de Panda Antivirus Platinum?

La instalación del firewall que incorpora Panda Antivirus Platinum se puede realizar en cualquier momento: durante la instalación de Panda Antivirus Platinum, o en cualquier otra ocasión (cuando, después de haber instalado Panda Antivirus Platinum, accedes a la activación o a la configuración del firewall).

Durante la instalación de Panda Antivirus Platinum

En este caso, la instalación del firewall forma parte de los pasos de instalación del antivirus. Uno de los pasos del proceso de instalación del antivirus, muestra la casilla **Activar la protección firewall (recomendado)**. Si en ese momento la marcas y pulsas el botón **Siguiente**, se instalará el firewall junto con el antivirus. En definitiva, la instalación del firewall durante la instalación del antivirus es muy sencilla y consiste en lo siguiente:

1. Uno de los pasos de instalación del antivirus presenta la casilla **Activar protección firewall (recomendado)**. Márcala y pulsa el botón **Siguiente**. Esto comienza la instalación del firewall. Si no la hubieses seleccionado solamente se instalará el antivirus. Si pulsas sobre la opción **¿Qué es un firewall?**, accederas a información ampliada sobre la definición y/o las funciones de un firewall.

2. Sólo si en el paso anterior marcaste la casilla **Activar protección firewall (recomendado)** y si tu ordenador cuenta con una única conexión de red y/o un único acceso telefónico, debes indicar si tu ordenador está conectado a una red de ordenadores. Si es así, marca la casilla **Este ordenador está contectado a una red local**.

   Sólo en el caso de que tu ordenador tenga configuradas varias conexiones de red y/o varios accesos telefónicos, podrás seleccionar aquellos que se utilizan para compartir ficheros e impresoras en la red. En tal caso, aparece una lista de con todas las conexiones de red y/o los accesos telefónicos de tu ordenador. Selecciona los que estimes oportuno (no es recomendable marcar aquellos que permiten la conexión directa a Internet -MODEM, xDSL, etc-) marcando la casilla correspondiente.

   Nota: si el sistema operativo de tu ordenador es Windows NT 4.0, no aparecerá la lista de adaptadores de red. Las reglas avanzadas de seguridad no se aplicarán sobre un único adaptador, sino sobre todos los existentes. Por otra parte, las opciones de configuración de las carpetas compartidas (ficha **Seguridad**, en la configuración del firewall), no estarán activas.

   En cualquier caso, pulsa el botón **Siguiente**.

3. Indica si deseas ser informado cuando los programas instalados en tu ordenador intenten acceder a la red. Para evitar ser informado de ello, marca la casilla **No preguntar cuando los programas comunes accedan a la red (recomendado)**. Puedes consultar la lista de los programas que se consideran comunes y están instalados en tu ordenador, pulsando el botón **Ver programas comunes de tu PC**. Pulsa el botón **Siguiente**, para concluir la instalación del firewall y continuar con la instalación del antivirus.

   Nota: ten en cuenta que la protección firewall estará instalada, pero no se activará hasta que no hayas reiniciado tu ordenador.

Si no instalaste el firewall durante la instalación de Panda Antivirus Platinum

En este caso, se procederá a instalar el firewall -si tú así lo deseas- en el mismo momento en el que accedas al área de configuración de la protección permanente de firewall. Entonces, aparece un asistente que te guiará paso a paso, del siguiente modo:

1. Aparece una ventana de bienvenida al aisistente. Pulsa el botón **Siguiente**, si deseas continuar con la configuración / instalación y activación del firewall.
2. Por defecto, aparece marcada la casilla **Activar la protección firewall (recomendado)**. Pulsa el botón **Siguiente**. Puedes obtener información sobre lo que es un firewall, pinchando sobre la opción **¿Qué es un firewall?**.
3. Selección de los adaptadores de red (tarjetas de red que tienes instaladas en tu ordenador, para que éste se conecte a una red de ordenadores). Existen dos posibilidades:

   Si tu ordenador sólo tiene un único acceso telefónico o una única conexión de red, debes indicar si está conectado a una red. En tal caso, marca la casilla **Este ordenador está conectado a una red local**.

   Si tu ordenador tiene varios accesos telefónicos y/o varias conexiones de red, se mostrará un listado con todos ellos. En él debes marcar aquellos que deben ser utilizados para compartir ficheros e impresoras en la red. Se recomienda no marcar aquellos adaptadores que permiten la conexión directa a Internet (MODEM, xDSL, etc) .

Nota: si el sistema operativo de tu ordenador es Windows NT 4.0, no aparecerá la lista de adaptadores de red. Las reglas avanzadas de seguridad no se aplicarán sobre un único adaptador, sino sobre todos los existentes. Por otra parte, las opciones de configuración de las carpetas compartidas (ficha **Seguridad**, en la configuración del firewall), no estarán activas.

En cualquier caso, pulsa el botón **Siguiente**.

4. Si no deseas ser informado cuando un programa común acceda a la red, marca la casilla **No preguntar cuando los programas comunes accedan a la red (recomendado)**. También puedes consultar la lista de los programas que son considerados como comunes en tu ordenador, pulsando el botón **Ver programas comunes de tu PC**. En cualquier caso, pulsa el botón **Siguiente**.
5. Con estos pasos, acabas de instalar y activar la protección permanente del firewall. Para que éste comience a funcionar, es necesario que reinicies tu ordenador. Sin embargo tienes dos posibilidades:

   Reiniciar Windows ahora. Si marcas esta casilla y pulsas el botón **Finalizar**, tu ordenador se reinicia. Cuando arranque, la protección firewall estará activa y en funcionamiento.

   Reiniciar más adelante. Si marcas esta casilla y pulsas el botón **Finalizar**, tu ordenador no se reinicia y la protección firewall queda inactiva (el firewall no te protege) hasta que reinicies tu ordenador en otro momento.

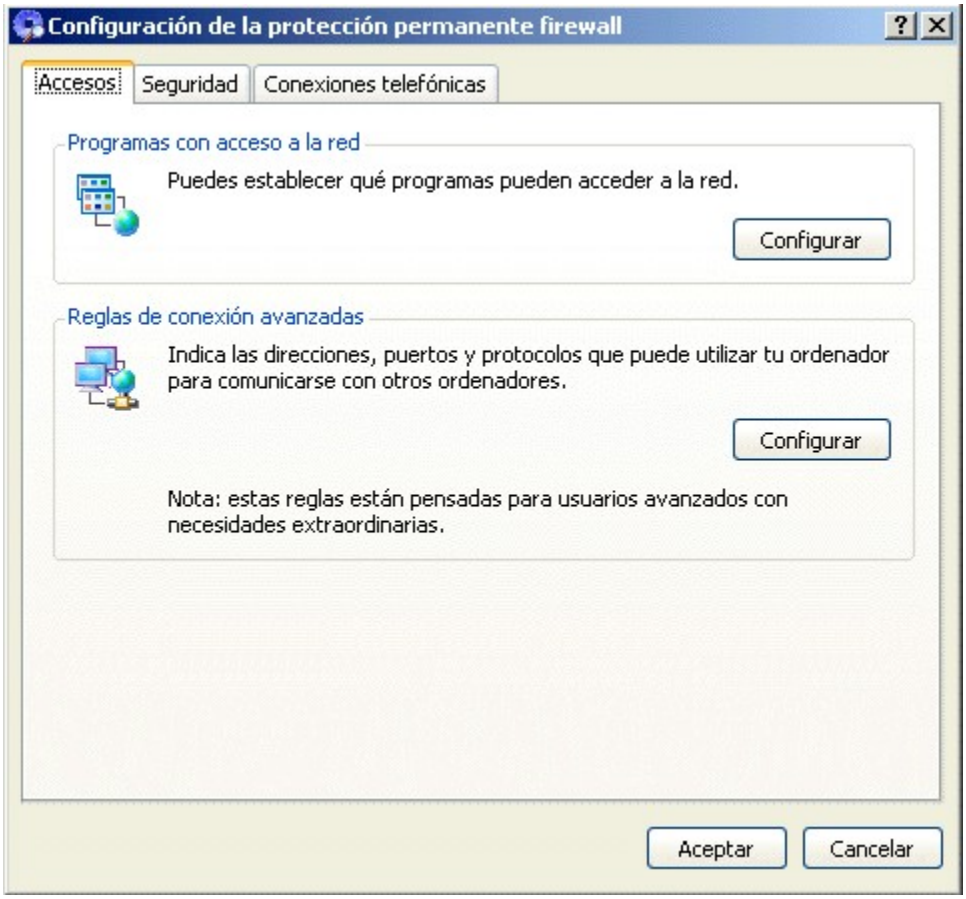
   Nota: recuerda que la protección del firewall estará inactiva (no entrará en funcionamiento) hasta que no hayas reiniciado tu ordernador.

Nota: si durante el proceso de instalación de tu Panda Antivirus Platinum, no indicaste que debía instalarse / activarse el firewall, también podrás hacerlo desde el botón **Inicio** de Windows. En tal caso, pulsa el botón **Inicio**, selecciona el grupo **Programas**, selecciona **Panda Antivirus Platinum** y pulsa sobre la opción **Desinstalar - Reparar**. Esto muestra un cuadro de diálogo en el que debes pulsar el botón **Reparar**. Si aun no has instalado el firewall, podrás hacerlo en este momento.

