

AVAST! antivirus
Edición Profesional
Versión 4.8

Guía de Usuario

CONTENIDO

Introducción.....	4
Acerca de ALWIL Software a.s.	4
Más ayuda.....	4
Amenazas para su ordenador	5
¿Qué es un virus?	5
¿Qué es un spyware?	5
¿Qué son los rootkits?	5
Características principales de avast! antivirus.....	6
Kernel antivirus	6
Protección residente (o protección “Por acceso”).....	7
Tecnología anti-spyware integrada.....	7
Tecnología anti-rootkit integrada	7
Gran autoprotección.....	7
Actualizaciones automáticas	7
Baúl de virus	8
Integración del sistema.....	8
Limpiador de Virus avast! Integrado (Virus Cleaner).....	8
Escaneo de la línea de comandos.....	9
Bloqueo de Scripts	9
Actualizaciones PUSH.....	9
Interfaz de usuario Avanzada	9
Requisitos del sistema	10
Cómo instalar avast! antivirus Professional Edition.....	11
Primeros pasos	16
Protección de contraseña	18
Cómo registrarse para obtener la Clave de Licencia	18
Inserción de la Clave de Licencia.....	20
Fundamentos en la utilización de avast! antivirus.....	21
Protección Residente “Por acceso”	21
Cómo ejecutar un escaneo de virus manual – la Interfaz Simple de Usuario.....	25
Seleccionar manualmente las áreas a ser escaneadas	27
Ajuste de la sensibilidad y ejecución del escaneo	29
Ejecución del escaneo y procesamiento del resultado	30
Cambiar la apariencia de la Interfaz Simple de Usuario	31
Qué hacer si se encuentra un virus	33
Resultados del último escaneo.....	37
Funciones avanzadas	38
Ajustar actualizaciones automáticas	38
Cómo programar un escaneo al inicio	39
Excluir ficheros del escaneo.....	41
Cómo crear un archivo de informe de los resultados del escaneo	42
Alertas.....	45
SMTP	46
Buscar la Base de Datos de Virus	47
Trabajar con ficheros en el Baúl de Virus	49
El Visor de Informes	51

Cómo trabajar con la Interfaz Avanzada de Usuario.....	54
<i>Cómo trabajar con las Tareas</i>	55
<i>Crear/editar una tarea</i>	55
<i>Crear una nueva tarea “Por demanda”</i>	56
<i>Crear una nueva tarea “Por acceso”</i>	64
Sesiones: Ejecutar una tarea “Por demanda”.....	65
<i>Programar tareas/actualizaciones existentes</i>	66
<i>Programar un escaneo al inicio</i>	68
<i>El baúl de virus</i>	68
<i>Cómo buscar la Base de Datos de Virus</i>	69
<i>Visor de Informes</i>	70
<i>Limpiador de virus</i>	70
<i>Instalación Silenciosa</i>	71
Cómo activar el protector de pantalla avast! antivirus.....	72
Ajustes de la Protección Residente.....	74
Otros ajustes avast!.....	90
<i>Ajustes comunes</i>	91
<i>Extensión Explorer</i>	91
<i>Apariencia</i>	91
<i>Interfaz Avanzada (sólo se muestra si se utiliza la Interfaz Avanzada de Usuario)</i>	91
<i>Confirmaciones</i>	92
<i>Modificar el idioma del programa</i>	94
<i>Sonidos</i>	95
<i>Actualizar (Conexiones)</i>	96
<i>Problemas</i>	97
Cómo utilizar el escáner de la línea de comandos.....	99
Cómo desinstalar avast! antivirus.....	100

Introducción

Bienvenido a avast! antivirus Professional Edition version 4.8.

avast! antivirus comprende un conjunto de galardonadas altas tecnologías que trabajan en perfecta sinergia, teniendo un objetivo en común: proteger su sistema y datos de más valor contra los virus de ordenador. Representa una de las mejores soluciones dentro de su gama para cualquier ordenador basado en Windows.

avast! antivirus incorpora tecnología anti-spyware y, certificado por el proceso de West Coast Lab's Checkmark, así como anti-rootkit y una fuerte capacidad de auto-protección para asegurar que sus datos más valiosos y programas estén siempre protegidos.

Acerca de ALWIL Software a.s.

Desde 1988, ALWIL Software has producido productos antivirus que han sido desarrollados en la multi-galardonada línea de productos avast! antivirus, haciendo de avast! uno de los productos más maduros y testados en el mercado antivirus.

Con su sede en Praga, en la República Checa, ALWIL Software desarrolla y comercializa los productos antivirus avast! que protegen cada uno de los principales sistemas operativos y tipo de dispositivos más vulnerables. Más detalles sobre la compañía y sus productos se pueden encontrar en nuestra página web, www.avast.com.

avast!® es una marca registrada en los Estados Unidos de América y otros países y se utiliza bajo licencia exclusiva de ALWIL Software a.s.

Más ayuda

Si se encontrara con alguna dificultad al utilizar su programa antivirus avast! y no le fuese posible resolverlo aún después de haber leído este manual, podrá encontrar la respuesta en el Centro de Soporte de nuestra página web en <http://support.avast.com>

- En la sección [Base de conocimiento](#), puede encontrar rápidamente las respuestas a algunas de las preguntas más frecuentes.
- Alternativamente, puede aprovecharse de los Foros de Soporte avast!. Aquí podrá interactuar con otros usuarios de avast! que han podido experimentar el mismo problema que usted y haber descubierto la solución. Deberá registrarse para poder utilizar el foro, pero es un proceso muy rápido y sencillo. Para registrarse y poder utilizar el foro, vaya a <http://forum.avast.com/>

Si aún no ha sido capaz de resolver su cuestión, puede “[Enviar un tique](#)” a nuestro equipo de soporte. También deberá registrarse para poder hacer esto y cuando nos escriba, por favor, asegúrese de incluir la mayor información posible.

Amenazas para su ordenador

Virus, spyware, rootkits y toda forma de software malicioso, son colectivamente conocidos como malware (abreviatura de software malicioso); los malware a veces también se denominan “badware”.

¿Qué es un virus?

Un virus de ordenador es un fragmento de software, normalmente malicioso por naturaleza, utilizado para propagarse por sí mismo o a otros programas de software similares, de ordenador a ordenador. Los virus por si solos pueden causar daños al sistema, pérdida de datos importantes, o pueden ser utilizados para instalar spyware, rootkits u otros malware en un sistema vulnerable.

Una forma clave de prevenir infecciones es disponer de una solución antivirus actualizada instalada en todos los ordenadores de la red, y asegurarse de que estén instaladas todas las correcciones de seguridad más actuales del sistema operativo del ordenador. Los usuarios deberían asimismo asegurarse de que la fuente de software de la que están descargando en internet es fiable, pues muchos tipos de malware se instalan junto a otros software aparentemente legítimos.

¿Qué es un spyware?

Spyware es un software instalado en el sistema de un ordenador, diseñado para recopilar información acerca del ordenador del usuario a menudo sin su consentimiento o conocimiento. Esta información puede dar lugar a los llamados robos de identidad, o ladrones de información valiosa (tales como detalles bancarios o de tarjetas de crédito) o datos de propiedad comercial.

Hoy en día muchos de los actuales spyware se desarrollan por anillos organizados de delincuencia con preferencia sobre individuales oportunistas solitarios, y se instalan a través de virus u otras formas de malware.

¿Qué son los rootkits?

Los rootkits son programas que se instalan en su sistema, guardándose al mismo tiempo a sí mismos, sus procesos, servicios y claves de registro ocultas, con el objetivo de permanecer invisibles para el usuario. Representan un riesgo considerable en la seguridad tanto a nivel domestico como en las redes empresariales, y son notoriamente difíciles de encontrar y eliminar.

Los rootkits se despliegan normalmente por sí mismos a través de otra vía de infección malware (tales como Troyanos, por ejemplo) y, por tanto, se recomienda que los usuarios de ordenadores dispongan de un antivirus actualizado / sistema anti-spyware instalado y en funcionamiento en su PC. Dicho sistema es avast! antivirus 4.8.

Características principales de avast! antivirus

avast! es la multi-galardonada línea de productos ALWIL Software a.s., certificada por ICSA Labs, Y Checkmark (tanto como antivirus y anti-malware). avast! antivirus recibe regularmente el premio Virus Bulletin 100% Award, por la detección del 100% de los virus en circulación, y ha sido ganador repetitivo del premio Secure Computing Award.

avast! antivirus se usa en más de 80 millones de hogares y oficinas en todo el mundo; está específicamente diseñado para tener unos requerimientos mínimos del sistema y actualizarse tanto a sí mismo como a las definiciones de virus automáticamente.

avast! antivirus representa una colección de altas tecnologías creadas para ofrecerle una protección inigualable contra todas las formas malware. Las características clave de avast! antivirus Home Edition y Professional Edition se comparan y describen más abajo.

Características clave	Home Edition	Professional Edition
Kernel antivirus basado en un alto rendimiento del motor antivirus	Sí	Sí
Gran protección residente	Sí	Sí
Anti-spyware integrado	Sí	Sí
Detección rootkit integrada	Sí	Sí
Gran autoprotección	Sí	Sí
Actualizaciones automáticas progresivas	Sí	Sí
Baúl de virus para depositar ficheros sospechosos	Sí	Sí
Integración del sistema	Sí	Sí
Limpiador de virus integrado	Sí	Sí
Escaneo de la línea de comandos	No	Sí
Script blocker	No	Sí
Actualizaciones PUSH	No	Sí
Interfaz de usuario avanzada y capacidad para crear y programar tareas concretas	No	Sí

Kernel antivirus

El kernel del antivirus es el núcleo básico del programa. La última versión del kernel del antivirus avast! combina extraordinarias capacidades de detección con un gran rendimiento. Puede contar con una detección al 100% de los virus en circulación (virus que ya se han propagado entre los usuarios) y una excelente detección contra caballos de Troya.

El kernel está certificado por [ICSA Labs](#); participa frecuentemente en los test de la revista Virus Bulletin, recibiendo a menudo el premio VB100.

Protección residente (o protección “Por acceso”)

La protección residente (la protección en tiempo real del sistema del ordenador), es una de las características más importantes de un programa antivirus hoy en día. La protección residente de avast! es una combinación de varias partes de “módulos residentes” que son capaces de detectar un virus antes de que tenga opción de infectar su ordenador.

Tecnología anti-spyware integrada

Avast! antivirus ahora dispone de tecnología anti-spyware integrada, la cual está certificada por el proceso de certificación de West Coast Labs Checkmark y ofrece incluso mayor protección de sus datos más valiosos y programas.

Tecnología anti-rootkit integrada

La tecnología anti-rootkit basada en la tecnología líder GMER que también está incorporada en el programa como un estándar. Si se descubre un rootkit, es inicialmente deshabilitado y después, si puede ser eliminado de forma segura sin afectar al rendimiento del ordenador, es eliminado. avast! antivirus incluye una base de datos de virus que puede ser automáticamente actualizada para proveer continua protección contra los rootkits.

Gran autoprotección

Algunos virus pueden intentar apagar un software antivirus de ordenador. Para proteger su ordenador incluso contra las últimas amenazas que podrían intentar desactivar su protección de seguridad, avast! dispone de la mejor y más fuerte autoprotección de su clase. Esto se basa en la multigalardonada tecnología antivirus avast! y provee un nivel extra de seguridad para asegurarse de que sus datos y programas estén siempre protegidos.

Actualizaciones automáticas

Las actualizaciones automáticas son otra clave necesaria en la protección contra virus. Tanto la base de datos virus como del programa en sí mismo pueden ser actualizados automáticamente. Las actualizaciones son *progresivas*, solo descargando datos nuevos o en falta, reduciendo significativamente el tiempo de transferencia. El tamaño típico de una base de datos de virus es decenas de KB mientras que las actualizaciones del programa suelen ser típicamente no superiores a cientos de KB.

Si su conexión a Internet es continua (tal como una conexión de banda ancha), las actualizaciones tienen lugar de forma completamente automática en intervalos de tiempo fijos. Si se conecta a Internet solo de forma ocasional, avast! monitoriza su conexión e intenta realizar la actualización cuando usted esté on-line. Esta característica se describe con detalle en la [página 38](#).

Baúl de virus

El Baúl de virus se puede ver como una carpeta en su unidad de disco con disponibilidad de unas propiedades especiales que le hacen un lugar seguro, aislado apropiado para el almacenamiento de ficheros potencialmente dañinos. Usted puede trabajar con los ficheros en el Baúl, aunque con algunas restricciones de seguridad.

Las propiedades principales del Baúl de Virus son aislamiento completo del resto del sistema operativo. Ningún proceso externo, como puede ser un virus, puede acceder a los ficheros que estén dentro, y el hecho de que los ficheros contenidos dentro del Baúl no puedan ejecutarse significa que no hay ningún peligro en almacenar dichos virus ahí. Para más información, véase la [página 49](#).

Integración del sistema

Avast! antivirus está completamente integrado en su sistema. La Extensión Explorer permite el inicio directo de un escaneo con solo hacer clic en una carpeta o fichero con el botón derecho del ratón y seleccionando la elección correspondiente del menú desplegable.

También se provee un salvapantallas especial el cual, cuando está activo, lleva a cabo un escaneo de virus. Avast! antivirus funciona con su salvapantallas favorito, con lo que usted no tiene que cambiar sus ajustes personales para poder utilizarlo. Para establecer el salvapantallas avast! antivirus, véase la [página 72](#).

En versiones 32-bit de Windows NT/2000/XP/Vista, también es posible ejecutar un “escaneo programado para el inicio” que le permitirá llevar a cabo un escaneo mientras el sistema se pone en marcha y *antes* de que un virus se pueda activar. Esto es útil en el caso de que usted sospeche que su ordenador ya se ha infectado por un virus.

Limpiador de Virus avast! Integrado (Virus Cleaner)

avast! antivirus ha sido esencialmente diseñado para proteger su ordenador contra infecciones de virus u otras formas de malware. Su función principal es la prevención más que la cura. Sin embargo, ahora incorpora un Limpiador de Virus especial que es capaz de eliminar algunos de los virus más comunes en ordenadores infectados.

Desafortunadamente, el número de virus en circulación está creciendo constantemente y en el caso de que su ordenador se infecte por un virus que no puede ser eliminado por el Virus Cleaner, puede que sea necesario buscar la asistencia de un experto.

Se puede encontrar más información sobre el Limpiador de Virus en la [página 70](#)

Escaneo de la línea de comandos

Para usuarios con experiencia, la Edición Profesional ofrece un escaneo de la línea de comandos. El programa ashCmd utiliza exactamente el mismo kernel de escaneo que avast!, con lo que los resultados son exactamente los mismos. El escaneo se lleva a cabo en la línea de comandos utilizando un rango de parámetros y conmutadores, y un modo STDIN/STDOUT especial está disponible. Este módulo está pensado para ser utilizado en programas BATCH y su output es el mismo que el de las tareas de la Interfaz de Usuario Avanzada (incluyendo los ficheros de reporte). Se puede encontrar una guía sobre cómo utilizar el escaneo de la línea de comandos en la [página 99](#).

Bloqueo de Scripts

El “script blocker” integrado es un módulo que protege su ordenador contra scripts de virus ocultos en páginas web. Tales scripts son normalmente inofensivos, pues los programas que los ejecutan les impide de acceder a cualquier fichero. Sin embargo, puede haber una brecha de seguridad en un navegador que puede ser aprovechada por un virus, lo cual podría resultar en infección de su ordenador. Por lo tanto, avast! Controla las páginas web que usted visita para cualquier script que pudiera ser potencialmente peligroso.

Actualizaciones PUSH

Una característica especial de la Edición Profesional son las actualizaciones PUSH. Supone un cambio dramático en la filosofía de las actualizaciones. Generalmente, cada programa instalado busca ocasionalmente las nuevas versiones disponibles. Las actualizaciones PUSH, sin embargo, son iniciadas por nuestro servidor; aparecerán en su ordenador respondiendo y ejecutando la actualización necesaria rápidamente. El sistema está basado en el protocolo SMTP (como el utilizado para mensajes de e-mail). La actualización en sí misma es controlada por los clientes de e-mail residentes de avast! (*MS Outlook e Internet Mail*). El sistema completo está protegido por cifrados asimétricos resistentes a abusos desautorizados.

Interfaz de usuario Avanzada

avast! antivirus Professional Edition incluye una interfaz avanzada de usuario donde se pueden crear “tareas” especiales que pueden ser programadas para ser ejecutadas en un momento concreto en el futuro, o de modo regular e.g. diariamente, semanalmente o mensualmente. Siempre que se ejecute una tarea se creará una nueva “Sesión” en la que se almacenarán los resultados, los cuales podrán ser visualizados posteriormente. A diferencia de la interfaz simple de usuario, cuando se trabaja en la interfaz avanzada de usuario es posible especificar de antemano qué acción debería llevarse a cabo si se detecta un virus. Por ejemplo, usted puede establecer que el programa intente reparar inmediatamente cualquier fichero infectado. También se puede especificar una acción alternativa para el caso de que la primera acción no fuese satisfactoria. Por ejemplo, si un fichero no se puede reparar, puede ser automáticamente movido al baúl de virus. Las características de la interfaz avanzada de usuario se describen detalladamente en la [página 54](#).

Requisitos del sistema

Las configuraciones de hardware descritas más abajo, representan la especificación del sistema **mínima** recomendada para dicho sistema operativo.

Para un ordenador con Windows® 95/98/Me:

486 Processor, 32MB RAM y 100 MB de espacio libre en el disco duro.

Para un ordenador con Windows® NT® 4.0:

486 Processor, 24MB RAM y 100 MB de espacio libre en el disco duro y Service Pack 3 (o superior) instalado

Para un ordenador con Windows® 2000/XP® Workstation (Not Server):

Pentium class Processor, 64MB RAM (128MB recomendados) y 100 MB de espacio libre en el disco duro

Para un ordenador con Windows® XP® 64-bit Edition:

Un AMD Athlon64, Opteron o Intel EM64T-enabled Pentium 4 / Xeon processor, 128MB RAM (256MB recomendados) y 100 MB de espacio libre en el disco duro

Para un ordenador con Windows® Vista:

Pentium 4 processor, 512MB RAM y 100 MB de espacio libre en el disco duro

El programa en sí mismo requiere sobre 60 MB de espacio libre en el disco duro; el resto del espacio recomendado está reservado para el fichero de la base de datos de recuperación de virus y su índice, y los ficheros de instalación.

Un **MS Internet Explorer 4** funcional o superior es requerido para que el programa pueda funcionar.

Este producto **no se puede instalar en sistemas operativos server** (familias de Windows NT/2000/2003 Server).

Nota: pueden surgir varios problemas como resultado de la instalación de más de un producto de seguridad en el mismo ordenador. Si usted ha instalado otro software de seguridad, se recomienda desinstalarlo antes de intentar instalar avast!

Cómo instalar avast! antivirus Professional Edition





Esta sección describe cómo descargar e instalar avast! antivirus Professional Edition en su ordenador y cómo instalar su clave de licencia en el software una vez que el proceso de descarga e instalación haya sido completado. Las ventanas que aparecen en las siguientes páginas se muestran según aparecen en Windows XP y pueden diferir ligeramente de otras versiones de Windows.

avast! antivirus Professional Edition puede ser descargado desde www.avast.com.

Se recomienda cerrar todos los programas de Windows antes de iniciar la descarga.

Haga clic en “Descargar” a continuación “Descargar programas” y después seleccione la versión a descargar.

