Muestra el estado del programa, de la protección permanente y los avisos.

Permite seleccionar las partes del ordenador que se analizarán y establecer análisis programados.

Analiza el elemento seleccionado.

Permite configurar las distintas opciones de análisis del antivirus ofreciendo la máxima flexibilidad.

Analiza todos los ficheros comprimidos en el análisis.

Analiza los archivos del sistema en cada análisis que se lleve a cabo.

Analiza todos aquellos archivos de correo electrónico que se encuentren durante el análisis.

Se analizarán todos los ficheros del ordenador.

Se analizarán únicamente los ficheros con las extensiones seleccionadas.

Permite indicar las extensiones de los ficheros que se desean analizar.

Activa los sonidos para el análisis que se está configurando.

Si se marca esta opción en el informe se registrarán todas las incidencias ocurridas durante el análisis.

Seleccionando esta opción se ofrecerá la posibilidad de analizar varios disquetes sucesivamente.

La ventana que muestra el proceso del análisis aparecerá minimizada.

Configura el comportamiento del análisis heurístico.

Establece la configuración original por defecto.

Este botón permite añadir directorios a la lista de directorios que se excluirán del análisis.

Este botón permite eliminar directorios de la lista de directorios que se excluirán del análisis.

Este botón permite añadir ficheros a la lista de ficheros que se excluirán del análisis.

Este botón permite eliminar ficheros de la lista de ficheros que se excluirán del análisis.

En esta casilla se pueden introducir nuevas extensiones que añadir a la lista de extensiones que se excluirán del análisis.

Este botón permite añadir la extensión escrita en la casilla a tal efecto a la lista de extensiones que se excluirán del análisis.

Este botón permite eliminar extensiones de la lista de extensiones que se excluirán del análisis.

Si se marca esta opción, se enviarán alertas al puesto cuando se detecte un virus.

Este botón permite configurar las alertas que se enviarán al puesto.

Permite indicar que se reproduzca un sonido cuando se detecte un virus. Dicho sonido puede ser desde un simple pitido hasta la reproducción de cualquier fichero WAV.

Permite seleccionar un archivo Wav.

Permite indicar que se debe mostrar un mensaje cuando se detecte un virus.

Si se marca esta opción, se enviarán alertas mediante el correo electrónico cuando se detecte un virus.

Permite indicar el mensaje de alerta que se desea enviar por correo electrónico.

Permite indicar que se debe enviar un mensaje de alerta a un puesto concreto de la red. Dicho mensaje es configurable.

Permite indicar el mensaje de alerta que se desea enviar al puesto.

Permite indicar el mensaje de alerta que se desea enviar al dominio.

Permite crear una nueva tarea de análisis mediante un asistente.

Permite editar los elementos a analizar, configurar el análisis o seleccionar la frecuencia con la que se realizará éste.

Elimina la tarea de análisis seleccionada.

Permite actualizar el antivirus mediante un asistente.

Indica que la actualización se encuentra en un disquete, un CD-Rom o una unidad de red local. Asimismo, permite indicar la localización concreta donde se encuentra la actualización.

Indica que la actualización se va a llevar a cabo desde Internet.

Esta opción permite realizar un análisis exhaustivo del ordenador.

Permite la creación de discos de rescate para el arranque del equipo desde un entorno libre de virus.

Permite configurar el comportamiento de los análisis permanentes para los ficheros e Internet.

Permite establecer la periodicidad con la que se realizará el análisis.

Muestra información sobre diversos aspectos relativos al análisis permanente: incidencias, acciones realizadas, nº de mensajes analizados o neutralizados,..etc.

Permite configurar todos los aspectos del análisis permanente: Tipos de ficheros a analizar o excluir del análisis permanente, acciones a realizar y alertas a enviar en caso de que se detecten virus.

Permite activar o desactivar la protección permanente.

Analiza todos los ficheros comprimidos a los que se intente acceder.

Si se marca esta opción en el informe se registrarán todas las incidencias ocurridas durante el análisis.

Se analizarán todos los ficheros del ordenador.

Se analizarán únicamente los ficheros con las extensiones seleccionadas.

Permite indicar las extensiones de los ficheros que se desean analizar.

Se eliminará el fichero infectado cuando la desinfección no sea posible.