Configuración del Firewall - Ficha Accesos

Dentro de esta pestaña hay diversas opciones que se agrupan para mayor comodidad, en lo que respecta a la configuración, determinación de las características, reglas y modo de funcionamiento del firewall.

NOTA: esta ficha de configuración, NO estará disponible si no has instalado el firewall incluido con Panda Antivirus Platinum.



Sección **Programas con acceso a la red**
A través de esta sección puedes determinar cuáles son los programas que tienes instalados en tu ordenador y que pueden acceder a Internet o a la red de área local -LAN- a la que estás conectado (tienen el permiso del firewall para hacerlo).

Pulsa el botón **Configurar** y se mostrará una lista de los programas (los que tengan permisos de acceso a la red). Dicha lista cuenta con las siguientes columnas: *Programa* (es el nombre del programa que puede comunicarse con el exterior por medio de la red) y *Comunicación* (indica si la comunicación está permitida, denegada, o si el firewall debe preguntarte).

- **Mostrar programas del sistema operativo**, si marcas esta casilla, la lista incluirá también los programas que pertenecen al sistema operativo que además están accediendo a la red por algún motivo.

- Botón **Añadir programa**. Te permite incluir programas que pueden acceder a la red, dentro de la lista. Si lo pulsas, deberás indicar la **Ruta** (nombre del programa y directorio en el que se encuentra -pulsa el botón que aparece a la derecha, para que te sea más sencillo seleccionar el programa-). Además, debes indicar cuál es el tipo de permiso o la **Acción** que el firewall debe aplicar sobre la comunicación de dicho programa en la red: *Permitir comunicación*, *Denegar comunicación*, o *Preguntar* (serás consultado cuando este programa intente acceder a la red). Sólo si seleccionas la opción **Permitir comunicación**, podrás configurar las opciones avanzadas.

  Además, puedes pulsar el botón **Opciones avanzadas** (este botón sólo estará activo en el caso de que la regla correspondiente al programa seleccionado en la lista, tenga asociada la acción **Permitir comunicación**). Dicho botón te permite indicar las **Direcciones** y los **Puertos** de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) que el programa puede utilizar. Esto significa que puedes seleccionar las direcciones de otros ordenadores (direcciones IP) a las que el programa se puede conectar. Además, también puedes seleccionar el punto por el que el programa puede conectarse y transferir información con la red e Internet (puerto). Si deseas ampliar información al respecto, consulta el apartado Configuración del Firewall - Opciones Avanzadas para Programas (Direcciones y Puertos), de esta ayuda.

- Botón **Opciones avanzadas**. Este botón sólo estará activo en el caso de que la regla correspondiente al programa seleccionado en la lista, tenga asociada la acción **Permitir**. Selecciona uno de los programas de la lista y pulsa este botón para indicar las Direcciones (números de acceso a otros ordenadores - direcciones IP) y los Puertos (canal de comunicación y conexión -entrada/salida- con otros ordenadores a través de la red) de comunicaciones que el programa puede utilizar. Si deseas ampliar información al respecto, consulta el apartado Configuración del Firewall - Opciones Avanzadas para Programas (Direcciones y Puertos), de esta ayuda.

- Botón **Quitar programa**. Selecciona uno o varios de los programas de la lista y pulsa este botón para eliminarlos de ella y así impedir que tenga acceso a la red y que cuente con unas opciones de configuración de acceso a través del firewall.

- **Reflejar en el informe cada vez que se aplique una regla**. Si marcas esta casilla, todas las incidencias que hagan referencia a una regla establecida en el firewall con respecto a los programas que pueden acceder a la red, se guardarán dentro del Informe de actividad en la red.

Sección **Reglas de conexión avanzadas**

Te permite determinar y poner en marcha las reglas de funcionamiento que deben aplicarse en el firewall.

Pulsa el botón **Configurar** y se mostrará una lista de reglas (las que haya establecidas en ese momento). Dicha lista cuenta con las siguientes columnas: *Nombre de la regla* (es el nombre que has asignado a las reglas que has definido) y *Acción a realizar* (es la tarea que cumple dicha regla).

- Botón **Añadir nueva regla**. Te permite crear y definir las características de una nueva regla que se aplicará al firewall. Si lo pulsas, se muestra una ventana con las siguientes fichas: **General**, **Protocolos y puertos** y **Direcciones**. Si deseas ampliar información al respecto, consulta el apartado Configuración del Firewall - Definición de Reglas en el Firewall (General, Protocolos y puertos, Direcciones), de esta ayuda.

- Botón **Editar regla**. Te permite acceder a las propiedades de la regla que tienes seleccionada en el listado y definir o modificar cada una de sus características. Si deseas ampliar información al respecto, consulta el apartado Configuración del Firewall - Definición de Reglas en el Firewall (General, Protocolos y puertos, Direcciones), de esta ayuda.

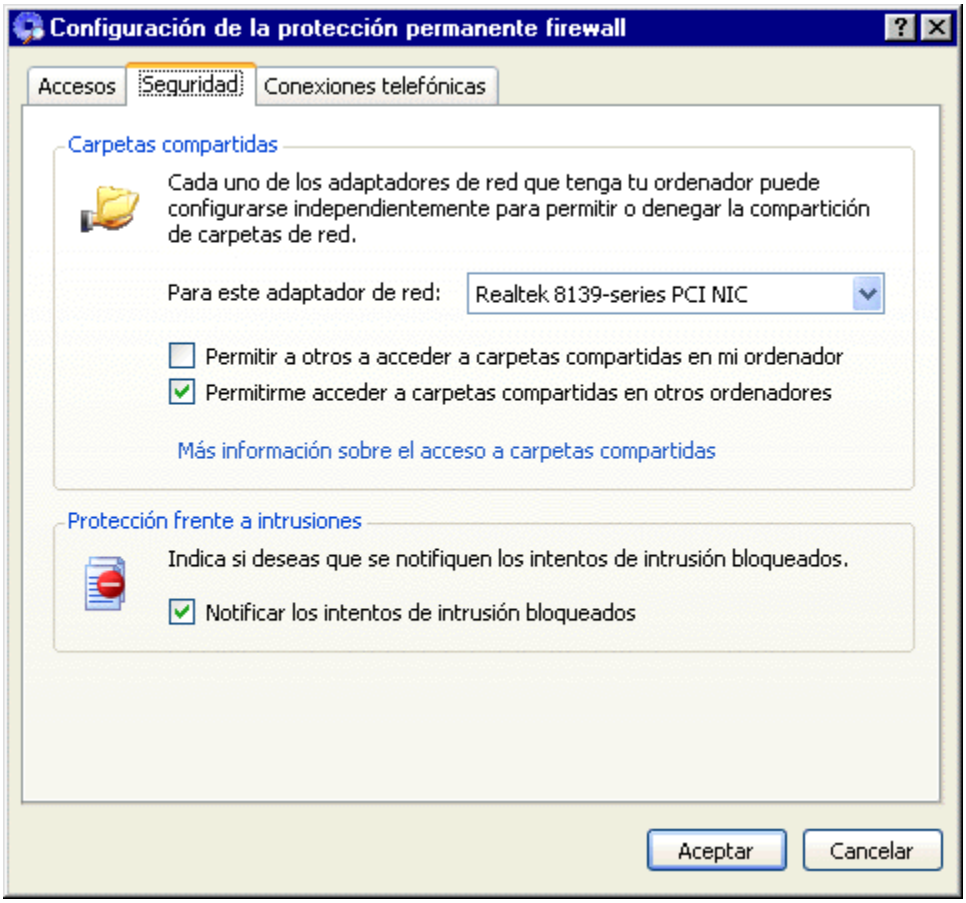
- Botón **Borrar regla**. Selecciona una o varias de las reglas de la lista y pulsa este botón para eliminarlas de ella e impedir que se apliquen.

- **Reflejar en el informe cada vez que se aplique una regla**. Si marcas esta casilla, todas las incidencias que hagan referencia a una regla establecida en el firewall con respecto a los programas que pueden acceder a la red, se guardarán dentro del Informe de actividad en la red.

Configuración del Firewall - Ficha Seguridad

Dentro de esta pestaña hay diversas opciones que se agrupan para mayor comodidad, en lo que respecta a la configuración, determinación de las características, reglas y modo de funcionamiento del firewall.

NOTA: esta ficha de configuración, NO estará disponible si no has instalado el firewall incluido con Panda Antivirus Platinum.



Nota: la configuración de seguridad para las **Carpetas compartidas** en la red, no estará disponible en ordenadores con Windows NT 4.0.

Sección **Carpetas compartidas**

En función de los posibles adaptadores de red (tarjetas de red que tienes instaladas en tu ordenador, para que éste se conecte a una red de ordenadores) que tengas instalados en tu ordenador (si estás conectado a una red, puedes tener instalado uno o varios distintos) y concretamente del que hayas seleccionado en la lista desplegable **Para este adaptador de red**, podrás determinar si, para el adaptador seleccionado, existen permisos para acceder a las carpetas o directorios compartidos en la red y si otros usuarios pueden acceder a las carpetas de tu ordenador que tú compartes en la red.