Seleccione la versión del idioma que necesite de la lista de idiomas disponible – véase más abajo – y haga clic en la casilla gris “Descargar”.

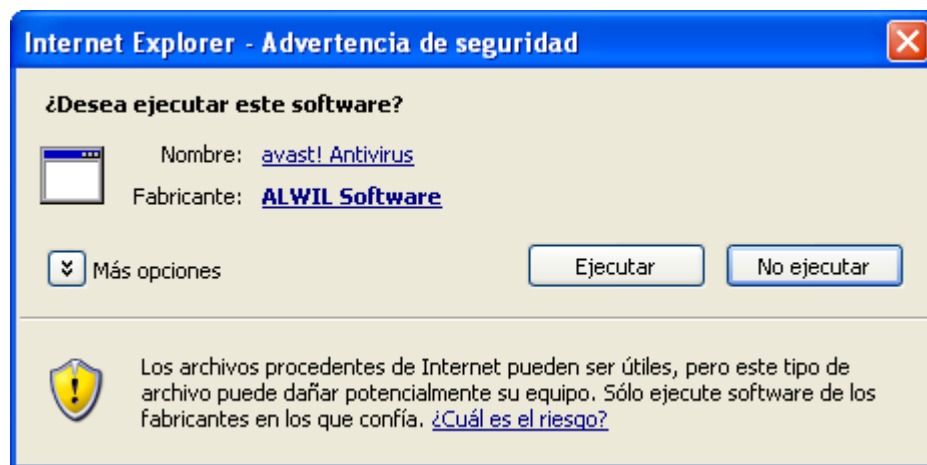
	Descargar avast! 4 Professional Edition
	avast! 4 Professional - versión en Inglés (tamaño 21.70 MB)
	avast! 4 Professional - versión en Árabe (tamaño 21.50 MB)
	avast! 4 Professional - versión en Búlgaro (tamaño 21.54 MB)
	avast! 4 Professional - versión en Catalán (tamaño 21.80 MB)

Si utiliza Internet Explorer como navegador web, le aparecerá el cuadro mostrado mostrado más abajo:



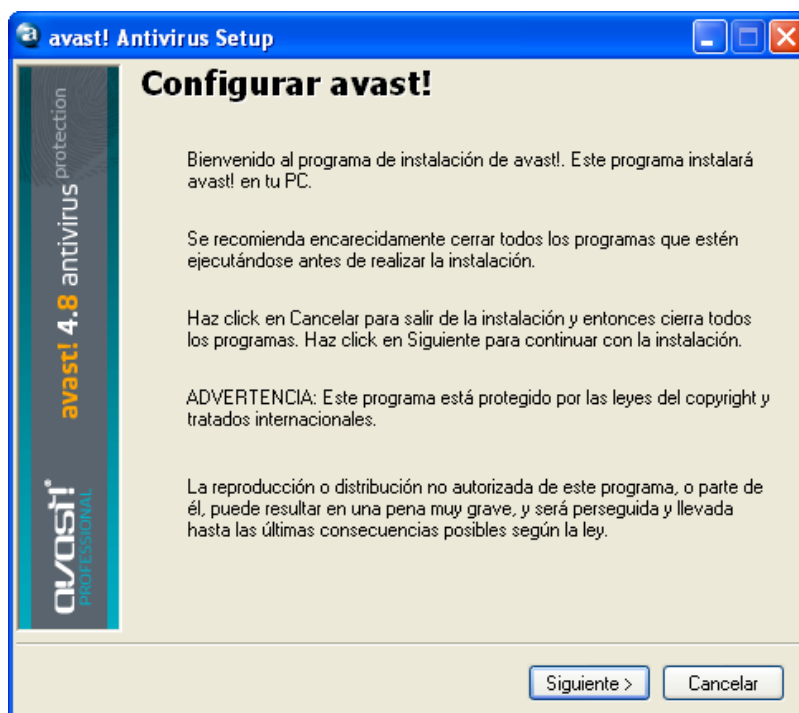
Haciendo clic tanto en “Ejecutar” como en “Guardar” se iniciará la descarga del fichero de instalación “Setupeng.exe” a su ordenador.

Si desea instalar avast! antivirus en su ordenador inmediatamente después de que el fichero se haya descargado, haga clic en “Ejecutar”. Una vez que el fichero de instalación haya sido descargado, se le presentará la siguiente ventana:



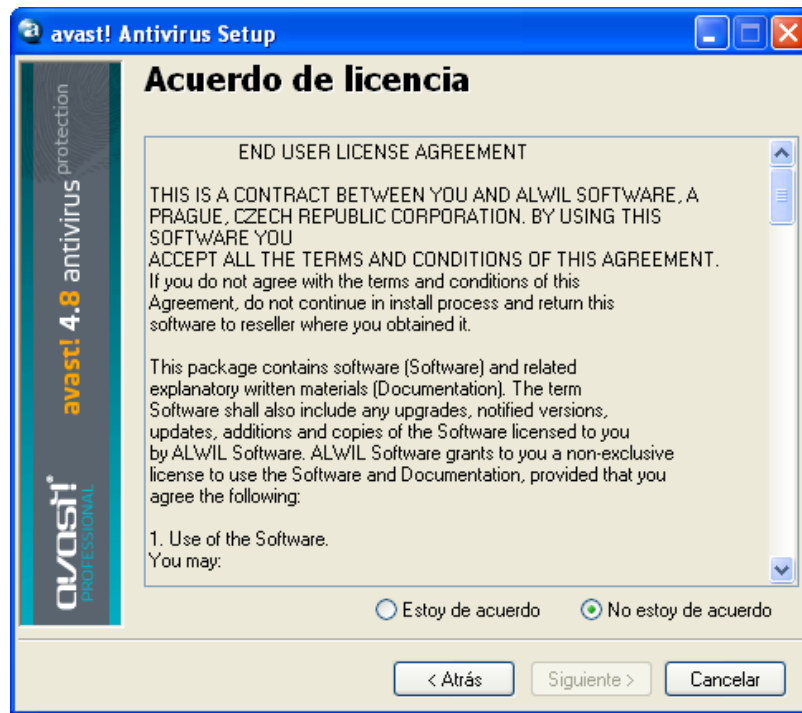
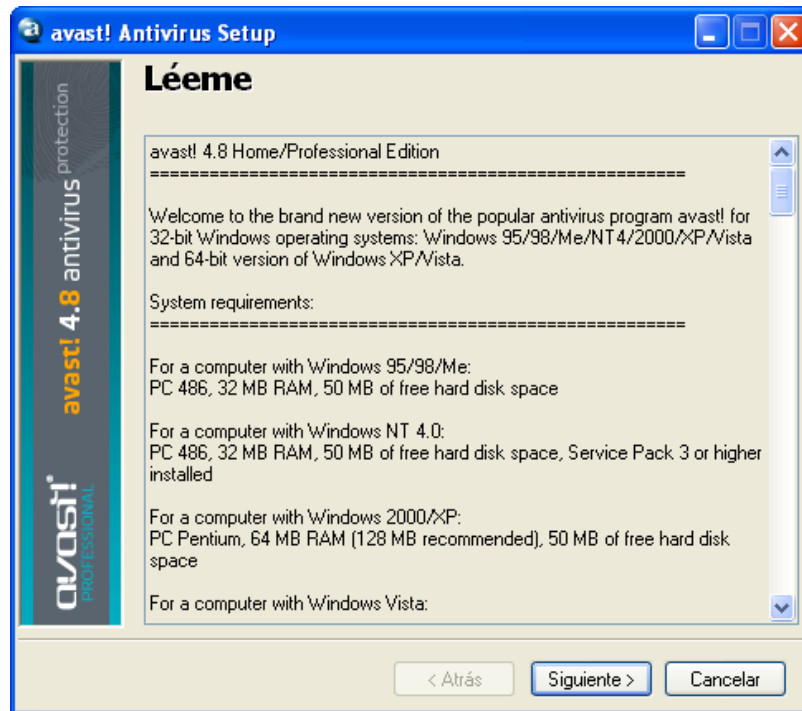
En otros navegadores web, puede que solamente tenga la opción de “Guardar” el fichero. Haciendo clic en “Guardar” descargará el software a su ordenador, pero no se instalará en este momento. Para completar el proceso de instalación será necesario ejecutar el fichero de instalación “Setupeng.exe”, por tanto ¡Recuerde dónde lo ha guardado! Haga doble clic en el fichero para ejecutarlo.

Haciendo clic de nuevo en “Ejecutar”, le llevará a la ventana Configurar avast!:



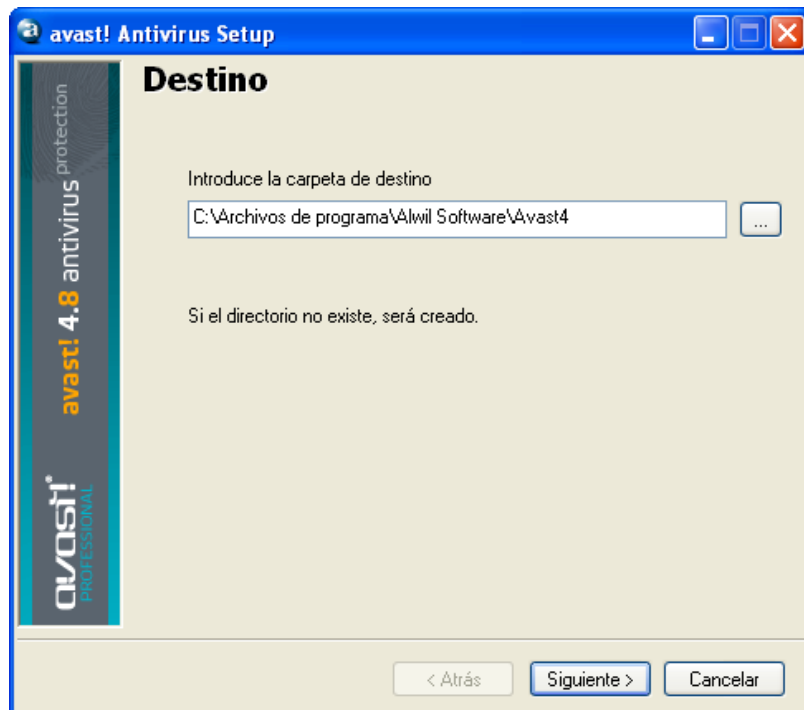
Haga clic en “Siguiete” y la instalación asistente le guiará durante el resto del proceso de instalación.

Primero se le pedirá que lea los requisitos mínimos del sistema, y después confirmar que está de acuerdo con las condiciones de licencia de usuario – vea las dos ventanas siguientes.

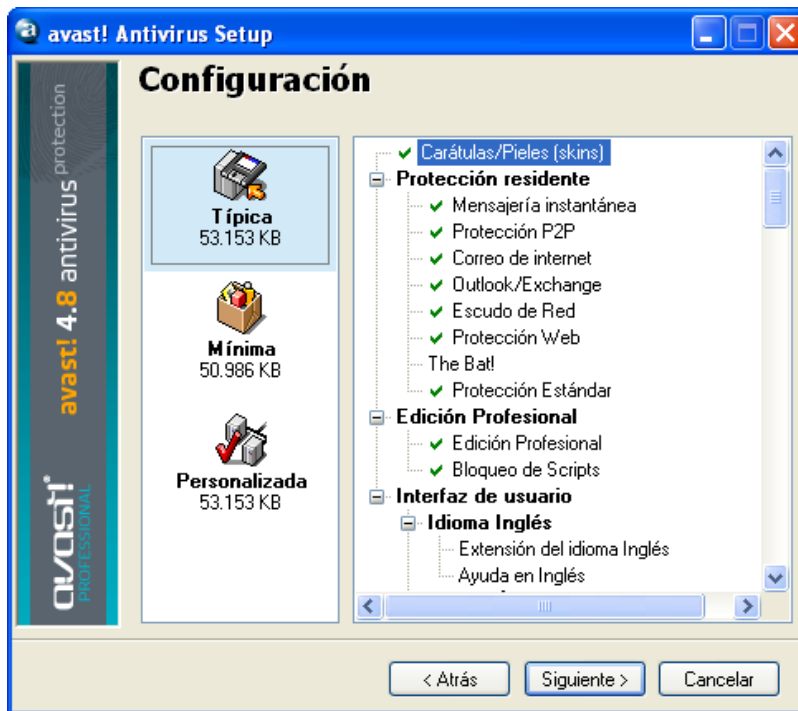


Para continuar, es necesario hacer clic en “Estoy de acuerdo” y después en “Siguiete”.

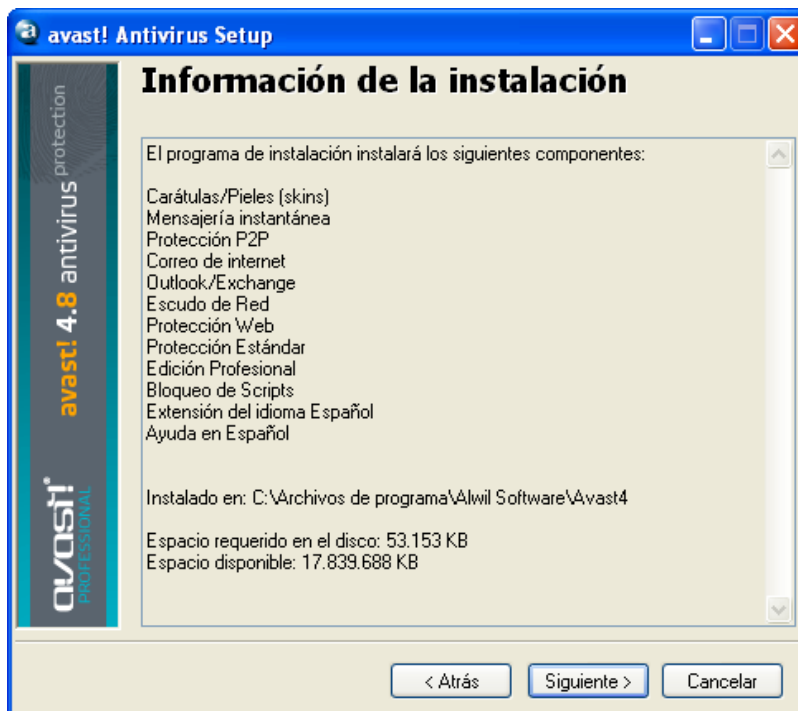
Después se le pedirá que confirme el directorio de destino, i.e. dónde deberían ser guardados los ficheros del programa. El programa lo seleccionará automáticamente o creará un nuevo directorio si aún no existe. Se recomienda aceptar el directorio de destino por defecto y simplemente hacer clic en “Siguiente” para continuar.



En la ventana siguiente se le pedirá confirmar la configuración. Las opciones más apropiadas para la mayoría de los usuarios son seleccionadas automáticamente. A no ser que usted desee cambiar alguno de los ajustes por defecto, e.g. la selección del idioma, sólo tendrá que hacer clic en “Siguiente” para continuar.



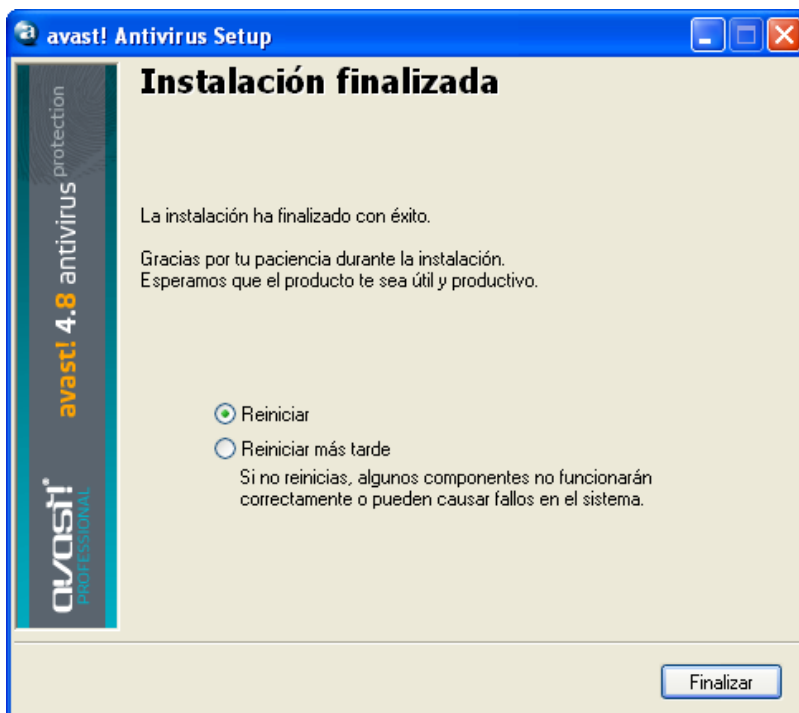
A continuación el programa confirmará qué debe ser instalado y dónde, así como la cantidad de espacio necesaria y disponible en el disco. Haga clic en “Siguiete” para continuar.



Posteriormente se le preguntará si desea programar una búsqueda de virus al inicio del sistema – véase [página 39](#).

La ventana final debería confirmar que la instalación ha sido completada satisfactoriamente, sin embargo, para completar íntegramente el proceso será necesario reiniciar su ordenador.

Con “Reiniciar” seleccionado, haga clic en “Finalizar” y su ordenador se reiniciará automáticamente.



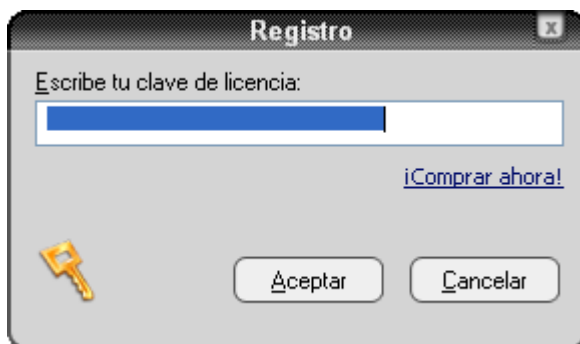
La instalación ya ha sido completada.

Primeros pasos

Al reiniciar su ordenador, debería ver un icono de una bola azul con una “a” en el medio, en la parte inferior derecha de la pantalla de su ordenador.

Avast antivirus Professional Edition se puede utilizar de forma gratuita durante los primeros 60 días, pero al final de dicho periodo, si deseara continuar utilizándolo, deberá comprar una clave de licencia.

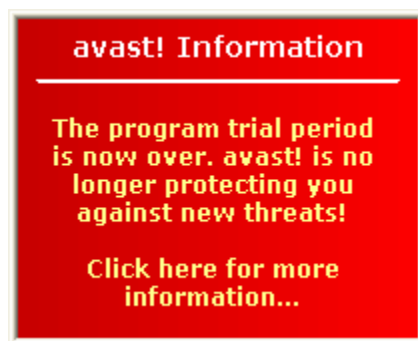
Por consiguiente, la primera vez que ejecute el programa le aparecerá la siguiente ventana:



No es necesario insertar inmediatamente una clave de licencia. Si desea ejecutar el programa hasta 60 días sin tener que solicitar una clave de licencia, simplemente haga clic en "Demo". Sin embargo, puede solicitar una clave de licencia ahora haciendo clic en "comprar ahora" y siguiendo el procedimiento descrito en la sección siguiente.