Moverá el archivo infectado a la localización que se indique. De esta forma se puede crear un espacio para albergar a los virus "en cuarentena".

Si se marca esta opción se realizará una copia de seguridad del archivo en el que se ha detectado un virus.

Si se marca esta opción se analizarán todos los mensajes de correo electrónico recibidos.

Si se marca esta opción se analizarán todos los mensajes de correo electrónico enviados.

Analiza todos los archivos comprimidos que se encuentren asociados a cualquier mensaje que se analice.

Analiza todos los mensajes que se encuentren incluidos dentro de otros mensajes.

Si se marca esta opción, los datos relativos al análisis en cuestión se registrarán en el informe.

Seleccionando esta opción se analizarán todos los archivos independientemente de su extensión.

Si se selecciona esta opción, sólo se analizarán los archivos con extensión EXE o COM.

Se analizarán únicamente los ficheros con las extensiones seleccionadas.

Permite indicar las extensiones de los ficheros que se desean analizar.

Se analizarán las aplicaciones que lleguen como ficheros adjuntos a los mensajes de correo electrónico.

Se analizarán las imágenes que lleguen como ficheros adjuntos a los mensajes de correo electrónico.

Se analizarán los ficheros de vídeo que lleguen adjuntos a los mensajes de correo electrónico.

Se analizarán los ficheros de audio que lleguen adjuntos a los mensajes de correo electrónico.

Se analizarán los ficheros de texto que lleguen adjuntos a los mensajes de correo electrónico.

Se analizarán los ficheros de tipo HTML que lleguen adjuntos a los mensajes de correo electrónico.

Se analizarán otros tipos de ficheros que no correspondan a ninguno de los anteriores.

Seleccionando esta opción se cambiará el nombre del archivo infectado en caso de no ser posible su desinfección.

Elimina los archivos infectados en caso de no ser posible su desinfección.

Moverá el archivo infectado a la localización que se indique. De esta forma se puede crear un espacio para albergar a los virus "en cuarentena".

Si se marca, activa el bloqueo de direcciones de Internet para impedirnos el acceso a ellas.

Si se marca activa el bloqueo de servicios de Internet para impedirnos su uso.

Si se marca esta opción se analizarán las unidades de red disponibles.

Seleccionando esta opción se bloqueará el acceso a las unidades de red en caso de infección, para impedir la propagación del virus por este medio.

Muestra información sobre los archivos que se encuentran en cuarentena.

Muestra información sobre los archivos infectados de los que se ha realizado una copia de seguridad.

Muestra información sobre los archivos que han sido enviados a **Panda Software**.

Muestra información y permite realizar diversas acciones sobre los ficheros en cuarentena, los ficheros que han sido enviados a **Panda Software** o los cuentan con copia de seguridad.

Analiza únicamente los ficheros que se encuentren en cuarentena.

Permite enviar a Panda Software los ficheros que se encuentren en cuarentena.

Permite mover un fichero en cuarentena a su ubicación original.

Permite eliminar los ficheros en cuarentena seleccionados.

Permite añadir un fichero infectado o sospechoso de estarlo a la lista de archivos ‘‘en cuarentena’’.

Permite restaurar las copias de seguridad de los ficheros que fueron eliminados por el antivirus.

Permite borrar definitivamente las copias de seguridad de los ficheros que el antivirus eliminó en su momento.

Analiza los ficheros que hayan sido enviados a **Panda Software**.

Mueve a su ubicación original los ficheros que hayan sido enviados a **Panda Software** para su análisis.

Elimina los ficheros seleccionados que hayan sido enviados a **Panda Software**.

Permite volver a realizar el envío de los ficheros seleccionados.

Muestra los servicios disponibles para los usuarios registrados de **Panda Software**.

Permite enviar a **Panda Software** los archivos detectados como sospechosos de estar infectados.

En esta sección se resuelven las dudas que otros usuarios nos han planteado con anterioridad.

Muestra un asistente mediante el cual es posible enviarnos las sugerencias que se crean oportunas.

Permite añadir los archivos que se desee enviar a **Panda Software**.

Si se selecciona esta opción se mostrará información sobre la solución **Panda Antivirus Global**.

Si se selecciona esta opción se mostrará información sobre la solución **Panda Invent**.