Nota importante: a la hora de configurar y trabajar con el firewall, ten muy en cuenta que las reglas

que apliques pueden afectar al funcionamiento de los programas y los recursos compartidos en la red con otros ordenadores. El impedir el acceso de ciertos programas a la red o no permitir el acceso a las carpetas comparticas, por ejemplo, conllevará que éstos no se pueden utilizar desde otros ordenadores conectados a la red.

La seguridad de las carpetas compartidas en la red, se define del siguiente modo:

- **Para este adaptador de red**. Despliega esta lista para que se muestre cada uno de los adaptadores de red (tarjetas de red que tienes instaladas en tu ordenador, para que éste se conecte a una red de ordenadores) que están instalados en tu ordenador. Para cada uno de ellos podrás definir las propiedades de seguridad de las carpetas compartidas. Despliega la lista y selecciona uno de ellos. Un adaptador de red puede consistir en una tarjeta de red a través de la cual tu ordenador se conecta a una red de ordenadores, o simplemente un MODEM, etc.
- **Permitir a otros acceder a carpetas compartidas en mi ordenador**. Si marcas esta casilla, otros usuarios conectados a la red podrán utilizar las carpetas que tú tienes compartidas en ella.
- **Permitir acceder a carpetas compartidas en otros ordenadores**. Si marcas esta casilla, podrás acceder a las carpetas que otros usuarios tienen compartidas en la red, dentro de otros ordenadores que no son el tuyo.

Sección **Protección frente a intrusiones**

En ocasiones es posible que otros usuarios, servicios o programas, intenten acceder a tu ordenador (de forma intencionada, o no y con un objetivo malicioso o benigno). Un ejemplo pueden ser programas que necesitan accesos a ficheros guardados en tu PC, programas de control, o troyanos. El firewall incorporado con Panda Antivirus Platinum te permite bloquear e impedir estos accesos. Si marcas la casilla **Notificar los intentos de intrusión bloqueados**, Panda Antivirus Platinum te notificará cuando esto suceda.

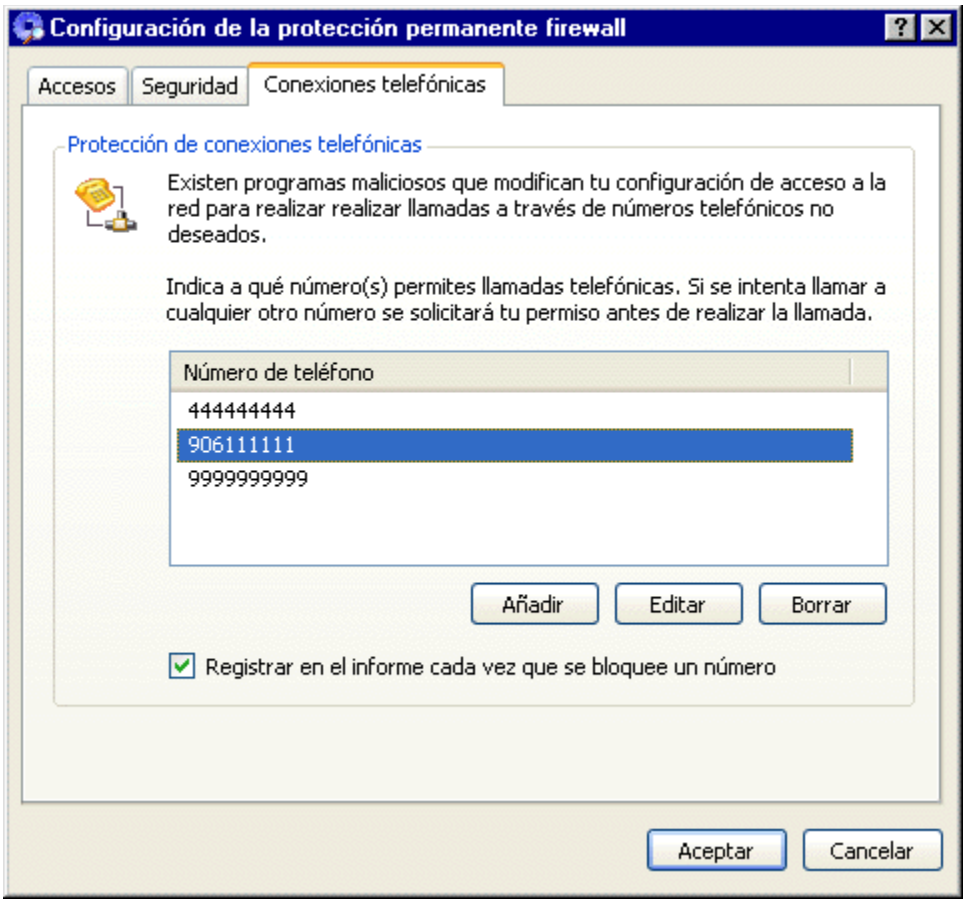
Configuración del Firewall - Ficha Conexiones Telefónicas

Mediante esta pestaña debes indicar la lista de los números de teléfono que tu ordenador debe marcar para realizar cada una de las conexiones a Internet que tú tienes establecidas y permites. El objetivo es evitar que que tu ordenador (mediante determinados programas que existen en Internet -*dialers*-) cuelgue la conexión telefónica que mantienes a Internet y realice sus propias conexiones mediante llamadas a otros números de teléfono (que no son los correspondientes a tus conexiones). Esto es lo que se conoce como un sistema *anti-dialer*, incorporado en el firewall de Panda Antivirus Platinum.

NOTA: esta ficha de configuración, NO estará disponible si no has instalado el firewall incluido con Panda Antivirus Platinum. Además, esta pestaña de configuración solamente aparece si cuentas con un módem y una conexión a Internet a través de él.

El objetivo de esta pestaña de configuración es controlar los accesos de determinados programas malignos que pueden encontrarse en la navegación a través de Internet. Éstos tratan de colgar la conexión telefónica en curso (la que utilizas para tu correcta conexión a Internet) y establecer otra a un número de teléfono del tipo 906, o similares. Esto es lo que se denomina *dialer*. No se trata de un virus, pero podría causarte problemas aumentando considerablemente tu factura de teléfono.

Panda Antivirus Platinum, a través de su firewall, incorpora un sistema *anti-dialer* para estos casos. Dicho sistema se puede configurar mediante esta ficha -**Conexiones telefónicas**-, indicando cuáles son los números de teléfono a los que el ordenador puede realizar llamadas para conseguir la conexión a Internet. Si el ordenador intenta realizar una llamada a un número de teléfono que no existe en esta lista, el firewall te pedirá confirmación antes de realizar dicha llamada.



La seguridad anti-dialer, se consigue manteniendo una lista con los números de teléfono permitidos para realizar tus conexiones a Internet, del siguiente modo:

- Botón **Añadir**. Te permite incluir un nuevo número de teléfono en la lista de números de teléfono permitidos. Cuando lo pulses, escribe el **Número de teléfono** permitido (no utilices guiones, espacios, etc) y pulsa el botón **Aceptar**.
- Botón **Editar**. Te permite modificar el nuevo número de teléfono incluido en la lista de números de teléfono permitidos, que hayas seleccionado en ella.
- Botón **Borrar**. Te permite eliminar números de teléfono que hayas marcado en la lista de números de teléfono permitidos.
- **Registrar en el informe cada vez que se bloquee un número.** Si marcas esta casilla, cada ver que el firewall detecte e impida una llamada de teléfono (para una conexión a Internet) a un número que no está en la lista, dicho suceso se registrará en el Informe de actividad en la red.