Una vez haya seleccionado ejecutar la versión Demo, esta casilla no aparecerá la próxima vez que ejecute el programa. Sin embargo, puede solicitar una clave de licencia en cualquier momento – véase la página siguiente "Cómo registrarse para una Clave de Licencia"

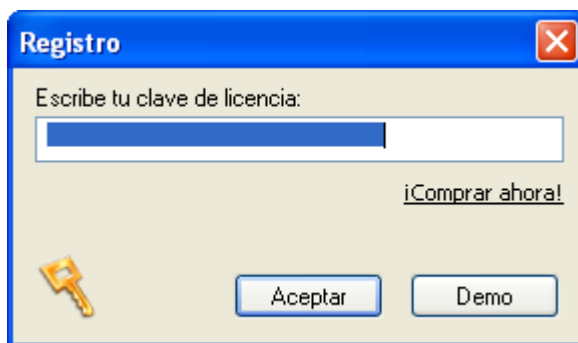
Después de 60 días, si la clave de licencia no se ha insertado en el programa, el siguiente aviso aparecerá en la esquina inferior derecha de la pantalla de su ordenador:



El siguiente mensaje también será mostrado siempre que inicie el programa:



Haciendo clic en “OK” aparecerá la casilla de Registro según se presenta a continuación:



El procedimiento de obtención e inserción de la clave de licencia se encuentra descrito en las páginas siguientes.

Protección de contraseña

Haciendo clic en la bola azul con la “a” en el medio que se encuentra en la esquina inferior derecha de la pantalla y seleccionando “Establecer/cambiar contraseña”, puede crear una contraseña para proteger su programa antivirus ante cambios no autorizados.

Cómo comprar la Clave de Licencia

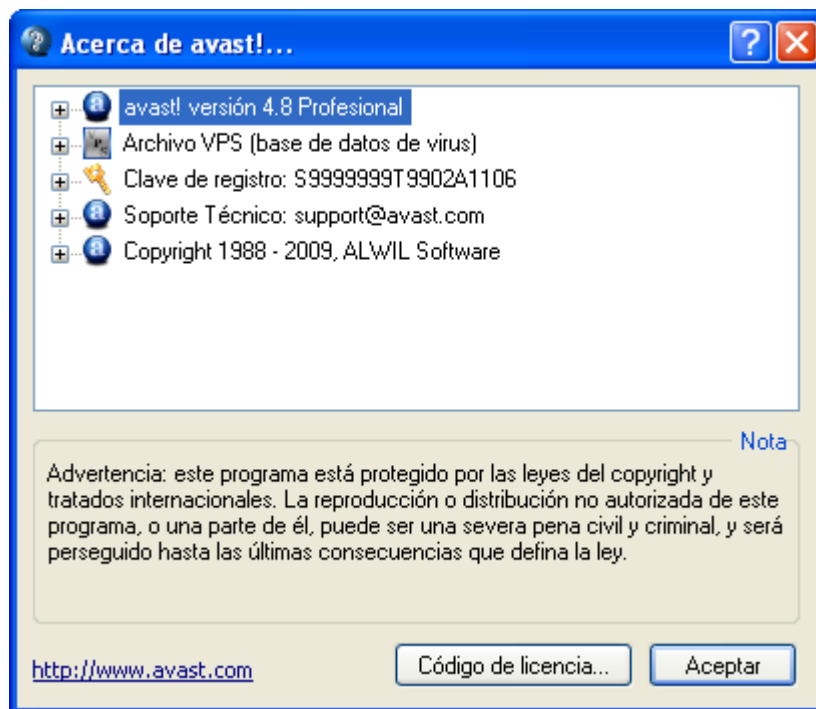
Si usted desea continuar utilizando el programa después de los 60 días gratuitos del periodo de prueba, necesitará comprar una clave de licencia válida e insertar la misma en el programa. Las claves de licencia para avast! antivirus Professional Edition se pueden comprar para un periodo de 12, 24 ó 36 meses.

Para más detalles sobre las opciones de pago, así como lista de precios y conversor de divisa, visite www.avast.com y haga clic en “comprar” en la parte superior de la página.

Para comprar una clave de licencia, haga clic en “comprar” y después en una de las “Desktop solutions”, “Small Business Solutions” o “Corporate Solutions”. Después seleccione “avast 4 Professional Edition”. En la ventana siguiente, haga clic en la opción “Comprar” y despliegue la ventana hacia abajo para seleccionar “1 Año”, “2 Años” ó “3 Años”.

En este momento necesitará confirmar el número de licencias que desea comprar e insertar sus datos personales y de pago. Una vez haya completado su compra, le llegará su clave de licencia a su dirección de correo electrónico en 24 horas.

Alternativamente, si usted ya ha descargado e instalado el programa, haga clic con el botón derecho del ratón en la bola azul con la “a” en el medio, en la esquina inferior derecha de su pantalla y seleccione “Acerca de avast! ...”



Haga clic en “Código de licencia” y aparecerá la casilla de Registro – haga clic en “Comprar ahora”.

Esto le llevará a la página web de avast! donde podrá seleccionar la duración de la licencia que usted necesita y comprar la misma según se ha descrito anteriormente.

Inserción de la Clave de Licencia

Una vez reciba su clave de licencia (enviada vía email a la dirección especificada durante el proceso de compra), deberá ser insertada en el programa. Esto permitirá que el programa se actualice automáticamente y prevenga los avisos de la clave de licencia.

Nota – el programa avast! debe ser descargado e instalado con anterioridad para poder insertar la clave de licencia.

Para ver un video instructivo mostrando cómo insertar la clave de licencia sin tener que iniciar el programa, haga clic [aquí](#) o visite www.avast.com y haga clic en “Soporte” en la parte superior de la pantalla. Haga clic en “Soporte Técnico” en el menú ofrecido más abajo. A continuación encuentre el título “Video de instrucciones” en la esquina inferior izquierda de la pantalla y haga clic en “Cómo insertar la clave de activación”.

Alternativamente, siga los pasos descritos más abajo.

1. Seleccione la clave de registro en el mismo e-mail en el que ha recibido de avast! Para ello, sitúe el cursor activo inmediatamente a la izquierda de la primera letra de la clave de licencia. Haga clic con el botón izquierdo del ratón y, con el botón izquierdo aún presionado, mueva el ratón hacia la derecha hasta que toda la clave quede seleccionada. Suelte el botón izquierdo del ratón, a continuación mueva el ratón hasta situar el cursor en el área seleccionada de la clave de licencia. Haga clic con el botón derecho del ratón y, en el menú desplegado, seleccione “Copiar”.
2. Haga clic con el botón derecho del ratón en el icono de la bola azul con la “a” en el medio en la esquina inferior derecha de su pantalla y haga clic con el botón izquierdo del ratón en "Acerca de avast!"
3. Haga clic con el botón izquierdo del ratón en la pestaña "Licencia" que puede encontrar en la esquina inferior derecha.
4. Sitúe el cursor en la casilla de la clave de licencia, haga clic con el botón derecho del ratón y, de la lista de las opciones del menú, seleccione “Pegar”. Ahora, la clave de licencia ya está insertada.
5. Haga clic en “OK”. Ahora puede seguir utilizando el programa durante 12, 24, ó 36 meses desde el final del 60º día del periodo Demo, según la licencia adquirida. Al final del periodo de la licencia, será necesario simplemente comprar e insertar una nueva clave de licencia.

Fundamentos en la utilización de avast! antivirus

avast! antivirus prove protección contra todo tipo de malware y contiene una potente “protección residente”, también denominada protección “on-access” puesto que controla los ficheros en el momento en el que se accede a los mismos.

Normalmente la protección residente prove toda la protección que necesita para prevenir que su ordenador se infecte de virus. Una vez que el programa haya sido descargado, la protección residente se ejecuta continuamente en segundo plano y supervisa todas las partes de la actividad de su ordenador. Sin embargo, si por cualquier motivo se desconecta la protección residente, o si ha estado inactiva durante algún tiempo, es posible llevar a cabo un escaneo manual retrospectivo (también conocido como escaneo “a petición”) de todos los ficheros en su ordenador.

avast! Antivirus también incluye un salvapantallas especial que escanea constantemente su ordenador cuando está conectado pero no está actualmente en uso.

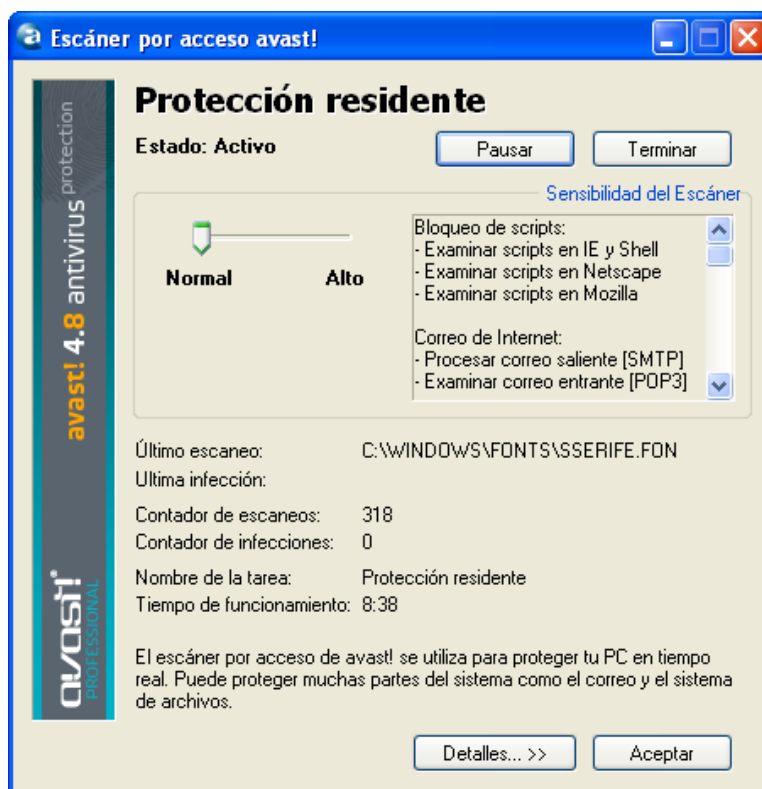
Protección Residente “Por acceso”

Esta parte del programa supervisa continuamente todo el ordenador y todos los programas abiertos para detectar cualquier actividad (e.g. un virus), de modo que previene cualquier daño a los ficheros de su ordenador. Se ejecuta de forma completamente independiente (se activa automáticamente al iniciar su ordenador) y si todo está BIEN, usted no se dará ni cuenta de que se está ejecutando.

El icono de la bola azul “a” que puede encontrar en la esquina inferior derecha de la pantalla del ordenador, al lado del reloj, muestra el estado actual de la protección residente. Normalmente, la presencia de la bola azul “a” indica que la protección residente está instalada y activa protegiendo su ordenador. Si la bola “a” tiene una línea roja cruzada, la protección está actualmente inactiva y su ordenador no está protegido. Si aparece en color gris, significa que la protección ha sido parada – véase página siguiente.

Se puede acceder a los ajustes de la protección residente haciendo clic con el botón izquierdo del ratón en la bola azul “a” que puede encontrar en la esquina inferior derecha de la pantalla de su ordenador, o haciendo clic con el botón derecho del ratón y seleccionando “Control de la protección por acceso”.

Se presentará la siguiente ventana:



En esta ventana usted puede suspender temporalmente la protección residente haciendo clic en “Pausar”, o “Terminar”. Aquí, ambas opciones tienen el mismo efecto. Sin embargo, la protección residente se reactivará automáticamente la próxima vez que reinicie su ordenador. Esto es simplemente una precaución para asegurarse de que su ordenador no se quede accidentalmente desprotegido.

También puede ajustar la sensibilidad de la protección residente haciendo clic en la línea a cualquier lado del cursor para cambiar la sensibilidad de “Normal” a “Alto”. Sin embargo, la protección residente actualmente está comprendida por varios módulos diferentes o “proveedores”, cada uno de los cuales está diseñado para proteger una parte distinta de su ordenador – véase página siguiente. Cualquier cambio que haga en esta pantalla se aplicará a todos los módulos de la protección residente al mismo tiempo.

La protección residente está constituida por los siguientes módulos o “proveedores”:

Mensajería Instantánea revisa los ficheros descargados por la mensajería instantánea o programas “chat” tales como ICQ y MSN Messenger y muchos otros. Mientras que los mensajes instantáneos en sí mismos no suponen ningún riesgo serio de seguridad en cuanto a virus se refiere, las aplicaciones IM de hoy en día están muy lejos de ser simples herramientas de “chateo”: la mayoría de ellas también permiten el intercambio de ficheros – lo cual puede muy fácilmente llevar a infecciones de virus si no ha sido adecuadamente monitorizado.

Correo de Internet revisa los mensajes de e-mail entrantes y salientes procesados por otros clientes además de MS Outlook y MS Exchange, tales como Outlook Express, Eudora etc.

Escudo de Red provee protección contra gusanos de internet worms tales como Blaster, Sasser etc. Esto solo está disponible en sistemas NT (Windows NT/2000/XP/Vista).

Outlook/Exchange revisa mensajes de e-mail salientes y entrantes procesados MS Outlook o MS Exchange y detendrá cualquier mensaje que contenga un virus potencial, para ser aceptado o enviado.

Protección P2P revisa los ficheros descargados a través de programas P2P comunes (intercambio de ficheros) tales como Kazaa etc.

Bloqueo de Scripts revisa los scripts en cualquier página web que usted visite para prevenir cualquier infección que pudiera ser causada por cualquier vulnerabilidad de su navegador web.

Protección Estándar revisa los programas que se están ejecutando y los documentos que están abiertos. Previene que cualquier programa infectado se inicie o que cualquier documento infectado se abra, de modo que previene que cualquier virus se active y cause daño alguno.

Protección Web protege su ordenador de virus mientras esté utilizando internet (buscar, descargar ficheros etc) y también puede bloquear el acceso a ciertas páginas web. Si usted descarga un fichero infectado, la Protección Estándar evitará que se inicie y cause cualquier daño. Sin embargo, la Protección Web detectará el virus antes – durante la descarga del fichero, proveyendo una protección aún más fuerte. La Protección Web es compatible con la mayoría de los navegadores web, incluyendo Microsoft Internet Explorer, FireFox, Mozilla y Opera. Gracias a una característica única denominada "Intelligent Stream Scanning" que permite escanear los ficheros descargados casi en tiempo real, su impacto en la velocidad de búsqueda es prácticamente inapreciable.

Se puede ajustar la sensibilidad de cada módulo por separado. Para ajustar la sensibilidad para módulo por individual, o para detener o terminar un módulo, haga clic en “Detalles...”. La ventana se mostrará de la siguiente forma:



En la columna desplegada, los módulos individuales se muestran en el panel de la izquierda hacia abajo. La sensibilidad de cada módulo se puede ajustar haciendo clic en el módulo pertinente en la parte izquierda, a continuación haciendo clic en la línea hacia la izquierda o derecha de la línea deslizante. En esta casilla también es posible suspender las partes individuales de la protección residente, tanto temporal como permanentemente, haciendo clic en “Pausar” o “Terminar”. Si hace clic en “Pausar”, el módulo pertinente se reactivará automáticamente la próxima vez que reinicie su ordenador. Si selecciona “Terminar”, el programa le preguntará si desea que ese módulo en especial siga apagado indefinidamente, o si debería reanudarse después de que el ordenador se reinicie de nuevo - véase [página 92](#). Si hace clic en “Sí”, ese módulo en especial permanecerá desactivado, incluso después de reiniciar su ordenador, hasta que usted lo active manualmente de nuevo.

Hay un rango de opciones adicionales que pueden ser seleccionadas para cada módulo, por ejemplo, es posible especificar los tipos de ficheros que deberían ser escaneados. Se puede acceder a estas opciones adicionales haciendo clic en “Personalizar”, las cuales están descritas en la [página 74](#) – ajustes de la Protección Residente.

Cómo ejecutar un escaneo de virus manual – la Interfaz Simple de Usuario

Al ejecutar el programa por primera vez, le aparecerá la imagen de un reproductor de radio/CD plateado/gris que contiene todos los controles de definición, ejecución y procesamiento de los resultados de un escaneo de virus – véase más abajo. Esta es la carátula o “skin” por defecto del programa (se puede modificar seleccionando otras “carátula” – véase [página 31](#)).

Inicialmente, el reproductor aparece detrás de una casilla que contiene los “5 puntos clave para empezar”. Haga clic en “Más información” para leer más, después “Página de inicio” para volver a la ventana principal. La información relevante se resume en las páginas siguientes. Puede volver a dichos puntos clave de nuevo en cualquier momento sólo con acceder a las [opciones del menú](#) (véase siguiente página) y seleccionando “Ayuda Introductoria”.



En la parte central del reproductor, ligeramente hacia la derecha, hay una ventana que muestra información sobre el estado actual:

- [Base de datos de virus actual](#) – la base de datos de virus contiene detalles de todos los virus conocidos actualmente y es utilizada por el programa para identificar cualquier fichero sospechoso.
- [Protección residente](#) – aquí puede ver el nivel de sensibilidad actual.
- *Fecha del ultimo escaneo* – fecha en la cual se ejecutó un escaneo manual por última vez
- *Fecha BDRV* – contiene detalles de los ficheros instalados en su ordenador y se utiliza para repararlos si hubieran sido dañados por un virus. La fecha mostrada es la fecha en la que la base de datos de recuperación de virus fue actualizada por última vez.
- *Actualizaciones automáticas* – muestra el estado de actualización tanto de la base de datos de virus como del programa – para modificar el estado de la actualización, haga clic en el estado actual en la parte derecha de la ventana – véase [página 38](#).

A ambos lados de la pantalla se pueden ver tres botones de control:

- **Superior izquierda** – este botón abrirá el [Baúl de virus](#). Para más información sobre cómo trabajar con ficheros en el baúl de virus, véase [página 49](#).
- **Centro izquierda** – Haciendo clic en este botón aparecerá una barra con un cursor para poder cambiar la sensibilidad de la Protección Residente. Haga clic en el cursor y muévalo hacia la izquierda o derecha para reducir o incrementar la sensibilidad. Nota – modificando el nivel de sensibilidad aquí afectará a todos los módulos de protección residente. Para ajustar los módulos individualmente, véase la [página 24](#)
- **Inferior izquierda** – haciendo clic en este botón o en el estado actual en la ventana, se actualizará la Base de Datos de Virus.

La Base de Datos de Virus también se puede actualizar haciendo clic con el botón derecho del ratón en el icono azul con la “i” en el medio, en la esquina inferior derecha de la pantalla de su ordenador y seleccionando una de las opciones para “Generar la VRDB”.

- **Los tres botones de la derecha** se utilizan para definir las áreas a ser escaneadas – cualquier combinación de discos duros locales, medios extraíbles (disquetes, CDs etc) y carpetas seleccionadas – véase página siguiente.
- **COMIENZO** – haga clic en este botón para empezar o reanudar el escaneo de las áreas seleccionadas. Este botón cambiará a **PAUSAR**.
- **PAUSAR** – haciendo clic en este botón se parará temporalmente el escaneo.
- **DETENER**. Haga clic en este botón para terminar el escaneo.

MENU – Haciendo clic en la flecha señalando hacia arriba en la esquina superior izquierda del reproductor, mostrará las **OPCIONES DEL MENÚ**. También se puede acceder a las opciones del menú haciendo clic con el botón derecho del ratón en cualquier parte del reproductor.

Cuando se utiliza el programa sin ninguna carátula o “skin” (véase [página 31](#)), se puede acceder a las opciones del menú haciendo clic en “Herramientas” o “Ajustes” en la parte superior de la ventana.

Se puede acceder a un menú de opciones sin necesidad de iniciar el programa, haciendo clic con el botón derecho del ratón en la bola azul “a” en la esquina inferior derecha de la pantalla de su ordenador.