Si se selecciona esta opción se mostrará información sobre la solución **Panda Security**.

Permite especificar desde dónde se realizarán la actualizaciones: Internet, disquetes, CD-ROM,...etc.

Muestra el informe de incidencias que el antivirus va recogiendo.

Imprime el informe completo.

Permite realizar una búsqueda de palabras en los campos seleccionados.

La búsqueda se realizará en el campo Incidencias.

La búsqueda se realizará en el campo Tareas.

La búsqueda se realizará en el campo Rutas.

La búsqueda se realizará en el campo Acciones.

Convierte el informe a un fichero de texto.

Elimina el fichero del informe.

Filtra la información que se desea ver en el informe.

Muestra la lista de virus con importante información sobre una parte de los virus que el programa detecta.

Imprime la información sobre el virus seleccionado.

Permite la utilización del perfil por defecto configurado en el Panel de Control para reflejar su correo en el antivirus y permitir su análisis.

Se preguntará el perfil de correo que se desea usar en el antivirus cada vez que se entre al mismo.

Permite indicar un perfil de correo concreto para que siempre se use en el antivirus.

Indica que se deben mostrar las unidades de CD-Rom en los distintos análisis como áreas analizables.

Indica que se deben mostrar las unidades de red en los distintos análisis como áreas analizables.

Indica que se deben mostrar las carpetas de correo electrónico en los distintos análisis como áreas analizables.

Indica que se deben mostrar como áreas analizables las bases de datos de Lotus Notes que se encuentren en el ordenador donde esté instalado el antivirus.

Indica que se deben mostrar como áreas analizables las bases de datos de Lotus Notes que se encuentren en el servidor.

Permite indicar el tamaño máximo del informe donde se registra la actividad del antivirus para evitar que ocupe demasiado espacio.

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.

Permite configurar la actualización como automática para que sea el propio antivirus el que se actualice de manera automática regularmente.

Muestra un mensaje que informa al usuario que la actualización se ha llevado a cabo con éxito.

Este botón reproduce el sonido que se haya indicado permitiendo comprobar que, efectivamente, sea el deseado.

Permite escoger un sonido concreto para asociarlo a un evento.

Permite desactivar la reproducción de los sonidos asociados a las diversas acciones.

Aquí se debe escribir la contraseña que se quiera poner a las áreas seleccionadas.

Permite cambiar la contraseña.

Se protegerá con contraseña el acceso a la configuración de **Panda Antivirus**.

Se protegerá con contraseña el acceso a la configuración de los análisis permanentes.

Se protegerá con contraseña el acceso a la actualización del antivirus.

Se protegerá con contraseña el acceso a la configuración de los análisis permanentes.

Se protegerá con contraseña el acceso a la configuración de las actualizaciones.

Permite seleccionar los elementos que se deseen analizar.

Elimina de la lista el elemento seleccionado.

Permite establecer la periodicidad con la que se realizará el análisis.

Permite la configuración del análisis permanente de comunicaciones: correo electrónico, puertos, bloqueo de direcciones de Internet,...etc.

Abre un asistente mediante el cual es posible realizar consultas técnicas.

Configura el análisis heurístico para que avise en todos aquellos archivos con alguna posibilidad de estar infectados por un nuevo virus. Aun en este nivel, la probabilidad de que el antivirus de una falsa alarma es muy baja.

Configura el análisis heurístico para que analice rápidamente pero vigilando todos aquellos archivos que presenten suficientes sospechas de estar infectados por un nuevo virus.

Configura el análisis heurístico para que lleve a cabo su tarea con la mayor velocidad. En este modo, el análisis heurístico sólo detectará archivos con alta probabilidad de estar infectados por virus desconocidos.

Si se marca esta opción y se detecta un virus, se moverá el archivo contaminado a la localización que se indique.

Si se marca esta opción y se detecta un virus, se borrará el archivo contaminado.

Si se marca esta opción y se detecta un virus, se desinfectará el archivo contaminado.

Si se marca esta opción y se detecta un virus, se modificará el nombre del archivo contaminado.

Si se marca esta opción y se detecta un virus, se mostrará información sobre el archivo contaminado.

El análisis se detendrá si se produce algún problema inesperado. Aceptado el aviso se podrá continuar con el análisis normalmente.