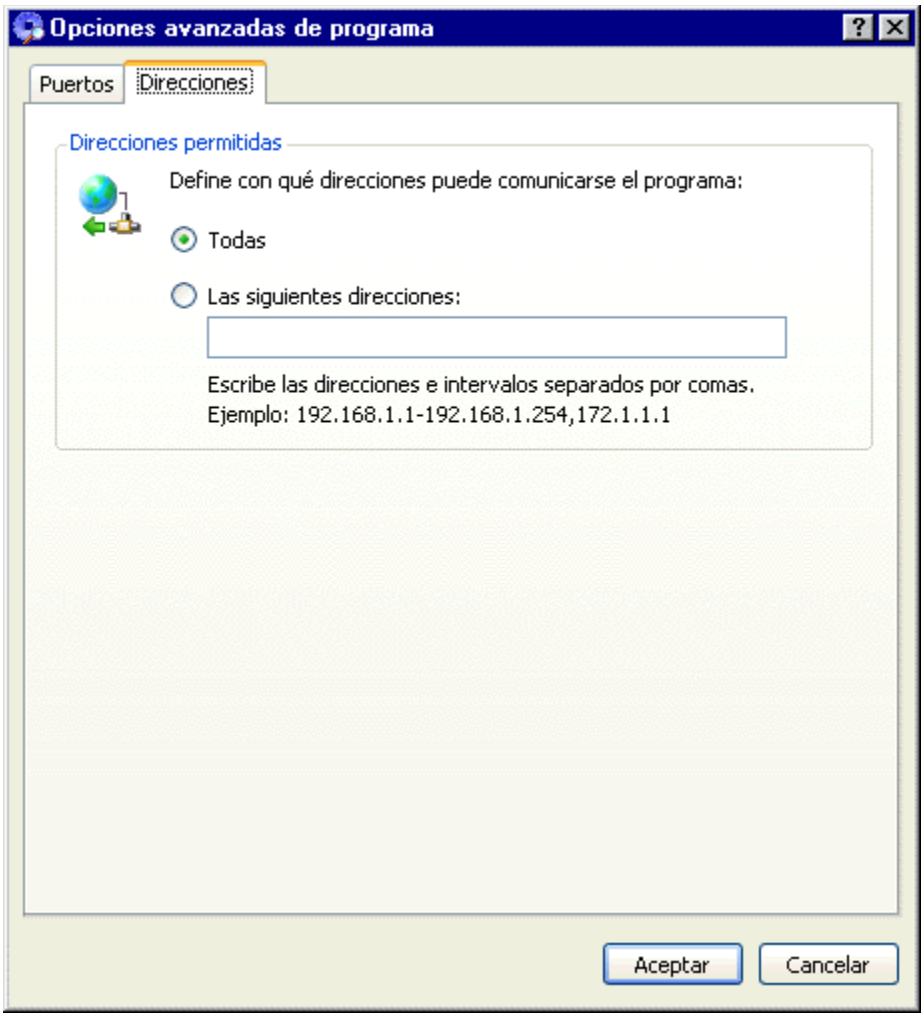
Configuración del Firewall - Opciones Avanzadas para Programas (Direcciones y Puertos)

Las **Opciones avanzadas** para la definición de accesos a la red por parte de los programas que tienes instalados en tu ordenador, consisten en la determinación de las **Direcciones** IP (dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes) y los **Puertos** de comunicaciones (punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) que pueden utilizar dichos programas.

Solamente se podrá acceder a estas opciones avanzadas en el caso de que la regla correspondiente a uno de los programas seleccionados tenga asociada la acción **Permitir**. Al acceder a estas opciones avanzadas de configuración se muestran dos fichas.

Ficha **Direcciones**

Dentro de esta ficha debes indicar cuáles son las direcciones IP (direcciones de otros ordenadores: estaciones y servidores de la red. Direcciones o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes en una red) que los programas podrán utilizar. Tienes las siguientes posibilidades:



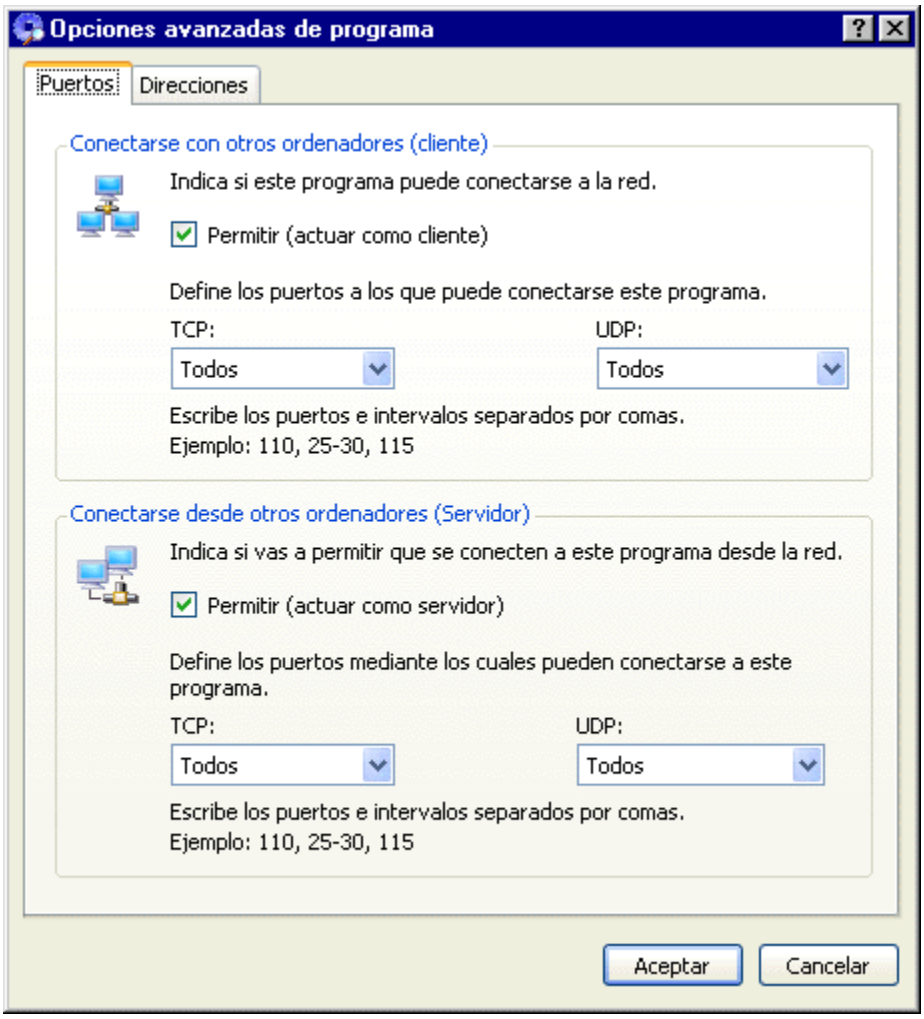
- **Todas.** Si marcas esta casilla, los programas a los que has dado permiso para que accedan a la red, podrán comunicarse con cualquier otro ordenador (con todas las direcciones IP que encuentren y que identifiquen a otros ordenadores).
- **Las siguientes direcciones.** Escribe las direcciones IP correspondientes a los ordenadores (estaciones y servidores de la red) con los que podrán comunicarse los programas (aquellos a los que podrán acceder). Puedes escribir direcciones independientes o intervalos de direcciones.

  Cuando escribas varias direcciones IP independientes, sepára cada una de ellas de las restantes con una coma (,). Si quieres definir un rango de direcciones, sepáralas con un guión (-).

  Por ejemplo: *192.168.1.1,192.168.1.45,172.1.1-172.1.1.250*

Ficha **Puertos**

Los puertos de comunicaciones son los puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa. Dentro de esta ficha debes indicar si el programa puede conectarse a la red y si desde la red se podrá utilizar dicho programa (si otros usuarios o programas se van a conectar a él desde la red). En ambos casos, debes definir las carácterísticas de funcionamiento. Tienes las siguientes posibilidades:



Conectarse con otros ordenadores (cliente). Te permite indicar si el programa podrá conectarse a la red.

- **Permitir (actuar como cliente).** Si marcas esta casilla se habilitan todos los campos de esta sección. Entonces puedes indicar los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) a los que podrá conectarse el programa:

  Puertos **TCP**: podrás seleccionar los siguientes puertos de comunicaciones tipo TCP (Transmission Control Protocol - protocolo que organiza los grupos de datos en los que se disgrega y organiza la información al realizar transferencias entre ordenadores, evitando posibles errores) a los que el programa puede conectarse: *Todos, ftp data, ftp, telnet, smtp, tftp, gopher, finger, (WWW) http, kerberos, rtelnet, pop2, pop3, sftp, nntp, irc* y *https*.

  Puertos **UDP**: podrás seleccionar los puertos de comunicaciones tipo UDP (User Datagram Protocol - tipo de protocolo de comunicaciones que permite la transferencia de información entre ordenadores, sin control del flujo de información), a los que el programa puede conectarse.

Conectarse desde otros ordenadores (Servidor). Te permite indicar si este programa podrá ser

utilizado desde otros ordenadores, conectados a la red.

- **Permitir (actuar como servidor).** Si marcas esta casilla se habilitan todos los campos de esta sección. Entonces puedes indicar los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) a través de los cuales se podrán realizar conexiones al programa desde otros puntos de la red:

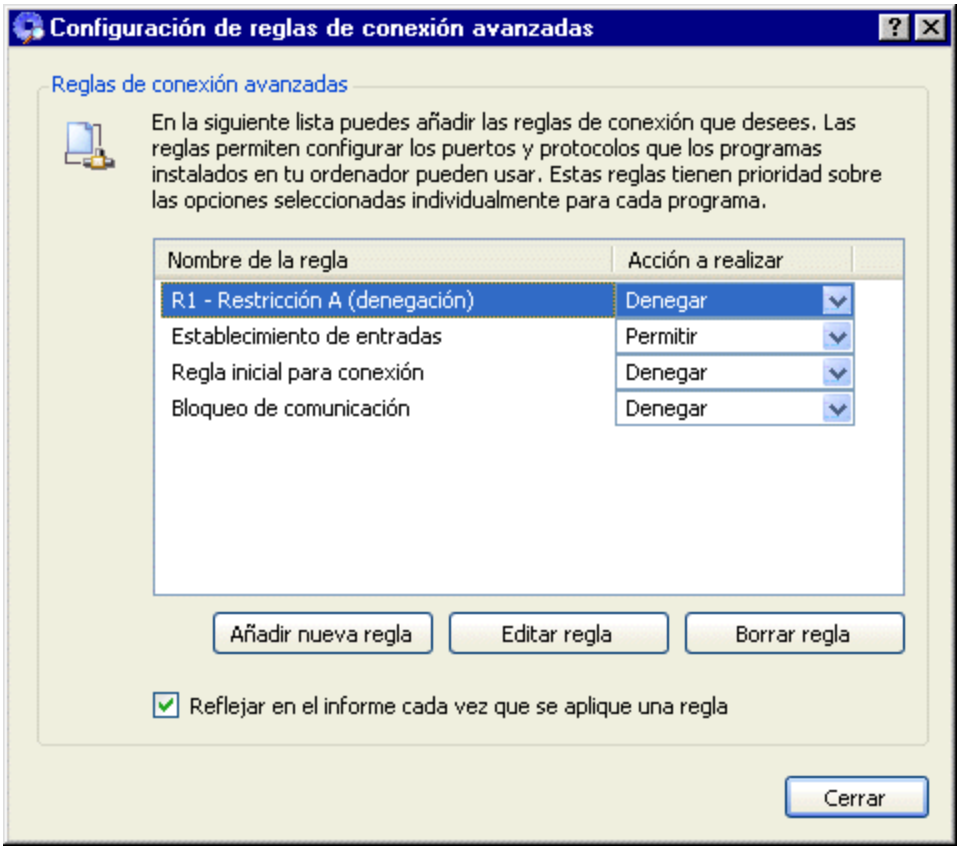
  Puertos **TCP**: podrás seleccionar los siguientes puertos de comunicaciones tipo TCP (Transmission Control Protocol - protocolo que organiza los grupos de datos en los que se disgrega y organiza la información al realizar transferencias entre ordenadores, evitando posibles errores), mediante los que otros ordenadores pueden conectarse con el programa: *Todos, ftp data, ftp, telnet, smtp, tftp, gopher, finger, (WWW) http, kerberos, rtelnet, pop2, pop3, sftp, nntp, irc* y *https*.

  Puertos **UDP**: podrás seleccionar los siguientes puertos de comunicaciones tipo UDP (User Datagram Protocol - tipo de protocolo de comunicaciones que permite la transferencia de información entre ordenadores, sin control del flujo de información), mediante los que otros ordenadores pueden conectarse con el programa.

Nota: en ambos casos (cuando el programa actúa como cliente y cuando el programa actúa como servidor), es posible introducir rangos de puertos que deberán estar separados por guiones (-) y una serie de varios puertos separados por comas (,). Además, es posible indicar los numeros correspondientes a cada uno de los puertos, sin necesidad de escribir el nombre del protocolo (conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí).

Configuración del Firewall - Definición de Reglas en el Firewall (General, Protocolos y puertos, Direcciones)

La definición de reglas en el firewall, consiste en la determinación de una serie de condiciones que éste debe cumplir. A la hora de definir, crear una nueva regla, o editar una ya existente, te encontrarás con una pantalla que cuenta con las siguientes fichas:



Ficha **General**
Dentro de esta ficha debes indicar el nombre de la regla, las acciones quie debe realizar y seleccionar el adaptador de red (tarjeta de red a través de la cual tu ordenador se conecta a una red de ordenadores) que debe utilizarse para aplicar dicha regla.

- **Nombre de la regla.** Escribe o modifica (si lo deseas) el nombre de la regla que estás creando o editando.
- **Acción.** Despliega la lista para seleccionar la acción que debe realizar dicha regla: *Denegar comunicación*, o *Permitir comunicación*.
- **Adaptador de red.** En el caso de que tengas varios adaptadores de red (tarjetas de red a través de las cuales tu ordenador se conecta a una red de ordenadores) instalados en tu ordenador, despliega la lista y selecciona aquel sobre el que debe aplicarse la regla que estás creando o editando.

Ficha **Protocolos y puertos**

Dentro de esta ficha debes indicar los protocolos (conjuntos de códigos y formatos -un lenguaje- que

se utiliza para que los ordenadores se entiendan entre sí), los puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) y la dirección de transferencia de la información (entrada/salida del o al ordenador) afectados por la regla que estás creando o editando.

- **Protocolo.** Despliega la lista y selecciona uno de los protocolos (conjuntos de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) disponibles: *Todos, TCP* (Transmission Control Protocol - protocolo que organiza los grupos de datos en los que se disgrega y organiza la información al realizar transferencias entre ordenadores, evitando posibles errores)*, UDP* (User Datagram Protocol - tipo de protocolo de comunicaciones que permite la transferencia de información entre ordenadores, sin control del flujo de información)*, Servicios ICMP* (Internet Control Message Protocol - protocolo que controla los mensajes de error durante la transferencia de información entre ordenadores)*,* o *Tipo IP*.
- **Sentido de la comunicación.** Selecciona la dirección en la que se transmite la información afectada por esta regla: *Entrada y salida*, *Entrada*, o *Salida*.

Dependiendo del **Protocolo** (conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) que hayas seleccionado en la primera lista, la ficha **Protocolos y puertos** mostrará contenido adicional o no. En el caso de que hayas seleccionado *Todos* los protocolos, no aparecerán opciones adicionales. Sin embargo, si has seleccionado cualquier otro protocolo (*TCP, UDP, Servicios ICMP,* o *Tipo IP*), se darán las siguientes situaciones:

- Si has seleccionado el protocolo (conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) *TCP* (Transmission Control Protocol - protocolo que organiza los grupos de datos en los que se disgrega y organiza la información al realizar transferencias entre ordenadores, evitando posibles errores) o el protocolo *UDP* (User Datagram Protocol - tipo de protocolo de comunicaciones que permite la transferencia de información entre ordenadores, sin control del flujo de información). Debes indicar los puertos (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) sobre los que se aplicará la regla: **Puertos locales** (los existentes en tu ordenador) y **Puertos remotos** (los existentes en otros ordenadores). En ambos casos, las posibilidades son las mismas: *Todos, ftp data, ftp, telnet, smtp, tftp, gopher, finger, (WWW) http, kerberos, rtelnet, pop2, pop3, sftp, nntp, irc* y *https*.
- Si has seleccionado el protocolo *Servicios ICMP* (Internet Control Message Protocol - protocolo que controla los mensajes de error durante la transferencia de información entre ordenadores). Debes seleccionar cada uno de los servicios ICMP sobre los que se aplicará la regla que estás creando o editando. Para ello basta con que marques la casilla correspondiente a cada uno de ellos.
- También puedes seleccionar el protocolo tipo IP.

  En los dos últimos casos (*Servicios ICMP* y *Tipo IP*), puedes **Activar todos** o **Desactivar todos** pulsando los botones que aparecen justo debajo de la lista (servicios en el caso de ICMP y direcciones en el caso del Tipo IP)

Ficha **Direcciones**

Dentro de esta ficha debes indicar las direcciones IP remotas (las de otros ordenadores, direcciones o códigos numéricos que identifican exclusivamente a cada uno de los ordenadores existentes en una red), afectadas por la regla que estás creando o editando.

- **Cualquier dirección.** Las características de la regla se aplicarán a todas las direcciones IP, representativas de cada uno de los ordenadores, con las que el ordenador trabaje.

- **Dirección de tarjeta de red (MAC).** Indica la tarjeta de red (el adaptador), sobre el que quieres que se aplique la regla definida en el firewall. Escribe la dirección correspondiente a una tarjeta de red, a un adaptador de red (dirección MAC - identificador de una tarjeta de red Ethernet - dirección del tipo *xx - xx - xx - xx - xx - xx*), sobre la cual deseas que se aplique la regla que estás creando o editando.
- **Direcciones IP.** Escribe las direcciones o códigos numéricos que identifican exclusivamente a cada uno de los ordenadores afectados por la regla que estás creando o editando. Puedes escribir direcciones independientes o intervalos de direcciones.

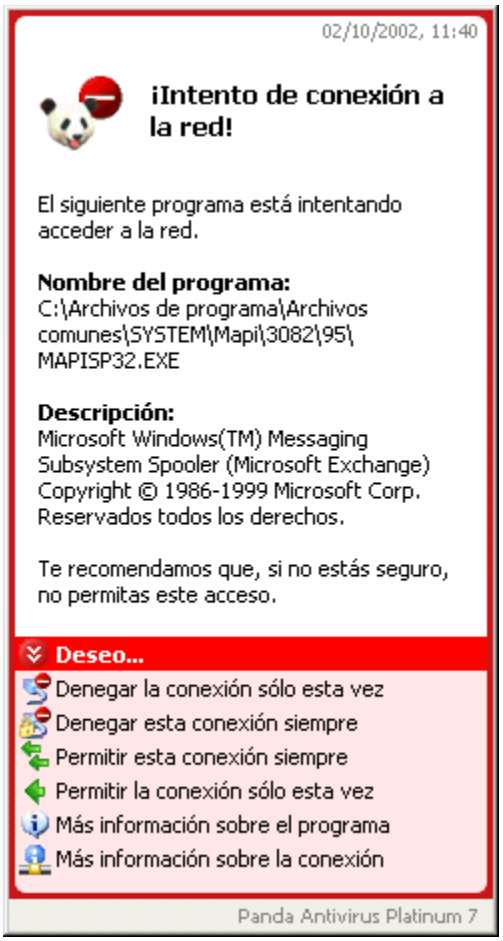
  Cuando escribas varias direcciones IP (direcciones o códigos numéricos que identifican exclusivamente a cada uno de los ordenadores) independientes, sepára cada una de ellas de las restantes con una coma (,). Si quieres definir un rango de direcciones, sepáralas con un guión (-).