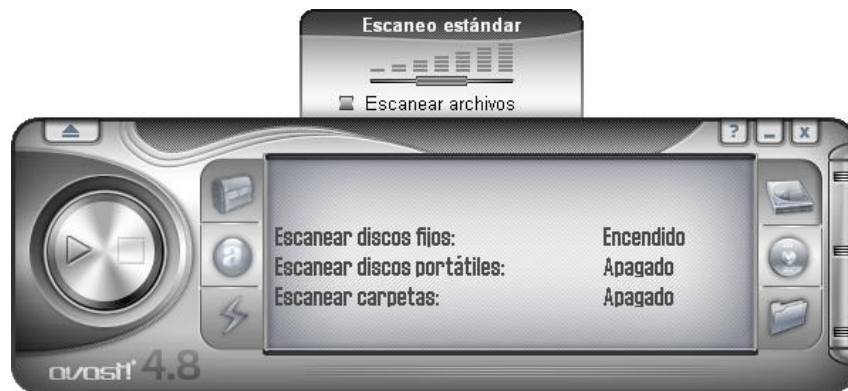
Todas las opciones del menú están descritas con más detalle en esta guía de usuario.

Seleccionar manualmente las áreas a ser escaneadas

Antes de iniciar el escaneo, debe elegir qué ficheros quiere escanear.

- ***Escanear discos locales***

Si usted simplemente quiere escanear todo en su ordenador (todos los ficheros en todos los discos duros), haga clic en el botón superior derecho. La ventana con el estado de información ahora será reemplazado por una nueva ventana – véase más abajo. Para volver al estado de información, haga clic con el botón derecho en el reproductor y seleccione “Información de estado”.



En la ventana, ahora verá la línea “Escanear discos fijos” y el estado ha cambiado de “Apagado” o “Encendido”.

También verá que aparece otra casilla encima del reproductor. Se puede utilizar para ajustar la sensibilidad del escaneo. Haciendo clic en el deslizante y manteniendo el botón del ratón presionado, puede mover el deslizante hacia la izquierda para reducir la sensibilidad, o hacia la derecha, para aumentar la sensibilidad. En esta casilla, también puede seleccionar si quiere archivar ficheros para ser escaneados. Estas opciones están descritas con más detalle en la sección siguiente.

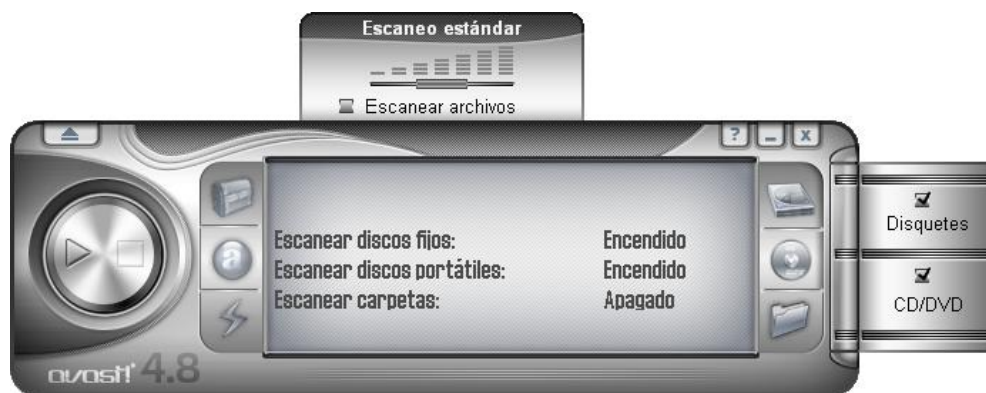
- ***Escanear discos portátiles***

Si desea escanear el contenido de algunos medios extraíbles, e.g. disquetes o CD/DVDs, haga clic en el botón del centro derecha.

Haciendo clic en este botón cambiará el estado de “Escanear medios extraíbles” de “Apagado” a “Encendido”.

También aparecerán dos casillas en la parte derecha del reproductor que pueden ser seleccionadas o no para indicar el tipo de medio extraíble que debería ser escaneado (algunos medios magnéticos y óptico-magnéticos, tales como discos ZIP, también cuentan como disquetes).

La casilla encima del reproductor también será mostrada, donde puede especificar la sensibilidad del escaneo y si los ficheros comprimidos también deberían ser escaneados.



- ***Escanear carpetas***

La última opción es el botón situado en la parte inferior derecha. Debería hacer clic en este botón si desea marcar que sólo ciertas carpetas sean escaneadas. Después de hacer clic en este botón, aparecerá una lista de carpetas en su ordenador de la cual usted deberá seleccionar las carpetas que quiere que sean escaneadas. Este ajuste, por consiguiente, ofrece la máxima flexibilidad, pero requiere que el usuario ajuste exactamente qué debería ser escaneado.

Usted puede ajustar la sensibilidad del escaneo y especificar si los ficheros comprimidos también deberían ser escaneados de la misma forma que para las demás áreas.

Se puede combinar más de un tipo de escaneo, por ejemplo se puede iniciar un escaneo de su disco duro y extraíbles haciendo clic tanto en el botón de discos duros locales como en el botón de medios extraíbles.

Ajuste de la sensibilidad y ejecución del escaneo

Al definir las áreas a ser escaneadas, también puede ajustar la sensibilidad del escaneo y si el programa debería escanear el contenido de los ficheros comprimidos i.e. ficheros con nombres que acaban en .zip, .rar, ace, .acj etc. Para incluir dichos ficheros, primero seleccione las áreas que quiere escanear (véase más arriba) y después haga clic en el recuadro de “escanear ficheros comprimidos” que aparece encima del reproductor. La sensibilidad del escaneo determina cuán minucioso será dicho escaneo. La sensibilidad se ajusta moviendo el deslizante hacia la izquierda o derecha. Usted puede elegir entre tres niveles predefinidos.

- **Escaneo Rápido.** Este escaneo, según indica su propio nombre, es bastante rápido pues los ficheros se examinan según sus nombres de fichero, y se escanean sólo aquellos ficheros considerados potencialmente peligrosos. Este tipo de escaneo a veces puede dar lugar a que no se detecten algunos virus en ciertos ficheros, sin embargo suele ser suficiente.
- **Escaneo Normal.** En este tipo de escaneo, los ficheros se analizan según su contenido (no según el nombre como en el Escaneo Rápido). Sin embargo, sólo se analizan las partes "peligrosas" de los ficheros, no los ficheros en su totalidad. Este tipo de escaneo también puede dar lugar a que no se detecte algún virus, sin embargo es mucho más efectivo que el Escaneo Rápido.
- **Escaneo Minucioso.** Este tipo de escaneo todos los ficheros son escaneados en su totalidad, y analiza todas las infecciones enumeradas en la base de datos. Este tipo de escaneo ofrece fiabilidad máxima, pero lleva mucho más tiempo de ejecución que el Escaneo Rápido o Escaneo Normal.

Después de haber seleccionado las opciones de escaneo, lo único que tiene que hacer es empezar el test. Para ello, haga clic en el botón Comenzar (flecha señalando hacia la derecha) en la parte izquierda del reproductor.

Método Alternativo

También puede definir las áreas a ser escaneadas abriendo las [opciones del menú](#) y haciendo clic en “Comenzar escaneo” y después “Seleccionar área de escaneo”. Una vez haya seleccionado el áreas a escanear, también puede especificar si los archivos comprimidos deberían ser incluidos seleccionando “Escanear archivos comprimidos”.

Haciendo clic en “Seleccionar la intensidad del escaneo” también puede especificar si el escaneo debería ser un Escaneo Rápido, Escaneo Normal, o Escaneo Minucioso según se describe más arriba.

Ejecución del escaneo y procesamiento del resultado

Después de hacer clic en el botón Comenzar, o seleccionando “Comenzar escaneo” en las [opciones del menú](#), el programa comienza a escanear las áreas seleccionadas. Este proceso puede llevar bastante tiempo, dependiendo del número y tamaño de los ficheros analizados y la velocidad de su ordenador. Tenga en cuenta que, aunque el Escaneo Minucioso sea el que más tiempo lleva, es el más efectivo.

Una vez se haya iniciado el programa, puede trabajar con otros ficheros o programas en su ordenador aunque el escaneo esté en proceso. Para ello, se recomienda minimizar el programa avast! para que se ejecute en un segundo plano. Si no, podría ver que su ordenador empieza a ser muy lento (el escaneo de virus es una tarea bastante exigente). Para enviar el escaneo al segundo plano, sólo tiene que hacer clic en el botón de minimizar (_) en la esquina superior derecha del reproductor mientras el escaneo se está ejecutando y desaparecerá de la ventana. Para traerlo de vuelta, simplemente haga clic en la casilla de “avast!” que encontrará en la barra horizontal en la parte inferior de la ventana.

Cuando el escaneo haya finalizado, y so no se detectaron ningunos virus durante el escaneo, la ventana del reproductor mostrará la información básica del escaneo, tal como el número de archivos y carpetas escaneadas, el tiempo del escaneo etc.

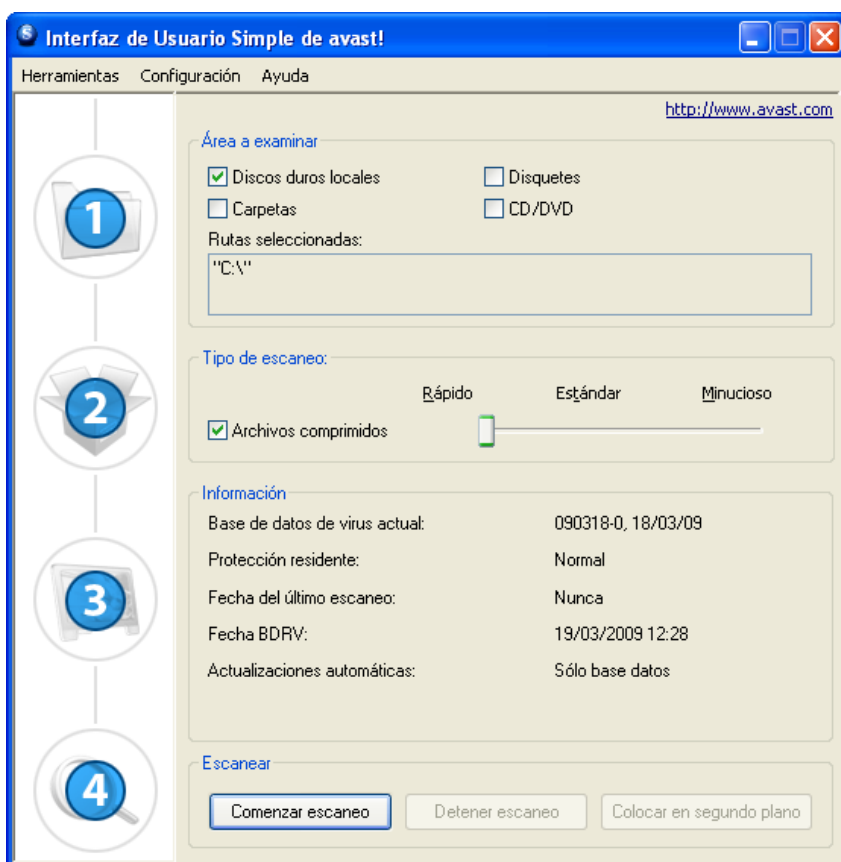


En el caso de que se hubieran encontrado algunos virus, el programa le preguntará qué hacer con los ficheros infectados. Hay varias opciones, e.g. mover el fichero al [Baúl de Virus](#), borrarlo, renombrarlo o moverlo, o, si es posible, incluso repararlo. También puede simplemente mantenerlo intacto, sin embargo, esta opción puede resultar en la propagación del virus y causar algún daño. Estas opciones están descritas con más detalle en la sección [“Qué hacer si se encuentra un virus”](#).

Cambiar la apariencia de la Interfaz Simple de Usuario

Si está utilizando la interfaz de usuario simple, se pueden seleccionar diferentes carátulas del programa. Se ofrecen tres carátulas (skins) estándar distintas, y otras se pueden descargar de Internet si se deseara – haga clic con el botón derecho del ratón en el reproductor avast! y de las [opciones del menú](#), haga clic en “Seleccionar carátula” y después en el vínculo “Obtén más carátulas...”. Alternativamente, si desea utilizar el programa sin ninguna carátula, seleccione “Configuración” en el menú de opciones, después desactive la casilla “Habilitar skins para la Interfaz Simple de Usuario”. La próxima vez que inicie el programa, las opciones aparecerán en su formato básico. Para reactivar la carátula, haga clic en “Configuración”, a continuación haga clic de nuevo en “Configuración”, y finalmente vuelva a marcar la casilla “Habilitar skins para la Interfaz Simple de Usuario”. La carátula se restaurará la próxima vez que inicie el programa.

Apariencia de la interfaz simple de usuario sin ninguna carátula:



Las áreas a ser escaneadas y el tipo de escaneo se ajustan posteriormente seleccionando las casillas correspondientes. Si desea escanear sólo carpetas específicas, al seleccionar la casilla “Carpetas” se abrirá una nueva ventana enumerando todas las carpetas de su ordenador. Para seleccionar una carpeta, solamente tiene que marcar la casilla correspondiente y aparecerá la casilla “Rutas seleccionadas” encima.

Puede ajustar la sensibilidad del escaneo moviendo el deslizador a la posición requerida y si quisiera incluir archivos comprimidos en el escaneo, haga clic en “Archivos comprimidos”.

Después de haber iniciado la ejecución del escaneo, puede continuar utilizando su ordenador para otras tareas haciendo clic en “Colocar en segundo plano”.

También puede ajustar la sensibilidad de la protección residente haciendo clic en “Configuración” y después en “Protección Residente”. Puede utilizar el deslizador para modificar la sensibilidad a “Estándar” o “Alta”, o puede apagar la protección residente completamente haciendo clic en la línea bajo “Apagar”. Sin embargo, según se ha mencionado previamente, cualquier cambio que haga aquí se aplicará igualmente a todos los módulos de la protección residente. Para ajustar la sensibilidad de los módulos individualmente, véase [página 24](#).

Puede acceder a otras funciones tales como el Baúl de Virus y la Base de Datos de Virus haciendo clic en “Herramientas” y seleccionando la opción requerida en la lista de opciones disponibles. Estas, y todas las demás funciones, se encuentran descritas con más detalle en esta guía de usuario posteriormente.

El estado de información actual se presenta en segunda mitad de la ventana y está descrito en la sección anterior.

Qué hacer si se encuentra un virus

Si el programa detecta un fichero sospechoso, el escaneo se interrumpirá en ese momento y aparecerá la siguiente ventana preguntándole cómo desea actuar:

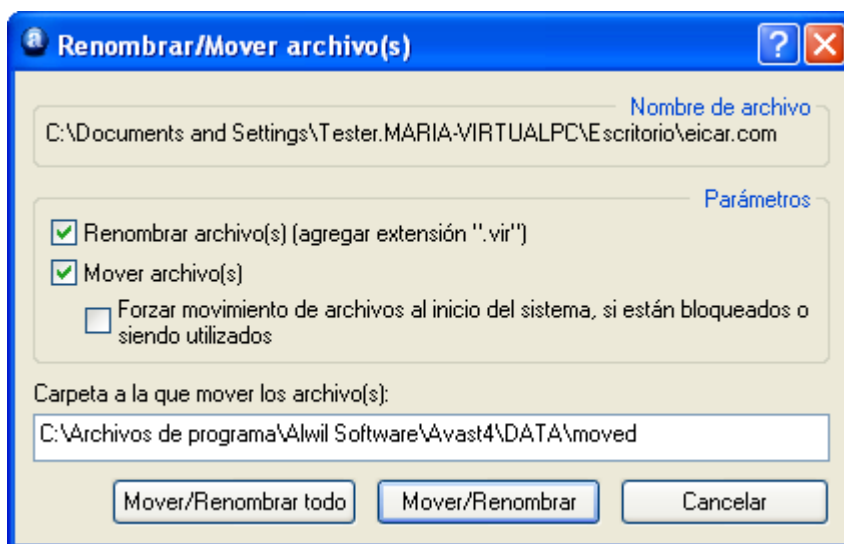


Si hace clic en “Continuar” no se llevará a cabo ninguna acción en relación al fichero identificado y aparecerá al final del escaneo en la lista de los resultados del escaneo – véase [página 37](#). Haciendo clic en “Detener” terminará el escaneo en ese mismo momento.

Si se detecta un virus por uno de los módulos de protección residente e.g. al intentar abrir un fichero infectado, o por el salvapantallas, la ventana será un poco diferente – los botones de “Continuar” y “Detener” serán reemplazados por uno solo “No hacer nada”. Si hace clic en ese botón para que no se lleve a cabo ninguna acción en ese momento, el fichero infectado permanecerá donde está pero el virus no se activará.

Alternativamente, si desea llevar a cabo alguna acción ahora, hay cuatro posibles opciones.

Opción 1: Mover el fichero afectado a otra carpeta en su ordenador. En el mismo momento, tendrá la oportunidad de renombrarlo. Haciendo clic en “Mover/Renombrar” aparecerá la siguiente ventana mostrando la casilla “Renombrar archivos” ya seleccionada.



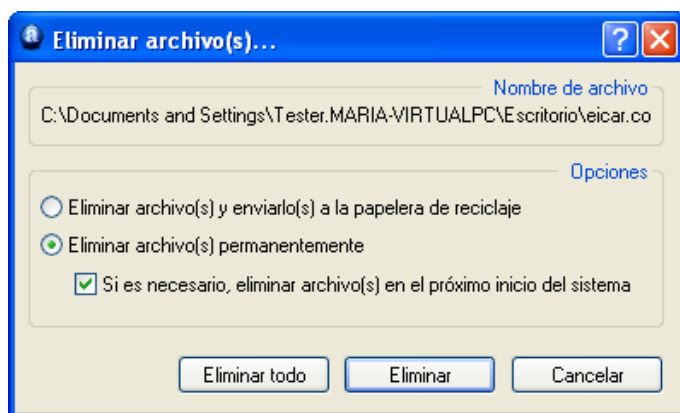
En la parte blanca de la pantalla, se puede especificar adónde quiere mover el fichero sospechoso. El programa selecciona automáticamente una carpeta de destino apropiada, o usted puede especificar una diferente.

Si también elige la opción “Renombrar fichero(s)...”, se añadirá la extensión “.vir” al final del nombre del fichero para identificarlo como un fichero potencialmente peligroso con lo cual usted no lo ejecutará accidentalmente, infectando su ordenador y causando daños.

Si no fuera posible mover el fichero en este momento e.g. debido a que esté siendo utilizado por otro programa, seleccionando la casilla “Forzar movimiento de archivos al inicio del sistema, si están bloqueados o siendo utilizados” el fichero se moverá automáticamente al destino seleccionado la próxima vez que se reinicie el ordenador.

Nota – en el caso de que se infecte un **fichero del sistema** i.e. un fichero que se utiliza para ejecutar un programa clave, al mover el fichero podría salir un mensaje de error la próxima vez que el ordenador intente ejecutar el programa. Sin embargo, si se mueve el fichero al Baúl de Virus, permanecerá en un área protegida de cuarentena donde no puede causar ningún daño a los demás ficheros y donde posiblemente podrá ser reparado antes de moverlo a su ubicación original – véase [página 8](#)

Opción 2: Borrar el fichero – haciendo clic en “Eliminar” aparecerá la siguiente ventana:



Dependiendo de la versión de Windows que esté utilizando, hay dos formas de eliminar el fichero.