Restaura la lista para que vuelva a contener únicamente las extensiones originales.

Elimina de la lista la extensión que se tenga seleccionada.

Elimina todas las extensiones de la lista.

Marcando esta casilla, también serán analizados los ficheros que no tienen extensión.

Este botón permite añadir la extensión escrita en la casilla a tal efecto a la lista de extensiones que se analizarán.

Marcando esta opción se realizará una copia de seguridad del archivo desinfectado.

Marcando esta opción se emitirá un pitido cuando se detecte un virus.

Marcando esta opción se reproducirá el fichero. Wav seleccionado cuando se detecte un virus.

Permite indicar que se debe enviar un mensaje de alerta al remitente del mensaje con virus.

Permite indicar que se debe enviar un mensaje de alerta a los restantes destinatarios de un mensaje infectado con virus.

Permite enviar un mensaje a un puesto seleccionado.

Escriba el mensaje que se enviará al puesto.

Permite enviar un mensaje a un dominio seleccionado.

Escriba el mensaje que se enviará al dominio.

Escriba el nombre del puesto al que se enviará el mensaje.

Escriba el nombre del dominio al que se enviará el mensaje.

Dirección IP del proxy que se utiliza para la conexión a Internet.

Número del puerto de comunicaciones, del proxy que se utiliza para la conexión a Internet.

Nombre del usuario que desea autentificarse, en el acceso a Internet a través del proxy.

Contraseña del usuario que desea autentificarse, en el acceso a Internet a través del proxy.

Muestra la antigüedad del fichero con los identificadores de virus.

Agiliza la realización de otras tareas durante el análisis.

Si se marca esta casilla se ofrecerá la posibilidad de acceder a las páginas bloqueadas al intentar acceder a éstas.

Añade la dirección en este campo en la lista de direcciones a bloquear.

Si se marca esta casilla se ofrecerá la posibilidad de acceder a los servicios bloqueados al intentar acceder a éstos.

Permite indicar la frecuencia con la que se llevará a cabo el análisis: una vez, horario, diario, semanal, mensual o anual.

Permite indicar la hora en la que comenzará el análisis.

Permite indicar la hora límite en la que debe finalizar el análisis. Si no hubiera acabado para dicha hora, se finalizaría en ese momento.

Permite activar o desactivar un análisis programado.

Hace que se lleve a cabo el análisis cada vez que se inicie el ordenador.

Hace que el análisis se haga cada cierto número de arranques del ordenador pudiéndose variar a voluntad el número de arranques.

Hace que el análisis se realice cada cierto número de días pudiéndose indicar dicho número.

Hace que el análisis se lleve a cabo sólo ciertos días de la semana.

Junto con la opción que permite indicar si se desea un análisis semanal, mensual, etc.. permite definir la frecuencia con la que se llevará a cabo el análisis.

Añade el elemento seleccionado a la lista de exclusiones.

Elimina el elemento seleccionado de la lista de exclusiones.

Elimina todos los elementos de la lista de exclusiones.

Permite introducir el nombre de usuario que se facilita al registrarse.

Permite introducir la contraseña que se facilita al registrarse.

Se debe seleccionar en caso de conectarse a Internet a través de un servidor proxy.

Permite indicar la ruta desde donde se realizará la actualización.

Permite establecer la configuración en caso de acceder a Internet a través de un servidor proxy.

Los cambios establecidos en la configuración se guardarán y se aplicarán.

Los cambios establecidos en la configuración no se guardarán ni se aplicarán.

Permite seleccionar la configuración establecida por defecto.

Muestra el nombre del fichero de sonido seleccionado.

Permite introducir la contraseña.

Permite confirmar la contraseña introducida.

Permite introducir la contraseña que se desea cambiar.

Permite establecer una nueva contraseña.

Permite acceder al área de soporte técnico de la Web de Panda Software.

Si se selecciona esta opción se mostrará información sobre la solución Panda PerimeterScan.

Si se pulsa este enlace, se accederá al área de registro online de la web de Panda Software.

Si se marca esta casilla se activará la protección permanente del firewall.

Permite establecer la configuración del firewall.

Permite indicar si se desea analizar las unidades de red o bloquear el acceso a las mismas.