  Por ejemplo: *192.168.1.1-192.168.1.254, 172.1.1.1*

Sistema de Avisos

Tu Panda Antivirus Platinum cuenta con un sistema completo de avisos que te mantendrá informado en todo momento sobre cada una de las acciones que se realizan (en el caso de las detecciones, desinfecciones, accesos a través del firewall, etc). Estos avisos aparecen de forma emergente en la zona inferior derecha de la pantalla y desaparecen cuando tú lo indicas.

Ejemplo del aviso emergente, correspondiente al registro online.



Ejemplo del aviso emergente, correspondiente a un intento de conexión a la red por parte de un determinado programa.

Cada uno de ellos cuenta con dos secciones. La sección superior te muestra el aviso mediante un tituliar y un texto explicativo. La sección inferior te propone acciones que puedes realizar pulsando sobre cada una de ellas con el ratón.

Entre los avisos más comunes o importantes, podemos destacar los siguientes:

Avisos correspondientes a las actualizaciones

Antivirus actualizado

Actualización no realizada (Usuario y Contraseña)

Actualización no realizada (Autenticación en el Proxy)

Actualización no realizada (Conexión)

Actualización interrumpida

Avisos correspondientes a los Análisis y Detecciones

Archivos desinfectables en cuarentena

Virus detectado

Virus neutralizado

Archivo peligroso

Avisos correspondientes al Firewall

Las opciones de correo y firewall no están operativas
Intento de intrusión bloqueado
Conexión telefónica no autorizada
Envío peligroso detectado
Script bloqueado

Avisos correspondientes a los servicios

Registra tu antivirus ahora

Avisos - Antivirus Actualizado

Título del aviso: el mensaje o título inicial de este aviso es **¡Antivirus actualizado!.**

Dicho aviso puede ser de dos tipos:

- El que hace referencia a la actualización del antivirus al completo (Upgrade). Este aviso te informa de que tu antivirus se ha actualizado correctamente y muestra el número de la nueva versión del antivirus. Además, se te aconseja reiniciar tu ordenador para que la actualización recién finalizada te permita disfrutar de las mejoras incorporadas en la nueva versión.
- El que hace referencia a la actualización del fichero que permite detectar a los virus -*archivo de identificadores de virus*- (Update). Este aviso te informa de que tu antivirus se ha actualizado correctamente y muestra el número de virus nuevos que se detectan y el número total de los virus que son reconocidos. Además te da siguientes opciones:

  Cerrar, pulsa esta opción para que desaparezca el aviso.

  Cerrar y no mostrar este aviso, pulsa esta opción para que desaparezca el aviso y no se muestre en próximas ocasiones (cuando el antivirus se vuelva a actualizar satisfactoriamente).

  Ayuda, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Actualización NO Realizada (Usuario y Contraseña)

Título del aviso: el mensaje o título inicial de este aviso es **¡Actualización Cancelada!.**

Aviso: este aviso te informa de que no ha sido posible actualizar tu Panda Antivirus Platinum.

Motivo: el nombre de **Usuario** y la **Contraseña** que escribiste en la ficha de configuración de las actualizaciones -tu identificación como usuario registrado de Panda Antivirus Platinum-, no son válidas o no son las correctas. Es decir, no se te ha identificado como un usuario registrado que pueda utilizar el servicio de actualización. La solución consiste en acceder a la configuración de las actualizaciones y volver a introducir el nombre de **Usuario** y la **Contraseña** correcta.

En la sección inferior encontrarás las siguientes opciones:

- **Revisar identificación de usuario**, pulsa esta opción para comprobar que el nombre de **Usuario** y la **Contraseña** que has introducido en la sección de configuración de las actualizaciones, son correctos. Si no lo son, introduce los datos correctos y vuelve a intentar realizar la actualización.
- **Volver a intentarlo ahora**, pulsa esta opción para que tu Panda Antivirus Platinum vuelva a intentar realizar su actualización en ese mismo momento, sin modificar ningún dato de la configuración.
- **Volver a intentarlo más tarde**, pulsa esta opción para que el proceso de actualización se posponga. En este caso, Panda Antivirus Platinum volverá a intentarlo pasado un tiempo.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.
- **Desactivar actualización automática**, pulsa esta opción para impedir que tu Panda Antivirus Platinum se actualice a sí mismo de modo automático (sin que tú indiques que lo haga en un determinado instante).

Avisos - Actualización NO Realizada (Autenticación en el Proxy)

Título del aviso: el mensaje o título inicial de este aviso es **¡Actualización NO Realizada!.**

Aviso: este aviso te informa de que no ha sido posible actualizar tu Panda Antivirus Platinum.

Motivo: el servidor proxy, mediante el cual has indicado que se debe realizar la conexión a Internet para realizar las actualizaciones (en el área de configuración de las actualizaciones), no ha permitido la conexión. Esto será debido a que los datos de configuración del servidor (por ejemplo, el **Nombre de usuario**, la **Contraseña**, la **Dirección IP** -dirección o código numérico que identifica exclusivamente a cada uno de los ordenadores existentes-, o el **Puerto** de comunicaciones -punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información - entradas / salidas-, del ordenador con el exterior y viceversa) no son los correctos (se aconseja la consulta del apartado configuración de las actualizaciones). También puede deberse a que el servidor proxy haya dejado de ser operativo, al menos momentáneamente. La solución consiste en acceder a la configuración de las actualizaciones y revisar las opciones de configuración correspondientes a la opción **Acceso a través de Proxy**.

En la sección inferior encontrarás las siguientes opciones:

- **Revisar la configuración del proxy**, pulsa esta opción para comprobar los datos correspondientes a la configuración de las actualizaciones mediante el **Acceso a través de Proxy**. Si los datos no son correctos, introdúcelos de nuevo correctamente. Si aun así el problema persiste, revisa el estado del proxy o contacta con el administrador de la red a la que estás conectado.
- **Volver a intentarlo ahora**, pulsa esta opción para que tu Panda Antivirus Platinum vuelva a intentar realizar su actualización (en ese mismo momento) mediante una conexión a Internet a través del proxy, sin modificar ningún dato de la configuración.
- **Volver a intentarlo más tarde**, pulsa esta opción para que el proceso de actualización se posponga. En este caso, Panda Antivirus Platinum volverá a intentarlo pasado un tiempo.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Actualización NO Realizada (Conexión)

Título del aviso: el mensaje o título inicial de este aviso es **¡Actualización NO Realizada!.**

Aviso: este aviso te informa de que no ha sido posible conectar a la página Web de actualizaciones de Panda Software.

Motivo: es posible que, en ese momento, no tengas acceso a Internet. Esta cancelación también puede ser consecuencia de que los datos incluidos en la configuración de las actualizaciones no sean los correctos. La solución consiste en comprobar que tienes una conexión a Internet y que ésta funciona. Del mismo modo será conveniente que revises la configuración de las actualizaciones.

En la sección inferior encontrarás las siguientes opciones:

- **Configurar actualizaciones**, pulsa esta opción para comprobar los datos correspondientes a la configuración de las actualizaciones. Si los datos no son correctos, introdúcelos de nuevo correctamente. Si aun así el problema persiste, revisa el estado de tu conexión a Internet.
- **Volver a intentarlo ahora**, pulsa esta opción para que tu Panda Antivirus Platinum vuelva a intentar realizar su actualización (en este mismo momento) mediante una conexión a Internet, sin modificar ningún dato de la configuración.
- **Volver a intentarlo más tarde**, pulsa esta opción para que el proceso de actualización se posponga. En este caso, Panda Antivirus Platinum volverá a intentarlo pasado un tiempo.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Actualización Interrumpida

Título del aviso: el mensaje o título inicial de este aviso es **¡Actualización interrumpida!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum comenzó a realizar correctamente su actualización, pero que ésta no se ha completado (no ha finalizado). El proceso de actualización se ha detenido por algún motivo.

Motivo: el origen de este aviso puede ser la falta de espacio en el disco duro para albergar y permitir realizar la actualización en óptimas condiciones. La solución consiste en comprobar la cantidad de espacio libre en el disco duro. Si no es suficiente, debes dejar más espacio libre en el disco para que la actualización se pueda llevar a cabo.

En la sección inferior encontrarás las siguientes opciones:

- **Liberar espacio**, si el sistema operativo que tienes instalado en tu ordenador lo permite, tu Panda Antivirus Platinum se encargará de preparar el espacio libre que necesite en el disco duro para efectuar su propia actualización.
- **Volver a intentarlo ahora**, pulsa esta opción para que tu Panda Antivirus Platinum vuelva a intentar realizar su actualización, en este mismo momento.
- **Volver a intentarlo más tarde**, pulsa esta opción para que el proceso de actualización se posponga. En este caso, Panda Antivirus Platinum volverá a intentarlo pasado un tiempo.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Archivos Desinfectables en Cuarentena

Título del aviso: el mensaje o título inicial de este aviso es **¡Archivos desinfectables en cuarentena!.**

Aviso: este aviso te informa de que, tras la realización de una actualización del antivirus, ya es posible desinfectar los ficheros que tenías ubicados en la Cuarentena del Hospital.