- ***Eliminar archivo(s) y enviarlo(s) a la papelera de reciclaje***

Esto moverá el fichero(s) a la papelera de reciclaje pero no los borrará permanentemente. Por lo tanto, pueden ser recuperados después. Esta opción puede no estar disponible en algunas versiones de Windows.

- ***Eliminar archivos(s) permanentemente***

Esto eliminará el archivo(s) de su ordenador permanentemente sin ninguna posibilidad de recuperarlos posteriormente. Sin embargo, esto sólo borrará el fichero infectado. Algunos virus instalan ficheros nuevos en su ordenador y si esos ficheros no contienen virus, no serán detectados como sospechosos. Mientras dichos ficheros estén ocupando espacio en su ordenador, no deberían presentar ningún riesgo de seguridad.

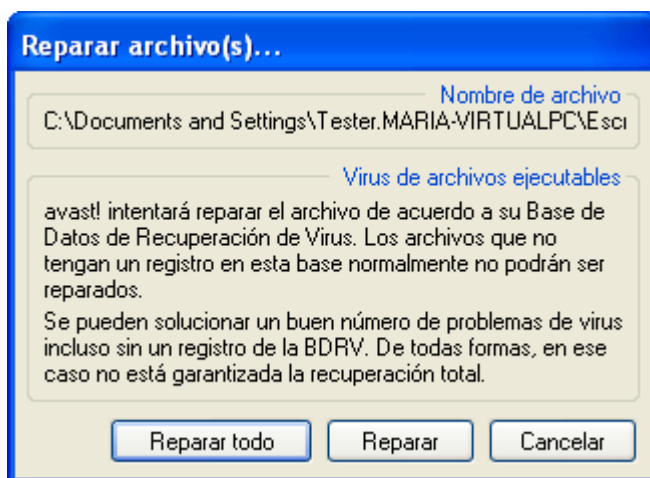
Si se detecta un virus que puede ser completamente eliminado por el limpiador de virus integrado, incluyendo la eliminación de nuevos ficheros creados por el virus, aparecerá un botón adicional – ***“Eliminar el virus del sistema completamente”*** – en la casilla de aviso de virus. Si esta opción está disponible, se recomienda utilizarla.

Si no es posible borrar el fichero en este momento e.g. debido a que esté siendo utilizado por otro programa, marcando la casilla “Si es necesario, borrar el archivo(s) en el próximo reinicio del sistema” se borrará el fichero automáticamente la próxima vez que se reinicie el ordenador. A continuación haga clic de nuevo en “Eliminar” para confirmar.

Nota – en el caso de que se infecte un ***fichero del sistema*** i.e. un fichero que se utiliza para ejecutar un programa clave, al borrar el fichero podría salir un mensaje de error la próxima vez que el ordenador intente ejecutar el programa. Por lo tanto, antes de borrar el fichero debería estar bastante seguro de que el fichero infectado no es un fichero del sistema, o de que puede reemplazarlo con un fichero limpio e.g. de un backup o copia de seguridad. Si no está seguro, se recomienda mover el fichero al Baúl de Virus. Aquí estará en un área protegida de cuarentena donde no puede causar ningún daño a los demás ficheros y donde posiblemente podrá ser reparado antes de moverlo a su ubicación original – véase [página 8](#)

Opción 3: Reparar el archivo.

Haciendo clic en “Reparar” aparecerá la siguiente ventana:



Si hace clic de nuevo en “Reparar”, el programa intentará restaurar el fichero infectado a su estado original.

Para poder reparar un fichero, el programa se remitirá a la **Base de datos de Recuperación de Virus**. Si hay información suficiente acerca del programa en la Base de Datos, hay bastantes posibilidades de que pueda ser reparado. Nota – sólo pueden ser reparados aquellos ficheros que han sido físicamente cambiados por un virus. Si han sido creados nuevos ficheros, permanecerán a menos que puedan ser eliminados por el limpiador de virus (virus cleaner) – véase Opción 2.

Si no hay información en la Base de Datos podría ser posible la reparación, pero la recuperación completa será menos factible. Con lo cual es muy importante que la Base de Datos sea continuamente actualizada – para actualizar la Base de Datos de Recuperación de Virus, haga clic con el botón derecho del ratón en la bola azul con la “i” en el medio, la cual puede encontrar en la esquina inferior derecha de la pantalla de su ordenador y seleccione una de las opciones para “Generar la VRDB” . La Base de Datos se actualizará con detalles de cualquier programa nuevo instalado en su ordenador desde la última actualización.

Opción 4: La **OPCIÓN RECOMENDADA** es mover el fichero al [Baúl de Virus](#).

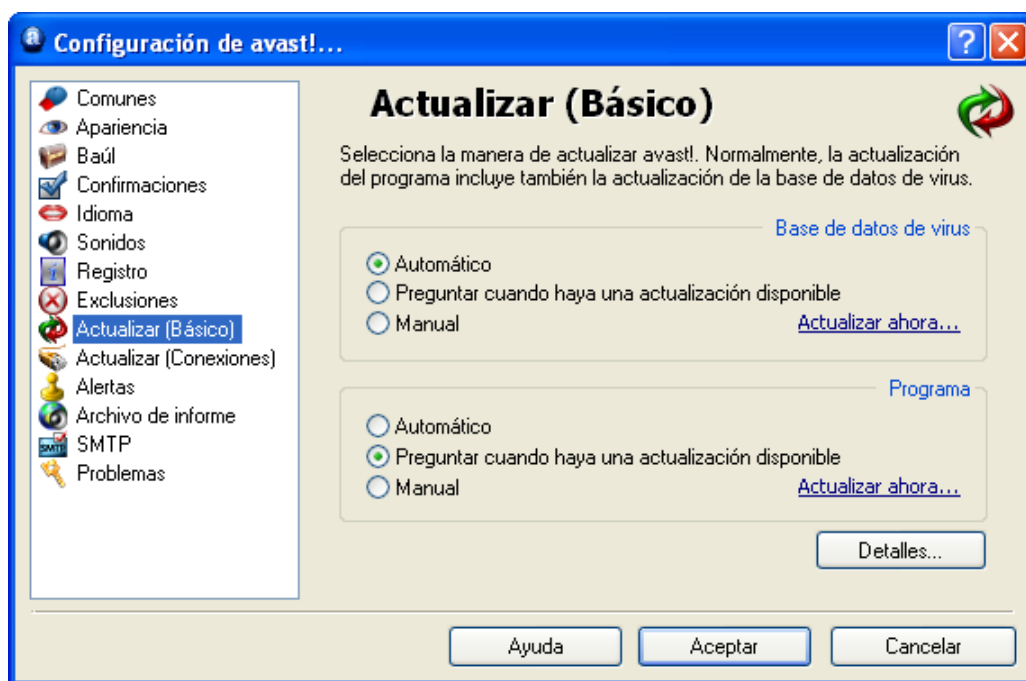
Nota – en el caso de que se infecte un **fichero del sistema** i.e. un fichero que se utiliza para ejecutar un programa clave, al mover el fichero podría salir un mensaje de error la próxima vez que el ordenador intente ejecutar el programa. Sin embargo, si se mueve el fichero al Baúl de Virus, permanecerá en un área protegida de cuarentena donde no puede causar ningún daño a los demás ficheros y donde posiblemente podrá ser reparado antes de moverlo a su ubicación original – véase [página 8](#)

Funciones avanzadas

Ajustar actualizaciones automáticas

Cualquier programa antivirus es bueno según su base de datos de definiciones de virus conocidos, por lo cual es importante actualizar regularmente tanto el programa como la base de datos de virus.

Usted puede seleccionar que tanto el programa como la base de datos de virus se actualicen automática o manualmente, o solamente seguir el aviso de que hay una actualización disponible de avast! Para cambiar el estado, también puede hacer clic en el estado actual (e.g. “Sólo base de datos”) en la ventana del reproductor de avast, o simplemente abrir las [opciones del menú](#) (véase [página 26](#)), seleccione “Configuración del programa”, después “Actualizar (Básico)”. A continuación sólo tiene que hacer clic en el estado deseado para la base de datos de virus y del programa (véase abajo).



Haga clic en “Aceptar” y el estado en la ventana se actualizará según se indica a continuación:

- **ENCENDIDO** si se selecciona “Automático” tanto para la base de datos de virus como para el programa
- **SOLO PROGRAMA** si se selecciona “Automático” sólo para el programa
- **SOLO BASE DE DATOS** si se selecciona “Automático” sólo para la base de datos de virus
- **APAGADO** si no se selecciona “Automático” ni para el program ni para la base de datos de virus

Para actualizar **manualmente** tanto el programa como la base de datos de virus, vaya a las [opciones del menú](#) (véase [página 26](#)) y seleccione la opción “Actualizar”.

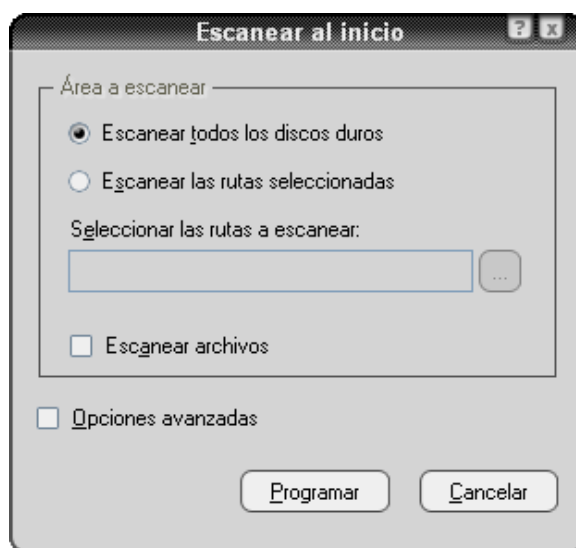
- Para actualizar la base de datos de virus, seleccione **Actualizar la base de datos**
- Para actualizar el programa avast!, seleccione **Actualizar el programa**

Cómo programar un escaneo al inicio

(Sólo para versiones 32 bit de Windows NT/2000/XP/Vista)

Se puede programar un escaneo automático al reiniciarse el ordenador, i.e. cuando se “carga” antes de que el sistema operativo actual esté activo. Esto es útil si usted sospecha que un virus ha podido instalarse en su ordenador, con lo que detectará el virus antes de que se active y antes de que tenga oportunidad de causar cualquier daño.

Para programar un escaneo al inicio, vaya a las [opciones del menú](#) (véase [página 26](#)) y haga clic en “Escaneo programado para el inicio”. Aparecerá la siguiente ventana:



Aquí puede seleccionar si desea escanear todos los discos o solamente áreas seleccionadas. Para escanear sólo las áreas seleccionadas, haga clic en “Escanear las rutas seleccionadas” y escriba el nombre de la ruta en el espacio en blanco o haga clic en la casilla cuadrada a su derecha para buscar el área que desea escanear. Cuando encuentre el área que desea escanear, haga clic en la misma y el nombre de la ruta se copiará automáticamente en la casilla proveída.

Si desea incluir ficheros comprimidos, marque la casilla “Escanear archivos”.

Marcando la casilla “Opciones avanzadas”, puede especificar qué se debería hacer con los ficheros infectados. Puede elegir de cualquiera de las siguientes opciones:

- Eliminar el archivo infectado
- Mover el archivo infectado
- Mover el archivo infectado al Baúl
- Ignorar el archivo infectado
- Reparar el archivo infectado

Al seleccionar “Mover el archivo infectado”, cualquier fichero sospechoso se moverá a la carpeta C:/Program Files\Alwil Software\Avast4\DATA\moved. La extensión “.vir” también será añadida al final del nombre de fichero para identificarlo como un fichero sospechoso, de modo que usted no lo ejecute accidentalmente, infectando su ordenador y causando daño a sus ficheros.

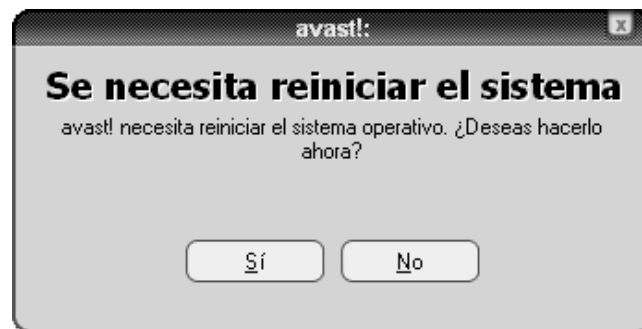
Si usted elige las opciones Eliminar o Mover ficheros infectados, se le pedirá que confirme qué quiere hacer con cualquier **fichero del sistema** infectado.

Los ficheros del sistema son ficheros que utiliza su ordenador para ejecutar sus programas y borrar o mover los mismos podría tener serias consecuencias. Por consiguiente, se le pedirá que confirme si desea:

- Permitir borrar o mover, o
- Ignorar borrar o mover ficheros del sistema

Seleccionado “Ignorar borrar o mover” prevendrá cualquier problema potencial, sin embargo, su ordenador aún tendrá riesgo de una infección potencial. La acción recomendada es mover todos los ficheros sospechosos al baúl de virus, donde posteriormente pueden ser tratados en un área protegida de cuarentena. Una vez movidos al baúl de virus, no pueden causar ningún daño a sus demás ficheros. Usted puede actuar con los ficheros infectados según se describe en la [página 49](#), e.g. se pueden borrar, si usted está seguro de que no hay peligro por hacer esto, se pueden mover de vuelta a su ubicación original, o simplemente se pueden almacenar hasta que usted decida qué hacer.

Una vez haya confirmado cómo se debería tratar cualquier fichero infectado, haga clic en “Programar” y aparecerá el siguiente mensaje:



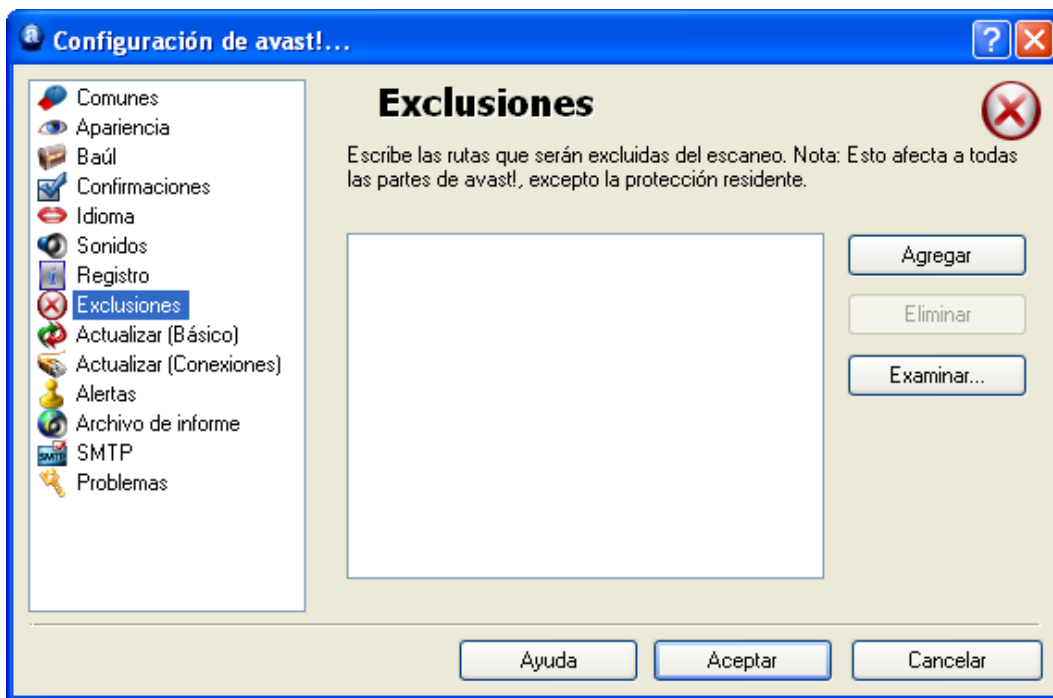
Haga clic en “Sí” para reiniciar su ordenador y ejecutar el escaneo al inicio ahora, o haga clic en “No” y el escaneo se llevará a cabo automáticamente la próxima vez que reinicie su ordenador.

Excluir ficheros del escaneo

Se pueden excluir algunas ubicaciones, o incluso ficheros individuales, de test, lo cual significa que no serán testados de virus durante ningún escaneo. Esto puede ser útil en varios casos:

- **Para evitar falsas alarmas.** Si el programa reporta una infección de virus en un fichero y usted está seguro de que es una falsa alarma, puede excluir el fichero para que no sea analizado y evitar más falsas alarmas. Por favor, informe a Alwil Software sobre cualquier fichero tal para que el problema pueda ser solucionado.
- **Para acelerar el proceso.** Si usted tiene una carpeta en su disco duro que contiene sólo imágenes, por ejemplo, puede excluirla del análisis añadiéndola a la lista de exclusiones, lo cual reducirá el tiempo invertido en el escaneo.

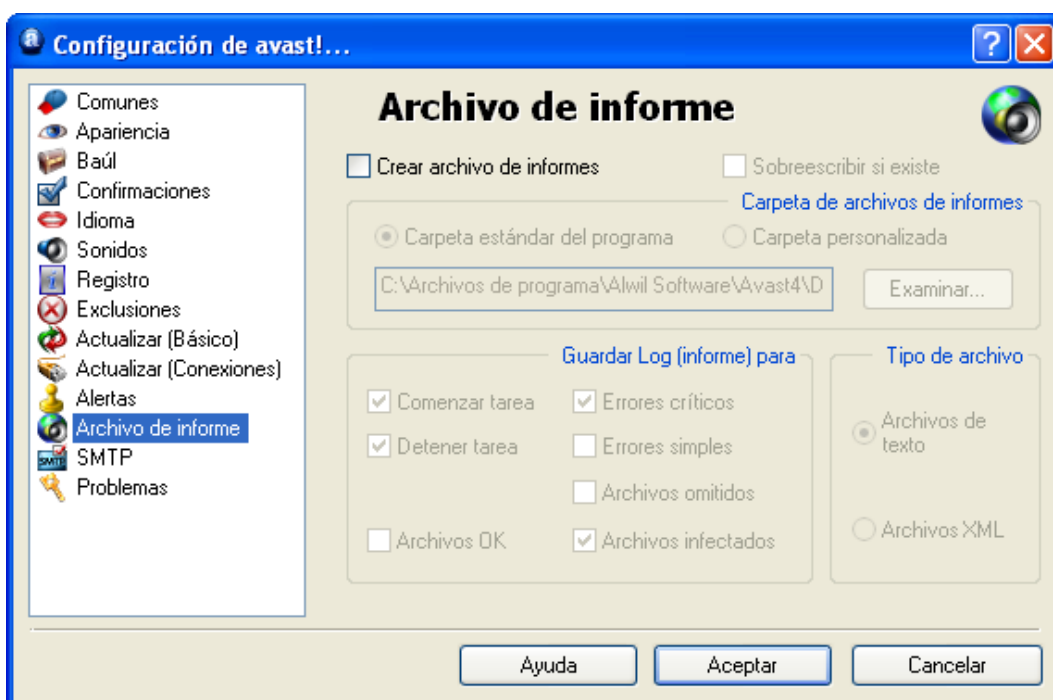
Tenga en cuenta que esas exclusiones afectarán a todos los escaneos futuros, excepto para la protección residente. Para excluir ciertos ficheros o carpetas de ser escaneados, simplemente haga clic en **“Configuración del programa” en el menú de opciones** (véase [página 25](#)), luego en “Exclusiones” y aparecerá la siguiente ventana:



Para excluir una carpeta o fichero, haga clic en “Examinar” y después marque la carpeta o fichero a ser excluido. Alternativamente, haga clic en “Agregar” y escriba manualmente la localización de la carpeta o fichero pertinente en la caja de Exclusiones. Si desea excluir una carpeta, incluyendo todas las subcarpetas, es necesario añadir “*” al final del nombre de la carpeta e.g. C:\Windows*. Para eliminar una carpeta o fichero de la lista de exclusiones, haga clic en la misma una vez para seleccionarla, y a continuación haga clic en “Eliminar”

Cómo crear un archivo de informe de los resultados del escaneo

Puede crear un archivo de informe permanente de los resultados de cada escaneo creando un registro que pueda visualizar posteriormente. Para crear un archivo de informe, primero acceda a las [opciones del menú](#) según se describe en la [página 26](#) y seleccione “Configuración”. Después haga clic en “Archivo de informe” y en la ventana siguiente, marque la casilla “Crear archivo de informes” según se muestra más abajo.