Si se selecciona está opción, no se ejecutarán los archivos de tipo script.

Seleccionando esta opción se analizarán las unidades de red disponibles.

Si se selecciona esta opción se bloquearán las unidades de red en caso de infección.

Permite seleccionar la acción que se realizará en caso de detectarse un virus.

Permite establecer la configuración de las alertas por correo electrónico.

Permite indicar la dirección de correo electrónico a la que se enviarán las alertas.

Permite seleccionar un protocolo para realizar el envío de alertas por correo electrónico.

Permite seleccionar el servidor mediante el que se enviará la alerta.

Permite indicar los tipos de archivos que serán considerados peligrosos.

Si se selecciona esta opción, se bloquearán los adjuntos potencialmente peligrosos.

Seleccionando esta opción, los archivos que presenten doble extensión serán bloqueados.

Marcando esta opción se bloquearán los ficheros con las extensiones que sean seleccionadas.

Permite seleccionar las extensiones de ficheros que se deseen bloquear.

Permite añadir una nueva extensión.

Permite seleccionar la acción que se realizará en caso de detectarse un fichero adjunto peligroso.

Permite establecer los programas que podrán conectarse a Internet.

Permite configurar reglas de conexión avanzadas.

Desplegando este menú podrá establecer si desea permitir o denegar el acceso del programa seleccionado a Internet. También podrá indicar si desea que se le pregunte cada vez que el programa en cuestión intente conectarse a Internet.

Si se selecciona esta opción, los programas propios del sistema operativo se mostrarán en la lista.

Permite añadir un nuevo programa a la lista.

Permite establecer las direcciones con las que se podrán comunicar los programas, así como la configuración de puertos.

Permite eliminar de la lista el programa seleccionado.

Seleccionando esta opción, todas las modificaciones efectuadas se reflejarán en un informe.

Permite indicar la ruta del programa que se desea añadir a la lista.

Permite buscar el programa que se desea añadir a la lista.

Se permitirán las comunicaciones con todas las direcciones IP.

Habilita el recuadro en el que podrá indicar las direcciones IP con las que desea permitir las comunicaciones.

Permite indicar las direcciones IP con las que se desean permitir las comunicaciones.

Si se selecciona esta opción, el programa seleccionado se podrá conectar a Internet. También será posible indicar los puertos a través de los cuales se establecerá esta conexión.

Permite seleccionar un protocolo o indicar los puertos TCP a través de los que se conectará el programa en cuestión.

Permite seleccionar un protocolo o indicar los puertos UPD a través de los que se conectará el programa en cuestión.

Si se selecciona esta opción se permitirá que otros equipos se conecten al programa seleccionado desde la red.

Permite añadir nuevas reglas de conexión.

Permite modificar los parámetros de la regla seleccionada.

Permite borrar la regla seleccionada de la lista.

Si se selecciona esta opción, las nuevas reglas que se apliquen quedarán reflejadas en un informe.

Permite indicar el nombre que se desee asignar a la nueva regla.

Desplegando este menú se podrá seleccionar la acción que realizará la nueva regla.

Desplegando este menú, se podrá seleccionar el adaptador de red sobre el que actuará la regla.

Permite seleccionar el protocolo sobre el que actuará la regla.

Permite indicar si la regla actuará sobre las comunicaciones de entrada, de salida o sobre ambas.

Si se selecciona esta opción, la regla se aplicará sobre cualquier dirección remota.

Permite indicar la dirección de la tarjeta de red sobre la que actuará la regla.

Permite indicar las direcciones IP sobre las que actuará la regla.

Permite indicar las direcciones IP sobre las que actuará la regla. Se podrán indicar direcciones completas, o intervalos separados por comas.

Permite seleccionar el adaptador de red, a través del cual se desea permitir o denegar el acceso el acceso a carpetas compartidas.

Se permitirá a otros usuarios acceder a las carpetas que se encuentren compartidas en este ordenador.

Permite el acceso a carpetas que se encuentren compartidas en otros ordenadores.

Si se selecciona esta opción, se mostrará un aviso cada vez que un intento de intrusión sea bloqueado.

Permite configurar el perfil de correo, opciones de actualización, restricciones por contraseña, sonidos, elementos analizables, etc.