Motivo: los ficheros que existían en la Cuarentena de tu Panda Antivirus Platinum (aislados allí por ti o por el propio antivirus), no tenían desinfección hasta este momento. Después de realizar una actualización del antivirus ya es posible deinfectarlos. La solución consiste en acceder a la Cuarentena y analizar / desinfectar los ficheros que se encuentran en ella.

En la sección inferior encontrarás las siguientes opciones:

- **Desinfectar y restaurar archivos**, si pulsas sobre esta opción, tu Panda Anttivirus Platinum -recién actualizado- se encargará de analizar todos los ficheros que se encuentran aislados en cuarentena. Si la actualización ya permite desinfectarlos, éstos serán desinfectados y se moverán desde la cuarentena a su ubicación original (se volverán a colocar en el directorio en el que se encontraban antes de que hubiesen sido colocados en cuarentena).
- **Mantener los archivos en cuarentena**, pulsa esta opción para que tu Panda Antivirus Platinum -recién actualizado- no analice los ficheros que se encuentran en cuarentena. En este caso dichos ficheros no serán desinfectados y continuarán estando en cuarentena.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Virus Detectado

Título del aviso: el mensaje o título inicial de este aviso es **¡Virus detectado!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum ha encontrado un virus en tu ordenador. Además, te muestra el **Nombre del virus** que ha encontrado y la **Ubicación del virus** (el lugar en el que lo ha detectado: fichero en el que se encuentra ese virus).

Motivo: mediante la actuación de la Protección Permanente (Antivirus -de correo-), se ha detectado que un fichero está infectado por un virus concreto. La solución es desinfectar ese fichero si es posible. Si no es posible, se recomienda mover dicho fichero a la Cuarentena. En cualquier caso, Panda Antivirus Platinum realizará la operación que tú indiques mediante las opciones disponibles en el propio aviso (sólo si seleccionaste la opción **Preguntar por la acción a realizar**, en la configuración de la protección permanente de correo).

A través de este aviso, siempre que en la configuración de la protección permanente de correo hayas seleccionado la opción **Preguntar por la acción a realizar**, puedes indicar la acción que tu Panda Antivirus Platinum debe llevar a cabo. Es decir, selecciona la acción que se debe realizar ante esta situación:

- **Desinfectar virus**, si pulsas sobre esta opción, el virus será desinfectado.
- **Información sobre el virus**, si pulsas sobre esta opción, podrás consultar información adicional sobre el virus detectado (si ésta estuviese disponible).
- **Mover archivo al área de cuarentena**, si pulsas sobre esta opción el fichero contaminado desaparecerá de su ubicación original (se moverá a otro directorio -el correspondiente a la cuarentena-) y pasará a formar parte de la Cuarentena (quedará aislado).
- **Borrar archivo infectado**, pulsa esta opción para indicar a tu Panda Antivirus Platinum que elimine el fichero contaminado por el virus.

Nota: recuerda que este aviso sólo se mostrará si previamente hubieses seleccionado la opción **Preguntar por la acción a realizar** en la configuración permanente de correo.

Avisos - Virus Neutralizado

Título del aviso: el mensaje o título inicial de este aviso es **¡Virus neutralizado!.**

Aviso: este aviso puede ser generado automáticamente por la protección permanente antivirus (tanto la de correo, como la de archivos), si alguna de ellas está activa. Te informa de que tu Panda Antivirus Platinum ha encontrado un virus en tu ordenador y lo ha neutralizado. Es decir, tu antivirus ha neutralizado el archivo infectado. Además, te muestra el **Nombre del virus** que ha encontrado y la **Ubicación del virus** (el lugar en el que lo ha detectado: fichero y directorio en el que se encuentra ese fichero infectado).

Motivo: mediante la actuación de la Protección Permanente (Antivirus -de correo-), se ha detectado que un fichero está infectado por un virus concreto y éste ha sido neutralizado.

En la sección inferior encontrarás las siguientes opciones:

- **Cerrar**, si pulsas sobre esta opción, el aviso desaparece.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.
- **Información sobre el virus**, si pulsas sobre esta opción, se muestra información correspondiente al virus que tu Panda Antivirus Platinum ha neutralizado (siempre que este virus sea conocido y su información esté disponible en la Enciclopedia de virus, dentro de la Web de Panda Software).

Avisos - Archivo Peligroso

Título del aviso: el mensaje o título inicial de este aviso es **¡Archivo peligroso!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum ha encontrado un fichero que considera peligroso.

Motivo: esto se debe a que tu Panda Antivirus Platinum no sólo detecta virus sino situaciones sospechosas y ficheros potencialmente peligrosos.

Archivo: se muestra el nombre del fichero considerado peligroso.

En la sección inferior encontrarás las siguientes opciones:

- **Mover los archivos al área de cuarentena**, si pulsas sobre esta opción el fichero desaparecerá de su ubicación original (el mensaje en el que va adjunto dicho fichero) y pasará a formar parte de la Cuarentena (quedará aislado).
- **Ignorar ese archivo**, pulsa esta opción para que tu Panda Antivirus Platinum no realice ninguna acción sobre el fichero y que el aviso desaparezca.
- **Borrar archivo peligroso**, pulsa esta opción para indicar a tu Panda Antivirus Platinum que elimine dicho fichero.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Las Protecciones de Correo y Firewall no están Operativas

Título del aviso: el mensaje o título inicial de este aviso es **¡Las protecciones de correo y de firewall no están operativas!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum no tiene activas las protecciones permanentes correspondientes al antivirus de correo electrónico y al firewall. Es decir, no se están analizando las transferencias de información y los accesos a través de correo electrónico, así como en los protocolos (conjuntos de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) y puertos de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa).

Motivo: el origen de este aviso puede ser que el sistema operativo que tienes instalado en tu ordenador, necesita que se actualice algún fichero para poder trabajar con este tipo de protección permanente (antivirus de correo electrónico y firewall). La solución consiste en actualizar algún fichero del sistema operativo que tienes instalado en tu ordenador.

En la sección inferior encontrarás las siguientes opciones:

- **Actualizar el sistema operativo ahora**, si el sistema operativo que tienes instalado en tu ordenador no está tan actualizado como para permitirte la utilización de la protección permanente de correo y del firewall, cuando pulses sobre esta opción podrás actualizar los ficheros necesarios y después podrás activar y utilizar este tipo de protecciones permanentes.
- **Actualizarlo más tarde**, si pulsas sobre esta opción, la actualización del sistema operativo se pospone. Esto quiere decir que, mientras tanto, no podrás activar la protección permanente de correo ni la protección permanente del firewall.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Intento de Intrusión Bloqueado

Título del aviso: el mensaje o título inicial de este aviso es **¡Intento de intrusión bloqueado!.**

Aviso: mediante este aviso se te informa de que alguien ha intentado acceder a tu ordenador desde el exterior y que el firewall lo ha bloqueado, impidiendo dicho acceso o intrusión.

Motivo: desde el exterior (otro ordenador conectado a al red local, o desde Internet), se ha detectado que un programa, o un usuario intentaba *entrar* en tu ordenador. La solución consiste en detectar cuál es el puerto de comunicaciones (puntos de acceso a un ordenador o medios a través de los cuales tienen lugar las transferencias de información -entradas / salidas-, del ordenador con el exterior y viceversa) y el protocolo (conjunto de códigos y formatos -un lenguaje- que se utiliza para que los ordenadores se entiendan entre sí) utilizado para hacerlo, así como la definición de reglas en el firewall que impidan este tipo de accesos.

Tipo de ataque: el firewall de tu Panda Antivirus Platinum te indicará en qué consiste la intrusión que ha conseguido bloquear (por ejemplo, un ataque que haya consistido en la revisión de los puertos de comunicaciones de tu ordenador: *Escaneo de puertos*).

En la sección inferior encontrarás las siguientes opciones:

- **No volver a mostrar este aviso**, si pulsas sobre esta opción y el firewall vuelve a bloquear una intrusión, no serás avisado de esta incidencia. El firewall simplemente se limitará a realizar el bloqueo, sin avisarte de ello.
- **Más información sobre la intrusión**, pulsa esta opción para que el aviso amplíe la información correspondiente al bloqueo de intrusiones que ha llevado a cabo.
- **Cerrar**, pulsa esta opción para que el aviso se cierre.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Conexión Telefónica no Autorizada

Título del aviso: el mensaje o título inicial de este aviso es **¡Conexión telefónica no autorizada!.**

Aviso: este aviso te informa de que tu ordenador está intentando realizar una llamada telefónica (para conectarse a Internet) a un número de teléfono no autorizado (éste no existe en la lista de números de teléfono correspondiente a las reglas definidas para el firewall).

Motivo: esto se debe a que mientras navegabas por Internet algún programa (del tipo *dialer*) está intentando que tu conexión a Internet se realice a través de otro número de teléfono. Sin embargo, ha sido detectado por el sistema *anti-dialer* correspondiente al firewall incluido en tu Panda Antivirus Platinum.