Si usted quisiera crear un nuevo archivo después de cada escaneo y no quiere mantener un registro de todos los resultados de previos escaneos, marque la casilla “Sobreescribir si existe”. Si no se marca esta casilla, los resultados de cada escaneo se añadirán al final del archivo de informe anterior.

También puede elegir dónde quiere guardar el archivo de informe – en la carpeta estándar del programa, la cual asigna automáticamente, o en una ubicación nueva que usted puede especificar haciendo clic en “Carpeta personalizada” e insertando la ubicación de la carpeta.

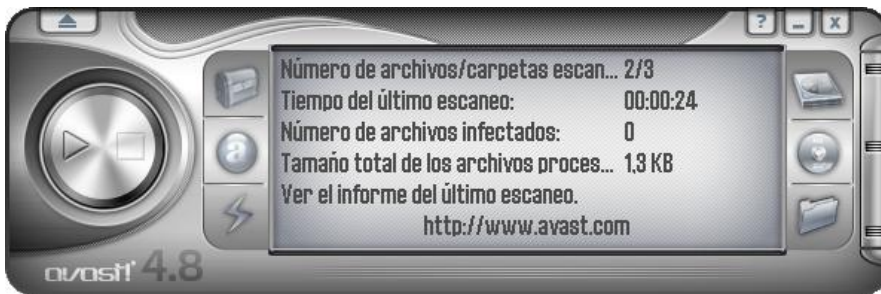
A continuación, usted puede especificar qué información será incluida en el archivo de informe:

- Comenzar tarea – fecha y hora en la que se inició el escaneo
- Detener tarea – fecha y hora en la que se completó el escaneo
- Archivos OK – ficheros que han sido escaneados sin haber detectado ninguno sospechoso. Si se escanean todos los discos locales, marcando esta casilla creará un reporte muy largo, probablemente de varios miles de líneas. Por tanto, se recomienda marcar esta casilla sólo cuando piense efectuar un escaneo limitado

y sólo si actualmente usted quiere que todos los ficheros limpios se registren como ficheros sin problemas.

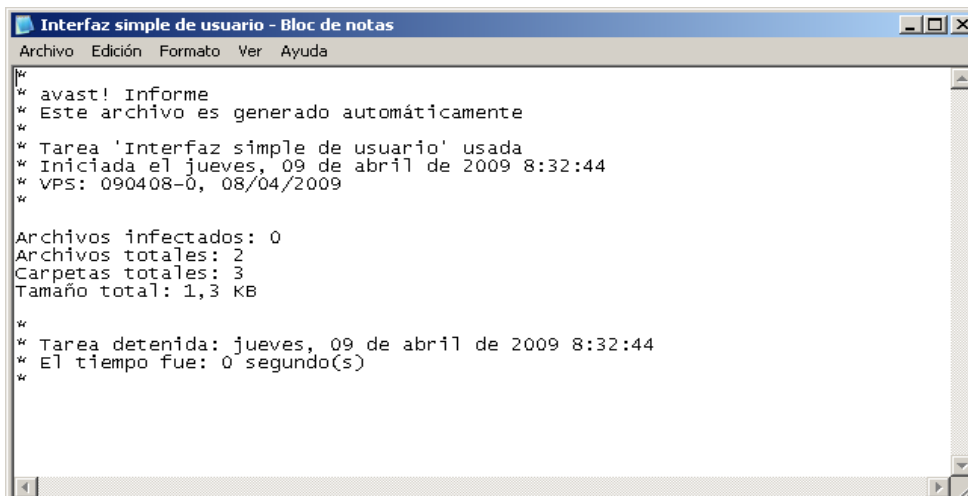
- Errores críticos: surgen cuando el programa detecta algo que no se esperaría normalmente. Estos son errores que generalmente requieren más investigación.
- Errores simples: son menos serios que los errores críticos y generalmente relacionados con ficheros que no han podido ser escaneados, pues estaban abiertos y en uso por otra aplicación.
- Archivos omitidos: son ficheros que no se escanean basándose en los ajustes del escaneo. Por ejemplo, en un escaneo rápido, los ficheros se escanean basándose en su extensión de fichero. Los ficheros con extensiones que no son consideradas peligrosas no se escanean. Cualquier fichero específicamente excluido del escaneo también se reportaría como fichero omitido.
- Archivos infectados: estos son ficheros que potencialmente contienen un virus.

Finalmente, puede especificar si el reporte debería figurar en la forma de fichero de texto o como un fichero XML. Después de ejecutar el escaneo, habrá una nueva línea en la ventana de información del estado – “Ver el informe del último escaneo” según se muestra más abajo.

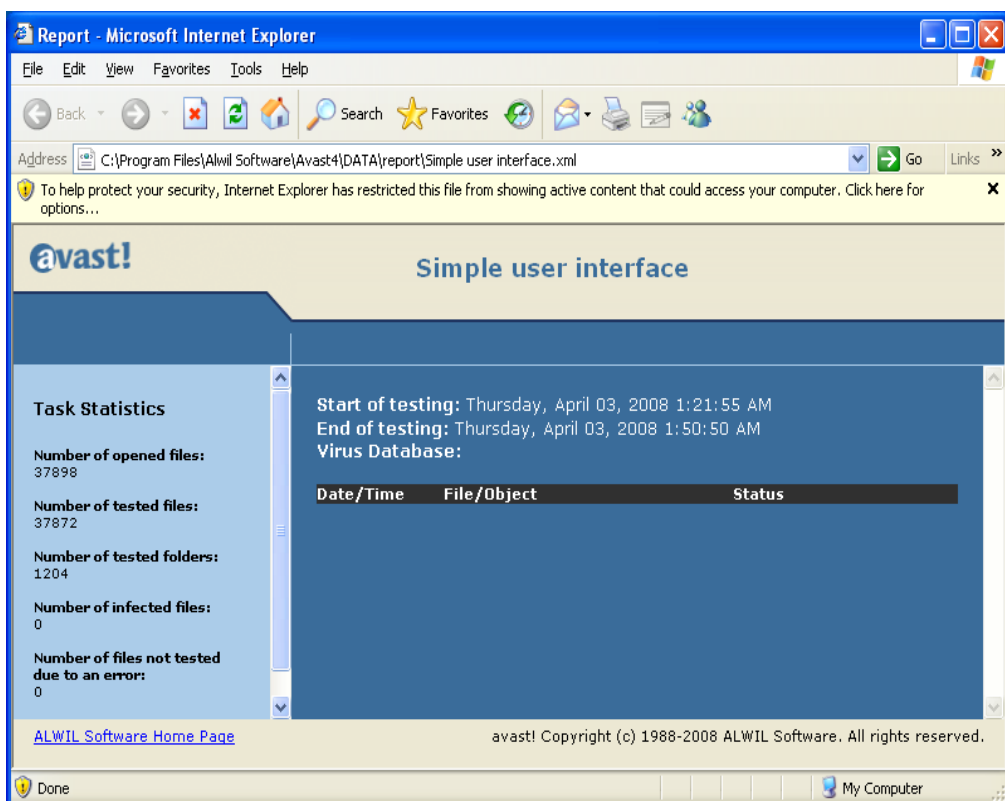


Haciendo clic en “Ver el informe del último escaneo” aparecerá el archivo de informe en el formato especificado. Alternativamente, abra las [opciones del menú](#) (véase [página 26](#)) y haga clic en “Ver informes de escaneo”

Informe en formato de texto:



Informe en formato XML



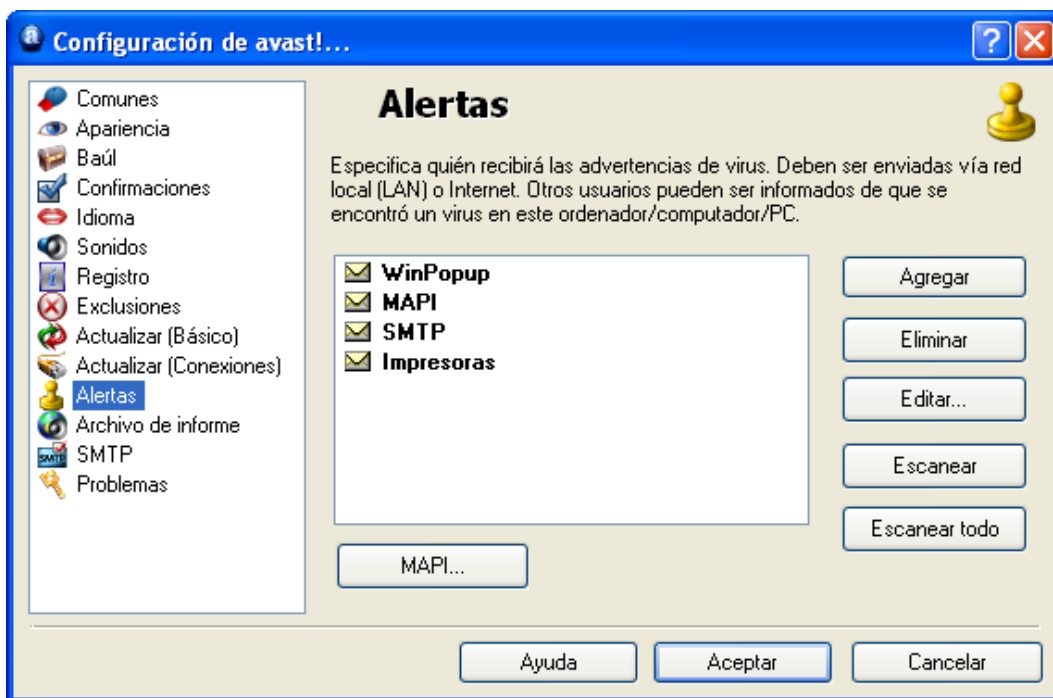
Los informes de previos escaneos se almacenan en la carpeta estándar del programa o en la carpeta personalizada del programa especificada al crear el informe – véase página anterior.

Si ha especificado Formato de texto sin haber marcado la casilla “Sobreescribir si existe”, también podrá ver los informes anteriores siempre que visualice el informe después de ejecutar un nuevo escaneo.

Si usted no quiere que se creen ninguno informes, simplemente vaya a “Archivo de informe” en las [opciones del menú](#) (véase [página 26](#)) y desmarque la casilla “Crear archivo de informe”.

Alertas

avast! puede enviar un mensaje de aviso sobre la aparición de virus. De las [opciones del menú](#), seleccione “Configuración” y después “Alertas”. Esta propiedad es útil para los administradores de red, que serán notificados sobre la presencia de un virus en cualquier ordenador de su red, con lo que pueden reaccionar rápidamente.



La alerta puede ser enviada en las siguientes formas:

- **WinPopup.**
Haga clic en “Agregar” y seleccione WinPopup. A continuación introduzca la dirección de IP o el nombre de la red del ordenador al cual enviar el aviso, o haga clic en “Examinar” y seleccione la dirección en la lista de opciones disponibles.
- **MAPI.**
La alerta se enviará en forma de e-mail, utilizando el protocolo MAPI. Introduzca la dirección a la que enviar el email, después haga clic en el botón MAPI en la parte inferior de la ventana, y a continuación inserte el nombre de perfil MAPI y la contraseña correspondiente.
- **SMTP.**
La alerta se enviará en forma de e-mail, utilizando el protocolo SMTP. Para crear una nueva alerta, haga clic en “Agregar” y después haga clic en SMTP. En la casilla que aparece, introduzca la dirección de email de la persona a la que se le debería enviar la alerta. También es necesario especificar algunos otros ajustes – véase la sección “SMTP” siguiente.

- **Impresoras.**
La alerta se enviará a la impresora especificada. Haga clic en “Agregar” y después en “Impresora”; a continuación haga clic en “Examinar” y seleccione la impresora de la lista de opciones disponibles.
- **ICQ.**
La alerta se enviará en forma de un mensaje ICQ. Introduzca el número de ICQ de la persona a la que se le debería enviar el aviso.
- **Windows Messenger.**
Introduzca la dirección de e-mail que utiliza el destinatario de la alerta para iniciar la sesión en el servicio Windows Messenger.

Para crear una nueva alerta, haga clic en “Agregar” y seleccione el tipo de alerta requerida, y después introduzca los detalles necesarios según se describe más arriba. Una vez se cree una alerta, se enviará un mensaje al destinatario definido en cualquier ocasión en la que se detecte un fichero sospechoso.

Para editar o borrar una alerta que ha sido creada, haga clic en la misma para seleccionarla, y después haga clic en “Editar” o “Eliminar”.

Haciendo clic en “Escanear” aparecerá un mensaje de análisis que se enviará a las direcciones seleccionadas, mientras que haciendo clic en “Escanear todo” enviará un mensaje de análisis a todos los destinatarios de la alerta de la lista.

SMTP

Haciendo clic en SMTP en la lista, en la parte izquierda de la pantalla, puede especificar los parámetros de su servidor SMTP. avast! utiliza esos ajustes para enviar mensajes de e-mail, especialmente al:

- Enviar mensajes de aviso (Alertas) cuando se ha encontrado un virus.
- Enviar ficheros desde el Baúl a ALWIL Software.
- Enviar informes avast! quebrados a ALWIL Software.

Usted debería insertar la siguiente información:

- Dirección del servidor – la dirección del servidor de correos salientes (e.g. smtp.server.com ó 192.168.1.25).
- Puerto – el número del puerto (por defecto es 25).
- Dirección del remitente - ("Remitente").

Si el servidor SMTP requiere autenticación al logearse, usted también debería marcar la casilla e introducir el nombre de usuario y la contraseña.

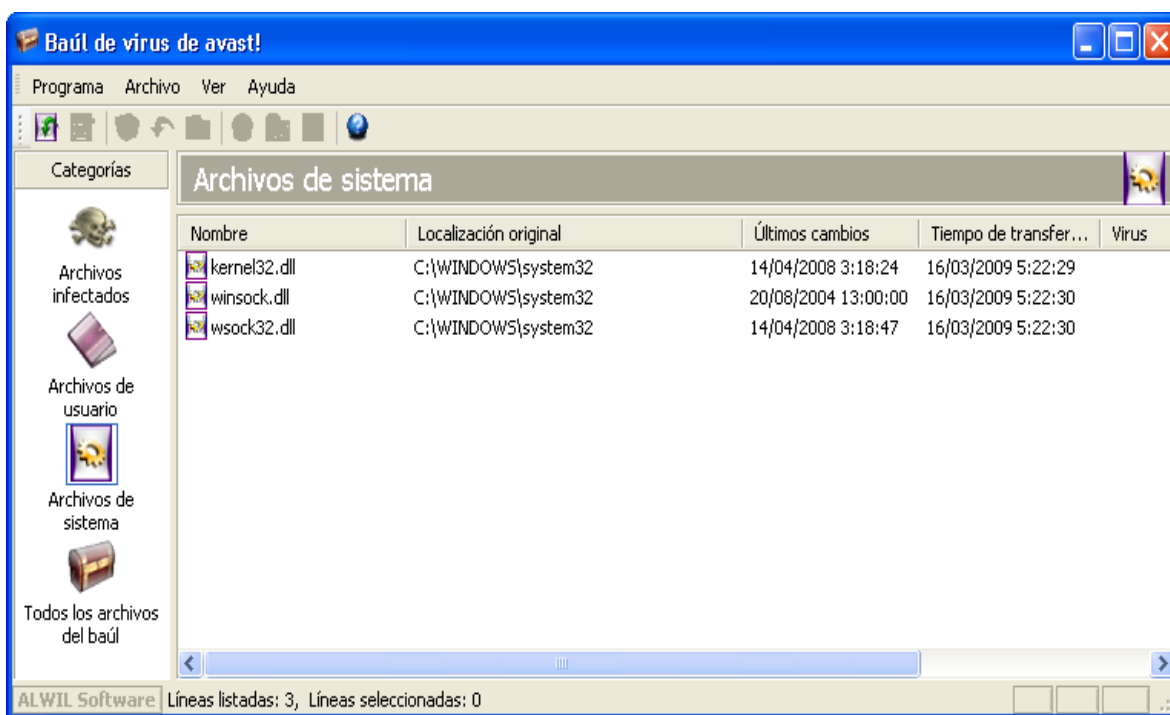
Características de búsqueda de virus:

- ***Lista de virus “peligrosos” (ITW)***
El virus está en la lista de virus extendidos entre los usuarios en todo el mundo.
- ***Virus gusano (Worm)***
Este es un tipo especial de virus que no infecta ficheros directamente, pero lleva a cabo otras acciones indeseadas tales como la propagación por sí mismo vía e-mail, sustracción de contraseñas etc.
- ***Virus de macro (Macro)***
Este tipo de virus utiliza el lenguaje macro de productos Microsoft en especial (e.g. Word, Excel).
- ***Virus que pueden ser reparados (Rep)***
Los ficheros infectados por estos virus pueden ser reparados por el programa avast! y devueltos a su estado original antes de la infección.
- ***Ten cuidado especial al eliminarlo (Care)***
Para estos virus, es necesario seguir una serie de pasos especiales al eliminarlos (de otro modo, se podría causar incluso mayor daño del que causaría el propio virus!).
- ***Infecta al sector de arranque (Boot)***
Este tipo de virus infecta al sector de arranque o boot sector de un disco duro o disquete.
- ***Infecta al sector MBR (MBR)***
Este tipo de virus infecta al sector de arranque del disco de un disco duro.
- ***Infecta archivos COM (COM)***
Este tipo de virus infecta ficheros ejecutables con extensión “.com”.
- ***Infecta archivos EXE (EXE)***
Este tipo de virus infecta ficheros ejecutables con extensión “.exe”.
- ***Reside en memoria (RES)***
Estos virus permanecen en la memoria RAM del ordenador e infecta ficheros que se está iniciando.

Trabajar con ficheros en el Baúl de Virus

Se puede acceder directamente al Baúl de Virus desde las [opciones del menú](#). Como resultado de sus propiedades únicas, el baúl de virus es un área de “cuarentena” eficaz, que puede ser utilizada para los siguientes propósitos:

- **Almacenamiento de virus.**
Si avast! encuentra un virus y usted por alguna razón decide no borrarlo, se le ofrecerá la opción de moverlo al Baúl. Con el virus en el Baúl, usted puede estar seguro de que no será ejecutado por error o accidente.
- **Almacenamiento de ficheros sospechosos.**
El Baúl es útil para el almacenamiento de cualquier fichero sospechoso, el cual se podrá someter a análisis posteriormente.
- **Copia de seguridad de los ficheros del sistema.**
Durante la instalación, hay copias de algunos ficheros de sistema que se almacenan en el Baúl, bajo la categoría "Archivos de sistema" (véase más abajo). Si el sistema principal de ficheros se infectara por un virus, las copias se pueden restaurar desde el Baúl a su ubicación original.