Número de teléfono: se muestra el número de teléfono no autorizado (no definido en las reglas del firewall) al que se ha intentado realizar la llamada.

Nombre del programa: se muestra el nombre del programa que está intentando que se produzca el marcado de un número de teléfono no autorizado.

En la sección inferior encontrarás las siguientes opciones:

- **Cerrar**, si pulsas sobre esta opción la llamada a ese número de teléfono no se efectúa.
- **Autorizar este número**, pulsa esta opción para que la llamada a ese número de teléfono se realice siempre que tenga lugar y que sea considerada como autorizada desde ese momento.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Envío Peligroso Detectado

Título del aviso: el mensaje o título inicial de este aviso es **¡Envío peligroso detectado!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum ha encontrado un fichero incluido en un mensaje de correo electrónico, que considera peligroso.

Motivo: esto se debe a que tu Panda Antivirus Platinum no sólo detecta virus sino situaciones sospechosas y ficheros potencialmente peligrosos incluidos dentro de los mensajes de correo electrónico.

Archivos adjuntos potencialmente peligrosos: se muestran los nombres de los ficheros incluidos en el mensaje que Panda Antivirus Platinum ha considerado peligrosos.

En la sección inferior encontrarás las siguientes opciones:

- **Eliminar los adjuntos del mensaje**, si pulsas sobre esta opción se borran los ficheros incluídos dentro del mensaje (los que se consideran peligrosos).
- **Mover los adjuntos al área de cuarentena**, si pulsas sobre esta opción los ficheros incluidos en el mensaje y considerados peligrosos desaparecerán de su ubicación original (del directorio en el que se encuentra actualmente) y del mensaje, pasando a formar parte de la Cuarentena (quedarán aislados).
- **Ignorar este aviso**, pulsa esta opción para que tu Panda Antivirus Platinum no realice ninguna acción sobre el mensaje ni sobre los ficheros incluidos en él.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Script Bloqueado

Titulo del aviso: el mensaje o título inicial de este aviso es **¡Script bloqueado!.**

Aviso: este aviso te informa de que tu Panda Antivirus Platinum ha encontrado un fichero escrito en un lenguaje de programación de tipo script. Para que la ejecución de éste no tenga lugar -pudiendo producir infecciones u otros problemas-, tu Panda Antivirus Platinum ha bloqueado el fichero.

Motivo: esto se debe a las reglas de seguridad que hayas establecido. Si en su momento indicaste que debían ser bloqueados todos los ficheros de script, tu Panda Antivirus Platinum habrá actuado en consecuencia.

Ubicación del archivo: se muestra el nombre del fichero bloqueado, así como la ruta y nombre del directorio en el que éste se encuentra.

En la sección inferior encontrarás las siguientes opciones:

- **Cerrar**, si pulsas sobre esta opción el aviso se cierra y el fichero continúa bloqueado por Panda Antivirus Platinum.
- **Desactivar bloqueos de script**, si pulsas sobre esta opción estarás indicando que la opción de seguridad que permite bloquear los ficheros de tipo *script*, no debe aplicarse.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.

Avisos - Registra tu Antivirus Ahora

Título del aviso: el mensaje o título inicial de este aviso es **¡Registra tu antivirus ahora!.**

Aviso: este aviso te informa de que debes registrarte como usuario de Panda Software. Este aviso se mostrará, por ejemplo, después de instalar Panda Antivirus Platinum o cuando intentas realizar una actualización del antivirus sin haberte registrado previamente como usuario de Panda Software.

Ejemplo del aviso emergente, correspondiente al registro online.

Motivo: si no te has registrado, no puedes utilizar los servicios incluidos en tu Panda Antivirus Platinum (por ejemplo, las actualizaciones). Sólo si te registras como usuario, recibes un nombre de **Usuario** y una **Contraseña** que te identifican y te permiten utilizar los servicios de Panda Antivirus Platinum. Por este motivo, si no te has registrado o si no has introducido estos datos en la configuración del antivirus, no puedes actualizar tu Panda Antivirus Platinum (o hacer uso de otros servicios con los que éste cuenta).

En la sección inferior encontrarás las siguientes opciones:

- **Registrar el antivirus**, si pulsas sobre esta opción, accederás directamente a la página Web de Registro online de Panda Software. Desde ella podrás introducir tus datos y registrate como usuario de Panda Antivirus Platinum.
- **Ayuda**, pulsa esta opción para acceder a una explicación sobre este aviso (concretamente ésta que estás leyendo) sobre el mensaje de aviso.
- **Configurar actualizaciones**, pulsa esta opción para acceder a la ventana que te permite determinar las características y el funcionamiento -configuración- de las actualizaciones correspondientes a tu Panda Antivirus Platinum.
- **Recordármelo más tarde**, pulsa esta opción para que el aviso se cierre. En este caso, el aviso se mostrará periódicamente hasta que te hayas registrado.

FAQ 36: Más Información Sobre el Acceso a Carpetas Compartidas

Para que sea posible compartir tanto carpetas como impresoras en la red a la que estás conectado, las redes Microsoft Windows utilizan un protocolo o sistema denominado *NetBIOS* (Network Basic Input/Output System). *NetBIOS* puede funcionar de forma independiente o sobre otro tipo de protocolo: por ejemplo, IPX/SPX (propio de las redes Novell NetWare), o TCP/IP (protocolo utilizado en Internet).

La tecnología empleada por el firewall que incluye Panda Antivirus Platinum permite el bloqueo de conexiones tipo *NetBIOS*, en el caso de que éstas funcionen sobre TCP/IP. Esto es debido a que dicho tipo de conexiones son las que entrañan riesgo real. Por lo tanto, con respecto a las conexiones tipo *NetBIOS*, se pueden producir varias situaciones:

- ***NetBIOS* funcionando de forma independiente (*NetBEUI*)**: en este caso, *NetBIOS* se conoce como *NetBEUI* (NetBIOS Enhanced User Interface) y no necesita de otro protocolo de transporte (funciona independientemente). Su objetivo es ser utilizado en redes de ordenadores muy pequeñas, donde todos ellos están conectados a un mismo segmento de la red (por ejemplo, todos conectados a un único concentrador o Hub). La característica especial de esta situación es que sólo puede comunicarse los ordenadores que existen en ese mismo medio. Por otra parte, la información es transmitida por un único ordenador en cada momento, llegando directamente a todos los demás sin necesidad de dar ningún *salto*.

  El firewall integrado con Panda Antivirus Platinum no evita las conexiones realizadas mediante esta forma de funcionamiento (*NetBEUI*). Sin embargo y debido a la naturaleza de este protocolo, no se utiliza para accesos no autorizados desde Internet. Esto quiere decir que su utilización no entraña riesgo.

- ***NetBIOS* funcionando sobre IPX/SPX (*NWLINK-NetBIOS*)**: en este caso, *NetBIOS* utiliza el protocolo *NWLINK-NetBIOS* y funciona en redes Novell NetWare. Esto permite el uso de *NetBIOS* sobre el protocolo IPX/SPX propio de este tipo de redes (Novell). Su utilización puede darse en el caso de redes de área local (LAN) de mediano o gran tamaño.

  El firewall integrado con Panda Antivirus Platinum no evita las conexiones realizadas mediante esta forma de funcionamiento (*NWLINK-NetBIOS*). Sin embargo, dicho protocolo no puede utilizarse para acceder desde Internet a los ordenadores conectados a la red de área local. Esto quiere decir que su utilización no entraña riesgo.

- ***NetBIOS* funcionando sobre TCP/IP**: en este caso, *NetBIOS* utiliza el protocolo *TCP/IP*. Esta es la forma más común de funcionamiento en la actualidad.

  Las primeras ventajas, son las siguientes. Se utiliza el mismo protocolo o tipo de comunicación (entrada / salida) en la red de área local a la que está conectado el ordenador, que en sus comunicaciones con Internet. Además, este sistema es soportado por una gran cantidad de elementos hardware y por gran cantidad de programas o aplicaciones (los más extendidos en la actualidad).

  Como contrapartida a dichas ventajas, también entraña grandes riesgos. Sabemos ya que la red de área local utiliza el mismo protocolo que Internet. En este caso, esto se traduce en que las carpetas compartidas dentro de la red local, también resultarán compartidas con otros usuarios u

ordenadores a través de las conexiones a Internet. Por lo tanto, los usuarios que se conecten a nuestro ordenador a través de Internet, también podrán acceder a las carpetas compartidas en la red de área local a la que estemos conectados.

El firewall integrado con Panda Antivirus Platinum tiene en cuenta dichas circunstancias. Para establecer una seguridad al respecto, el firewall de Panda Antivirus Platinum permite indicar cuáles son los adaptadores (conexiones de red o accesos telefónicos) sobre los que es posible otorgar el permiso de acceso. Así, la conexión tipo *NetBIOS* a dichas carpetas se realizará únicamente a través del adaptador (conexión de red o acceso telefónico) que se utiliza en la red de área local a la que estés conectado.

{ewl RoboEx32.dll, WinHelp2000, }