Haciendo clic con el botón derecho del ratón en cualquier fichero, ofrecerá las siguientes opciones. Alternativamente, haciendo clic con el botón izquierdo del ratón en un fichero para seleccionarlo y a continuación haciendo clic en el correspondiente icono en la parte superior de la ventana, o haciendo clic en “Archivo” y seleccionar la opción requerida (Nota: Si hace **dobles clic** en un fichero, no lo ejecutará – sus propiedades aparecerán en su

lugar. Esta es una medida de seguridad para protegerle aún más de una infección accidental dentro del Baúl):

- ***Refrescar todos los archivos***
Seleccione esta opción si quiere estar seguro de que está mirando en la lista completa de ficheros. El programa refresca la lista automáticamente, pero usted puede utilizar esta opción si no quiere esperar.
- ***Agregar.***
Usted puede agregar ficheros sólo a la categoría "Archivos de usuario".
- ***Eliminar.***
Si usted selecciona esta opción, el fichero se borrará de forma irreversible, i.e. los ficheros no son simplemente enviados a la papelera de reciclaje! Antes de borrar cualquier fichero, usted debería estar seguro de que no se trata de un archivo del sistema. Borrar un archivo del sistema podría llevar a consecuencias bastante serias.
- ***Restaurar.***
El fichero será restaurado a su ubicación original y al mismo tiempo eliminado del Baúl.
- ***Extraer.***
El fichero se copiará a la carpeta seleccionada.
- ***Escanear.***
El fichero se escaneará para los virus.
- ***Propiedades.***
Las propiedades del fichero serán presentadas; se puede añadir un comentario al fichero.
- ***E-mail a ALWIL Software.***
El fichero seleccionado se enviará (por e-mail) a ALWIL Software. Usted debería utilizar esta opción sólo en casos especiales - e.g. si usted sospecha que el programa ha identificado incorrectamente un fichero como un virus. No olvide incluir tanta información como le sea posible – e.g. la razón por la que está enviando el fichero, la versión de su base de datos de virus, etc. Esto mejorará el servicio que le ofrezcamos

Haciendo clic en “Configuración del programa” y después en “Baúl” usted puede ajustar el tamaño máximo permitido del Baúl y por consiguiente la cantidad máxima de espacio que ocupe en su ordenador. Usted también puede especificar el tamaño máximo de cualquier fichero por individual que debería ser enviado al Baúl.

El Visor de Informes

Después de cualquier escaneo, avast! antivirus crea varios ficheros de informes donde almacena la información sobre cualquier error o fichero sospechoso. La información sobre instalaciones y actualizaciones del programa y de la base de datos de virus, también se puede encontrar ahí. Para visualizar los informes, simplemente seleccione “Visor de informes (logs)” de las [opciones del menú](#) (véase [página 26](#)).

La información almacenada en los ficheros de informes está dividida en las siguientes categorías:

Información	Sólo información, todo está OK.
Nota	Información importante, todo está OK. Incluye información a cerca de las actualizaciones del programa y de la base de datos.
Advertencia	Ha aparecido un error o se ha identificado un virus, pero el programa puede trabajar o arreglar el problema.
Error	Ha aparecido un error, el programa no puede trabajar.
Error Crítico	Un error crítico del programa, el programa se terminará.
Alerta	Hay posible riesgo para todo el ordenador.
Emergencia	Peligroso para todo el ordenador (seguridad, borrar archivos de sistema).

Haciendo clic en “Configuración” y después en “Registro”, usted puede ajustar el tamaño máximo de cada fichero en el registro.

En el Visor de Informes se pueden buscar registros específicos, filtrar registros según criterios específicos, o exportar los registros a otra ubicación.

Encontrar un registro

1. Presione las teclas “CTRL” y “F” a la vez, o
2. haga clic en “Editar” en la esquina superior izquierda de la pantalla y después en “Buscar”, o
3. haga clic sobre la lupa en la esquina superior izquierda de la ventana, o
4. haga clic con el botón derecho del ratón en la lista de registros y después haga clic en “Filtrar” en el menú presentado

Aparecerá una casilla en la cual usted puede escribir todo o parte del nombre del registro que quiere encontrar. Si usted sabe el nombre exacto, marcando la casilla “Sólo palabras completas” se asegurará de que aparezcan solamente las coincidencias exactas. De igual modo, si usted sólo quiere buscar registros utilizando letras mayúsculas o minúsculas, marque la casilla “Coincidir mayúsculas y minúsculas”. Haciendo clic en “Arriba” o “Abajo” determinará si los registros están enumerados en orden ascendente o descendente.

A continuación haga clic en “Buscar siguiente”. Se mostrará el primer registro. Cualquier otro registro que coincida con el nombre introducido se podrá encontrar haciendo clic en “Buscar siguiente”, hasta que no se puedan encontrar más registros.

Filtrar la lista de registros. Se utiliza para limitar una lista larga de registros a una lista más corta que cumpla ciertos criterios e.g. una palabra clave específica o parte de una palabra.

1. Oprima las teclas “CTRL” y “R” a la vez, o
2. haga clic en “Editar” en la esquina superior izquierda de la pantalla y después en “Filtrar”, o
3. haga clic en el embudo amarillo en la esquina superior izquierda de la pantalla, o
4. haga clic con el botón derecho del ratón en la lista de registros y después haga clic en “Encontrar” en el menú presentado

Aparecerá una casilla en la que podrá especificar los criterios de filtro:

Incluir

Introduzca una palabra clave o parte de una palabra que debería ser incluida en los registros. Puede realizar una búsqueda y escribir e.g. * en lugar de letras que usted desconoce. Cuando hay múltiples palabras clave, se deben separar por un punto y coma (;).

Excluir.

Introduzca una palabra clave o parte de una palabra que no debería ser incluida en los registros.

Rango de tiempo

Aquí usted puede definir el principio y final del periodo para el cual le gustaría que aparecieran los registros.

Seleccionar las líneas marcadas

Si se selecciona esta opción, los registros que coincidan con el criterio seleccionado, simplemente aparecerán seleccionados en la lista.

Mostrar sólo las líneas marcadas (ocultar el resto)

Si se selecciona esta opción, sólo se mostrarán los registros que coincidan con los criterios seleccionados. Los demás registros no serán visibles. Esta opción es útil si la lista original fuera muy larga.

Ordenar registros

Al hacer clic en cualquiera de los encabezamientos de las columnas se ordenarán los registros en orden ascendiente o descendiente según la información en dicha columna. Haciendo clic de nuevo en los encabezamientos de las columnas, la lista volverá a su orden original.

Exportar registros

Aquellos registros encontrados filtrados, o toda la lista de registros pueden ser exportados y guardados como un fichero nuevo. Para exportar registros encontrados o filtrados, seleccione la opción “Exportar las líneas seleccionadas” o haga clic en la flecha verde de la izquierda que puede encontrar en la esquina superior derecha de la pantalla. Para exportar toda la lista, seleccione “Exportar la lista actual” o haga clic en la flecha verde de la derecha. En la nueva ventana que se presenta, elija la carpeta de destino para el fichero exportado y escriba el nuevo nombre de fichero, a continuación haga clic en “Guardar”.

Cómo trabajar con la Interfaz Avanzada de Usuario

Si usted está utilizando la interfaz sin una carátula (o “skin”), al hacer clic en “Herramientas” y “Cambiar a la Interfaz avanzada” le aparecerán los cambios que se muestran más abajo. Si usted está utilizando la interfaz con una carátula, haga clic en “Configuración” y después “Cambiar a la Interfaz Avanzada de Usuario”.

Para volver a la Interfaz Simple de Usuario, haga clic en “Ver” en la esquina superior izquierda de la pantalla, y a continuación “Interfaz simple de usuario”



Los escaneos se ejecutan en la Interfaz Avanzada de Usuario creando “Tareas”. Al crear una tarea, simplemente defina qué áreas deberían ser escaneadas, el nivel de sensibilidad requerido etc. La ventaja de crear una Tarea es que se puede guardar y ejecutarse más tarde, o ejecutarse de nuevo utilizando la opción “Programador”. Una vez se ha ejecutado una tarea, se guardan los resultados para que puedan ser revisados posteriormente.

Cómo trabajar con las Tareas

El programa viene con cuatro tareas ya establecidas. Si hace clic en “Tareas” en la lista de carpetas, o en la lista de estructura de carpetas, verá esto en la ventana superior derecha. Si hace clic en una tarea, verá una breve descripción de la tarea in ventana inferior derecha.

La primera tarea es la **tarea de protección residente** que se ejecuta continuamente para proveer protección a su ordenador en tiempo real escaneando ficheros en cualquier momento en el que se accede a los mismos. La tarea de protección residente se inicia automáticamente al iniciarse el ordenador.

Las otras tres tareas se pueden utilizar para escanear áreas específicas de su ordenador y se puede iniciar haciendo doble clic en ellas, o haciendo clic en ellas con el botón derecho del ratón y seleccionando “Ejecutar”:

Al iniciar la tarea **“Escanear: disquetera A:”** se escaneará cualquier dispositivo de disquetes.

La tarea **“Escanear: selección interactiva”** se puede utilizar cuando usted quiere escanear áreas específicas de su ordenador. Al iniciar esta tarea aparecerá una nueva pantalla en la que usted podrá seleccionar las áreas a ser escaneadas marcando las casillas correspondientes.

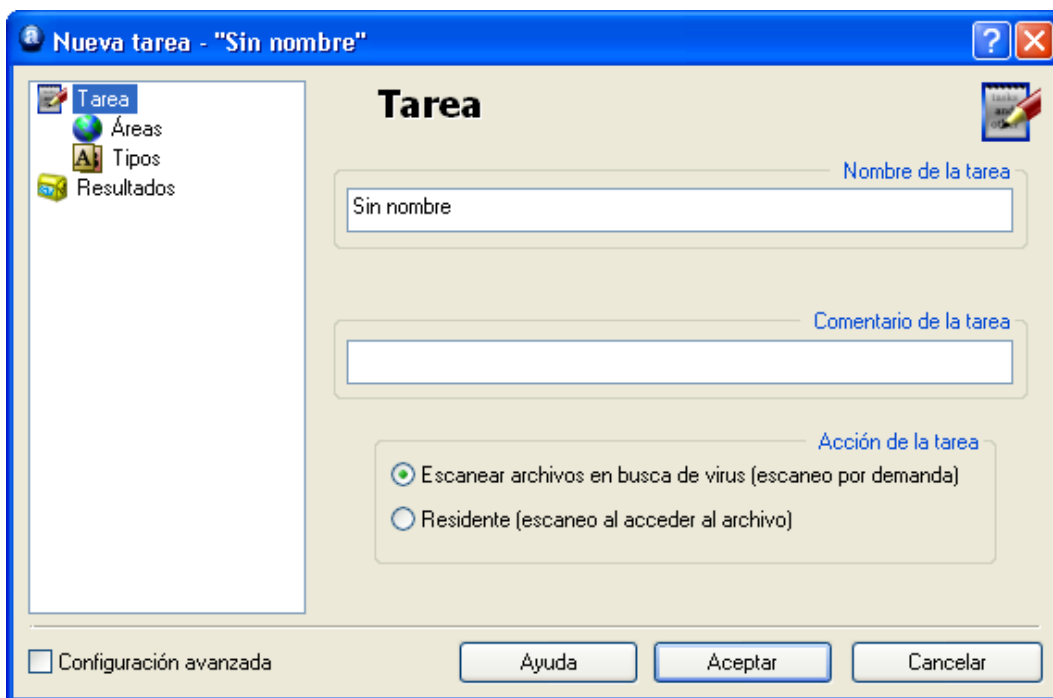
Al iniciar la tarea **“Escanear: discos locales”** se escanearán todos los ficheros y discos duros de su ordenador.

Crear/editar una tarea

Usted también puede crear sus propias tareas, las cuales también podrá ejecutar tan a menudo como desee. Esto es útil si hay ficheros o carpetas concretas en su ordenador que quiere que se escaneen de forma regular.

El hecho de crear una nueva tarea supone varios pasos tales como la definición de las áreas a ser escaneadas, cómo deberían ser reconocidos los ficheros, qué información debería aparecer en el informe etc. Haciendo clic en “Aceptar” al final de cualquier paso, se guardará la tarea en ese estado. Si no se han especificado algunos ajustes, la tarea se guardará con los ajustes por defecto. Para hacer cualquier modificación después de que la tarea haya sido guardada, sólo es necesario seleccionar la misma en la lista de tareas y hacer clic en “Editar” que puede encontrar en la parte superior de la pantalla. De igual modo, para borrar una tarea que ha sido guardada, seleccione dicha tarea y haga clic en “Eliminar”, que puede encontrar a la derecha de “Editar”.

Primero haga clic en “Tareas” en la parte superior de la pantalla, o haga clic con el botón derecho del ratón en “Tareas” en la lista estructurada de carpetas y a continuación haga clic en “Crear nueva”. O, simplemente, haga clic en “Nuevo” en la parte superior de la pantalla y aparecerá la siguiente ventana:

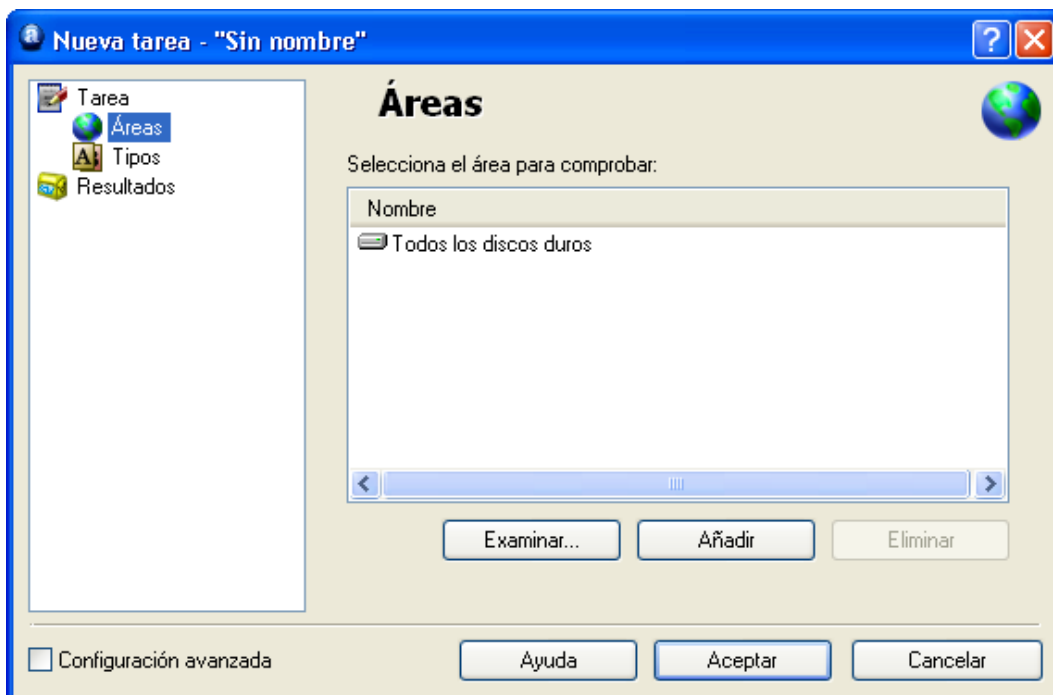


En esta pantalla usted puede asignar un nombre a la tarea, el cual aparecerá en la lista de tareas en la ventana principal. Por lo tanto, dicho nombre debería representar la tarea que se llevará a cabo e.g. “Escanear: Mis documentos”. También puede añadir cualquier comentario adicional que le pueda ser útil. Finalmente, en esta ventana puede especificar si la tarea debería ejecutarse “por demanda” i.e. sólo cuando usted requiera que se ejecute, o “al acceder al archivo”, lo que significa que se escanearán las carpetas o ficheros especificados siempre que intente abrir los mismos.

Crear una nueva tarea “Por demanda”

- ***Áreas***

Con la opción “Escanear archivos en busca de virus (escaneo por demanda)” seleccionada, el paso siguiente para crear una nueva tarea “por demanda” es definir las áreas que deberían ser escaneadas. Para ello, haga clic en “Áreas” y aparecerá la siguiente pantalla:



Las áreas a ser escaneadas incluyen automáticamente “Todos los discos duros”. Si usted no quiere escanear todos los discos duros, borre esto haciendo clic en la opción y a continuación en “Eliminar”. Puede especificar las áreas que se deben escanear haciendo clic en “Examinar” y seleccionando el área (s) marcando las casillas correspondientes.

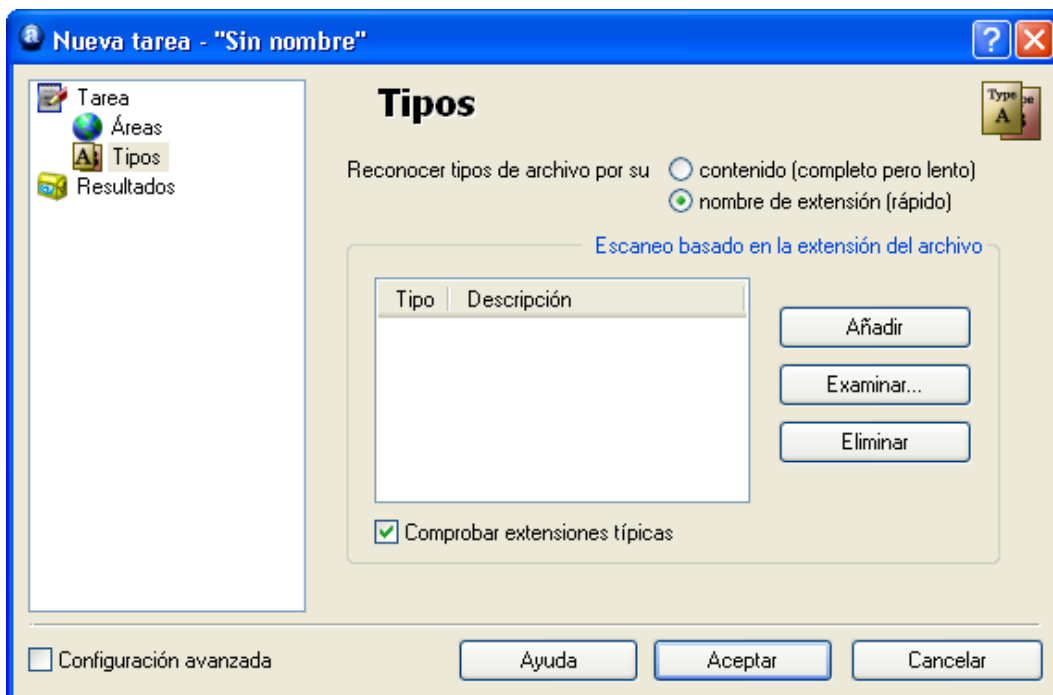
Al hacer clic en “Añadir” usted puede seleccionar entre varias áreas predefinidas. Tenga en cuenta que si usted selecciona “Selección interactiva”, deberá especificar el área objetivo de escaneo cada vez que ejecute la tarea. Si selecciona “Otro”, deberá escribir el área a escanear manualmente en la casilla que dice “<área tipo>”.

- **Tipos**

Una vez haya seleccionado el área(s) que se van a escanear, haga clic en “Tipos” para especificar qué ficheros deberían ser escaneados. Los ficheros se pueden organizar como sospechosos dependiendo de su contenido, que es más minucioso por tanto más lento, o basado en el nombre de su extensión.

Si usted selecciona un escaneo basado en el contenido, puede especificar que se escaneen todos los archivos marcando la casilla “Comprobar todos los archivos”. Si selecciona esta casilla, significa que incluso aquellos archivos que normalmente no contienen virus, tales como pueden ser ficheros de imágenes, también serán escaneados. Si deja esta casilla sin marcar, esos archivos no se escanearán y será reportado en la sección de resultados como “ningún elemento seleccionado”.

Si selecciona un escaneo basado en la extensión, podrá especificar qué extensiones deberían ser reconocidas como sospechosas – véase la pantalla de la página siguiente.



Para escanear ficheros basados en una o más extensiones específicas, haga clic en “Examinar” y aparecerá una lista de extensiones. Si puede encontrar la extensión que usted quiere añadir, haga clic en la misma y a continuación haga clic en “Aceptar” para añadirla a la lista. Si la extensión que usted quiere añadir no está en la lista, puede añadirla manualmente. Haga clic en “Añadir” y después escriba la extensión del fichero que quiere añadir. Para añadir otra extensión, haga clic de nuevo en “Añadir”. Si quiere eliminar la extensión de un fichero de la lista, sólo tiene que hacer clic en dicha extensión para seleccionarla y a continuación hacer clic en “Eliminar”.

Si la casilla “Comprobar extensiones típicas” está marcada, significa que se escanearán automáticamente todas las extensiones conocidas como “peligrosas”.

Cualquier fichero con otras extensiones que no sean las especificadas, no se escanearán y aparecerá en la sección de resultados “ningún elemento seleccionado”.

- **Resultados**

A continuación, haciendo clic en “Resultados” puede especificar qué resultados se deberían almacenar después de haberse completado el escaneo. Normalmente, es suficiente almacenar la información de los archivos infectados, errores “complicados”, y archivos excluidos del escaneo, pero también se pueden almacenar otros resultados haciendo clic en la casilla apropiada. No se recomienda marcar la casilla “Archivos sin errores”, pues podría producir un gran número de resultados que generarían un archivo de datos muy amplio.

Si no quiere almacenar los resultados del escaneo, simplemente desmarque la casilla en la parte de abajo del todo de la pantalla.

Un gran número de opciones adicionales están disponibles marcando la casilla “Configuración avanzada” que puede encontrar en la esquina inferior izquierda en cualquiera de las ventanas anteriores. Esto expandirá la lista de opciones según se muestra más abajo:



- **Sensibilidad**

Al marcar la casilla “Escanear los archivos enteros (puede ser muy lento en archivos grandes)” aparecerán los archivos que han sido testados en su totalidad, y no sólo aquellas partes más frecuentemente afectadas por los virus. La mayoría de los virus se encuentran tanto al principio de un archivo, como al final. Marcando esta casilla tendrá lugar un escaneo más detallado, pero a la vez más lento.

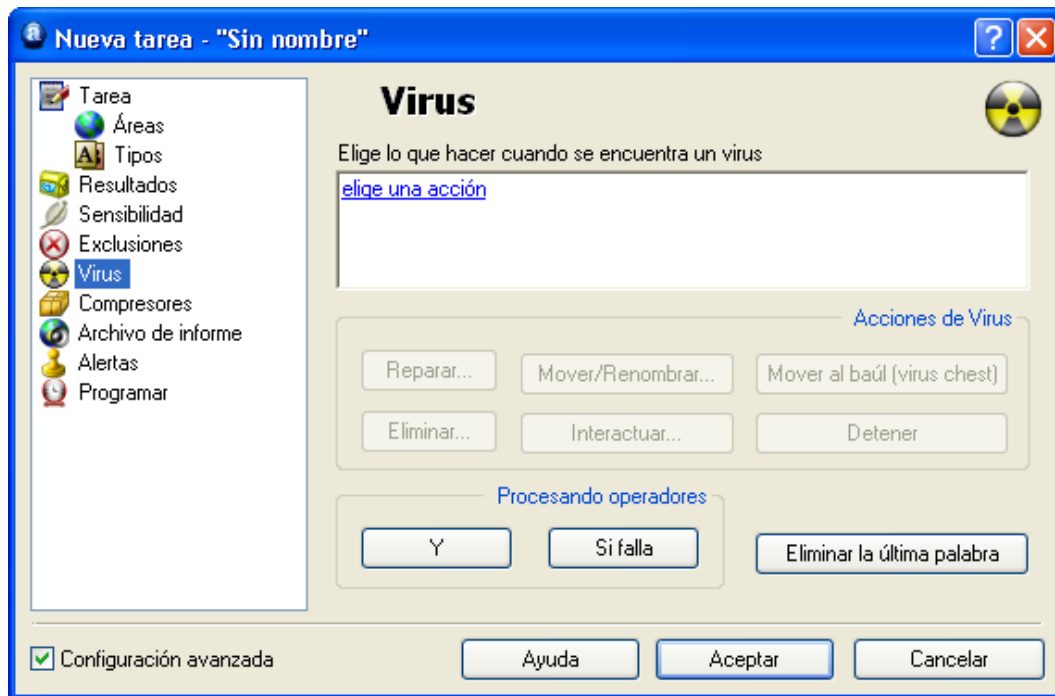
Marcando la casilla “Ignorar objetivos de virus” se analizarán los archivos en la base de datos de virus. Si no se marca, los archivos se analizarán sólo contra aquellos virus que afecten al tipo o archivo dado. Por ejemplo, el programa no buscará virus que infecten archivos con la extensión “.exe” en archivos con una extensión “.com”.

- **Exclusiones**

Aquí se pueden excluir ciertos archivos o carpetas de ser escaneados. Esto funciona exactamente de la misma forma que se describe en la [página 41](#), con la única excepción de que las exclusiones ajustadas aquí sólo se aplican a la tarea específica. Aquellos archivos o carpetas que se han excluido en el menú “Configuración” se excluirán automáticamente de todos los escaneos. Los archivos excluidos se mostrarán en la sección de resultados como “ningún elemento seleccionado”

- **Virus**

Haciendo clic en “Virus” aparecerá la siguiente pantalla:



En esta pantalla usted puede especificar qué acción se debería llevar a cabo cuando se detecta un virus. La opción por defecto es “Elige una acción”. Esta es la opción de “Interactuar”.

Si se deja como la acción seleccionada, significa que siempre que se detecte un fichero sospechoso, le aparecerá una lista de posibles opciones de las cuales deberá seleccionar una. Esto significa que puede especificar qué acción debería tomar individualmente para cada fichero sospechoso.

Haciendo clic en “Elige una acción” mostrará las opciones que se ofrecerán cuando se detecte un fichero sospechoso, i.e. Eliminar, Reparar, Mover al baúl, Mover/Renombrar, o Detener. Solamente aparecerán las opciones que se marquen. Si se desmarca alguna opción, no aparecerá como disponible cuando se detecte un fichero sospechoso.

Estas opciones se describen en la [página 33](#) en la sección “Qué hacer si se encuentra un virus”.

Al seleccionar esta acción, si se detecta un virus se suspenderá el escaneo hasta que usted especifique qué acción se debería tomar. Por tanto, se recomienda seleccionar una o más de las otras acciones, tales como mover los ficheros al baúl de virus, si usted va a programar la tarea para que se ejecute cuando usted no esté utilizando el ordenador.

Para seleccionar una acción diferente, haga clic en “Eliminar la última palabra”. La acción por defecto se borrará y las seis posibles acciones aparecerán ahora seleccionadas en el

centro de la pantalla. Haciendo clic en cualquiera de ellas, insertará la acción a la casilla presente más arriba. Esta acción se aplicará a todos los archivos sospechosos que sean detectados. Para eliminarlos, simplemente haga clic de nuevo en “Eliminar la última palabra”.

Las primeras cuatro opciones se describen detalladamente en la [página 33](#). Al hacer clic en “Interactuar” se reinsertará “Elige una acción”. Haciendo clic en “Cancelar”, simplemente detendrá el escaneo tan pronto como sea detectado el archivo sospechoso.

Se puede especificar más de una acción utilizando la pestaña “Y”. Por ejemplo, puede especificar que cualquier fichero infectado sea reparado y movido a otra ubicación haciendo clic en “Reparar”, después en “Y” y después “Mover/Renombrar”.

También puede especificar cualquier acción alternativa que deberían llevarse a cabo en el caso de que falle la primera acción seleccionada. Por ejemplo, usted podría seleccionar “Reparar” como la acción preferida, pero después haciendo clic en “Si falla” y “Mover al baúl” usted puede asegurarse de que cualquier fichero que no pueda ser reparado se moverá al baúl de virus – véase [página 49](#) .

Nota – si selecciona “Eliminar”, podrá especificar si el fichero debería ser eliminado permanentemente (acción por defecto), o simplemente movido a la papelera de reciclaje. Si selecciona “Eliminar archivo(s) permanentemente”, también podrá especificar si el archivo(s) debería ser eliminado la próxima vez que se reinicie el ordenador en el caso de que no pudieran ser eliminados ahora, haciendo clic en la casilla “Si es necesario, eliminar archivo(s) en el próximo inicio del sistema”.

- ***Compresores***

En esta página usted puede especificar qué archivos comprimidos se analizarán durante la tarea. El ajuste por defecto es sólo auto-extraíble ejecutable. Usted puede especificar que los archivos adicionales deberían ser procesados, aunque esto ralentizará el escaneo. Seleccione la opción “Todos los formatos” si quiere que se analicen todos los ficheros comprimidos que se pueden escanear.

- ***Archivo de informe***

Aquí usted puede crear un informe que contenga la información clave sobre una tarea completa. La información incluida en el informe es esencialmente la misma que se ha almacenado en las sesiones de resultados.

Las opciones varias para crear el informe son las que se describen en la [página 42](#) de este manual.

Nota: El nombre por defecto del informe es task_name.rpt. El informe es un fichero de texto simple que puede ser fácilmente visualizado y modificado.

- **Alertas**

Las alertas pueden ser tanto generales, que serán enviadas siempre que se detecte un virus, o pueden ser generadas sólo cuando se detecta un virus por la tarea concreta a la que está vinculada.

Las alertas que se pueden añadir a la tarea se muestran en la casilla “Alertas disponibles”. Las alertas generales se crean haciendo clic en “Configuración” and “Alertas” según se describe en la [página 45](#), sin embargo, aquellas alertas han sido creadas de este modo no se pueden vincular a una tarea.

Si la alerta que usted desea añadir se muestra aquí, haga clic en la misma para seleccionarla, después haga clic en la pestaña “→”. Esto moverá la alerta a la casilla de “Alertas utilizadas”, lo cual significa que ahora está vinculada a la tarea.

Si la alerta que usted desea añadir no se muestra aquí, haga clic en “Nueva” para crear una alerta nueva.

Usted puede asignar un nombre a la alerta, por ejemplo un nombre que la conecta con la tarea y además puede añadir otras informaciones en la casilla “Comentario”. La alerta se creará exactamente del mismo modo descrito en la [página 45](#)

Una vez haya creado la alerta nueva, haga clic en Aceptar y se ubicará directamente en la casilla “Alertas utilizadas”.

Para eliminar una alerta de la casilla “Alertas utilizadas”, haga clic en la misma para seleccionarla, después haga clic en la pestaña “←”, lo cual la moverá a la casilla “Alertas disponibles”.

Para modificar o eliminar una alerta, seleccione la misma y haga clic en “Modificar” o “Eliminar”.

Si necesita crear una alerta SMTP, no olvide introducir los detalles SMTP después de haber finalizado la creación de su tarea haciendo clic en “Configuración” y “SMTP”.

Tenga en cuenta que las alertas vinculadas a las tareas solamente se enviarán si una tarea específica detecta un virus. Si el virus es detectado por una tarea diferente, no se enviarán. Si usted quiere que se envíe una alerta siempre que un virus sea detectado por cualquier tarea, debería crear una alerta general según se describe en la [página 45](#).

Todas aquellas alertas creadas de esta forma se pueden ver haciendo clic en la carpeta “Alertas” en la lista estructurada de Carpetas. Aquí, usted también puede crear nuevas alertas que se pueden utilizar al crear tareas futuras. Para hacer esto, haga clic en “Alertas” en la parte superior de la pantalla, o haga clic con el botón derecho del ratón en la carpeta Alertas en la lista estructurada de carpetas, y a continuación seleccione la opción crear “Nueva alerta”.

Se puede modificar o eliminar una alerta creada previamente seleccionando la misma y haciendo clic en “Alertas” en la parte superior de la pantalla, y después seleccionando “Editar alerta” o “Eliminar alerta”.

Programador

Durante el proceso de creación de una tarea, se puede programar para que se ejecute automáticamente en una hora y fecha concreta, o repetitivamente, e.g. daily, semanal o mensualmente.

En la ventana “Programar”, haga clic en “Añadir”. Aparecerá una nueva ventana – “Configuración del programador de eventos”. Introduzca un nombre para el evento programado – e.g. “Escaneo diario: todos los discos duros” y cualquier información adicional en la casilla “Descripción” e.g. “Escanear todos los discos duros cada tarde”.

Configuración del programador de eventos

Programador de eventos

Nombre: Escaneo diario de todos los discos duros

Descripción: Escanear todos los discos duros cada tarde

Desactivado

No comenzar la tarea si está funcionando con batería

Terminar la tarea si comienza el modo batería

Tareas programadas

Escanear: discos locales

Tiempo programado

Tipo de programación: diariamente

Hora de comienzo: 16 : 40

Lunes Viernes

Martes Sábado

Miércoles Domingo

Jueves

La hora está en formato militar (0:00-23:59).

Aceptar Cancelar

Seleccione la casilla “Desactivado” si usted no quiere que se active el escaneo aún, o si quiere cancelarlo posteriormente sin tener que eliminarlo permanentemente.

Debajo de esto, hay otras dos casillas de verificación. La casilla “No comenzar la tarea si está funcionando con batería” es principalmente útil para usuarios de ordenadores portátiles. Seleccionar esta casilla asegurará que no se inicie el evento si el ordenador está funcionando con batería.

Al seleccionar la casilla “Terminar la tarea si comienza el modo batería” la tarea se detendrá si el ordenador se desconecta de la electricidad y cambia a la batería mientras se está ejecutando el evento. Otra vez, esto es útil principalmente para propietarios de ordenadores portátiles.

En la casilla “Tareas programadas”, seleccione el nombre de la tarea actual. Finalmente, en la casilla “Tipo de programación” usted puede especificar cuándo y con qué frecuencia se debería ejecutar la tarea. Las opciones disponibles son una vez, diariamente, semanalmente, y mensualmente. Si usted selecciona una vez, simplemente tendrá que introducir la hora y fecha en la que se debería ejecutar; si elige diariamente, deberá seleccionar los días concretos en los que se debería ejecutar la tarea y la hora a la que se debería ejecutar cada día. Si usted elige semanalmente (o mensualmente), es necesario seleccionar el día (fecha), además de la hora desde la que se debería llevar a cabo la tarea.

Para editar posteriormente un evento programado, haga clic en dicho evento con el botón derecho del ratón en la ventana del Programador y seleccione “Propiedades”. Para borrar un evento, haga clic en “Eliminar”.

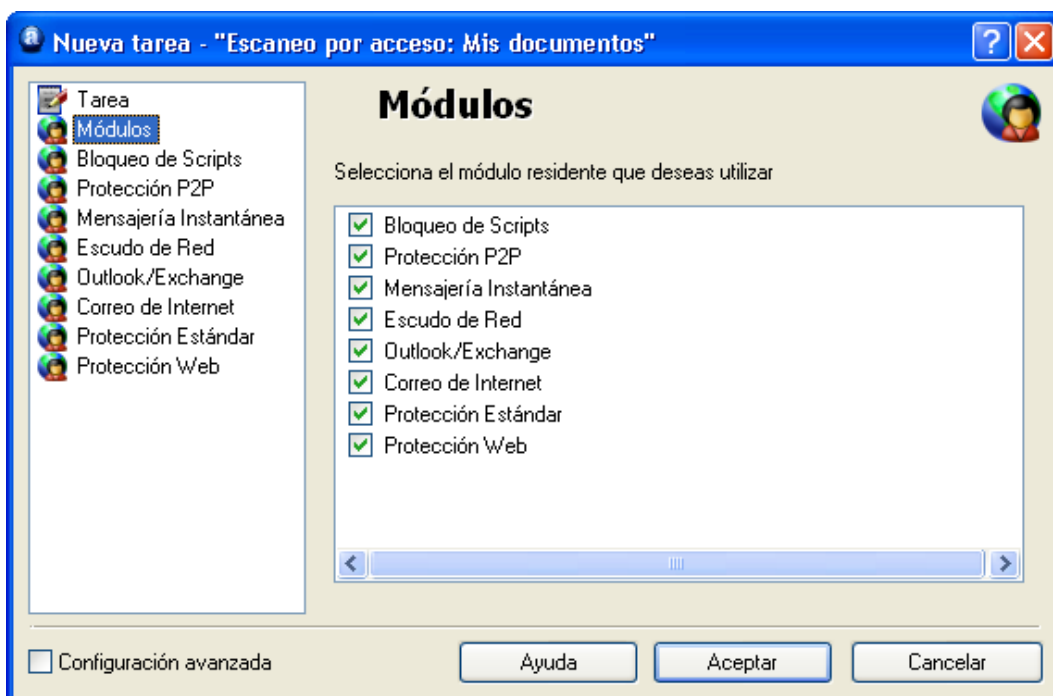
Crear una nueva tarea “Por acceso”

Siempre que se esté ejecutando la tarea de protección residente por defecto, controlará todas las áreas de la actividad llevada a cabo en su ordenador. Si necesita hacer algunos cambios en la protección residente, se recomienda parar la tarea por defecto y crear y ejecutar una nueva tarea, en vez de cambiar la tarea por defecto, con el objetivo de no perder los ajustes de la misma. Si desea parar una tarea, sólo tiene que hacer clic en dicha tarea con el botón derecho del ratón y seleccionar “Detener”. Detener o hacer cualquier modificación en la tarea de protección residente por defecto aquí, es lo mismo que “terminar” o cambiar la protección residente según se describe en la sección de protección residente de esta guía de usuario.

Al ejecutar cualquier tarea de protección residente, se parará automáticamente cualquier otra tarea de protección residente. Una vez esté activa cualquier tarea de protección residente, se indicará con la presencia del icono de la bola azul con la “a” en el medio en la esquina inferior derecha de la pantalla. Si ninguna tarea de protección residente está activa, el icono de la “a” se mostrará con una línea roja a través del mismo.

Para crear una nueva tarea residente, primero haga clic en “Nueva” en la parte superior de la pantalla para abrir una nueva Ventana de tareas. Después haga clic en “Residente” en la parte inferior de la Ventana de tareas (véase página 57) y aparecerá una nueva ventana con la lista de todos los módulos residentes. Para crear una tarea basada sólo en módulos seleccionados, haga clic en “Módulos” y a continuación desmarque los que no sean

requeridos, véase abajo. También puede ajustar la sensibilidad del escaneo haciendo clic en cada módulo de la lista en la parte izquierda de la pantalla y haciendo clic en “Configurar como normal” o “Configurar como alto”



Marcando la casilla “Configuración avanzada” se expandirá la lista de la izquierda incluyendo un número adicional de opciones para cada módulo. Incluyen opciones para escanear solamente tipos de ficheros concretos, para especificar qué acciones tomar si se descubre un fichero infectado – véase página 72 – Ajustes de la Protección Residente – así como las opciones para crear Informes y Alertas, según se describe en la sección anterior.

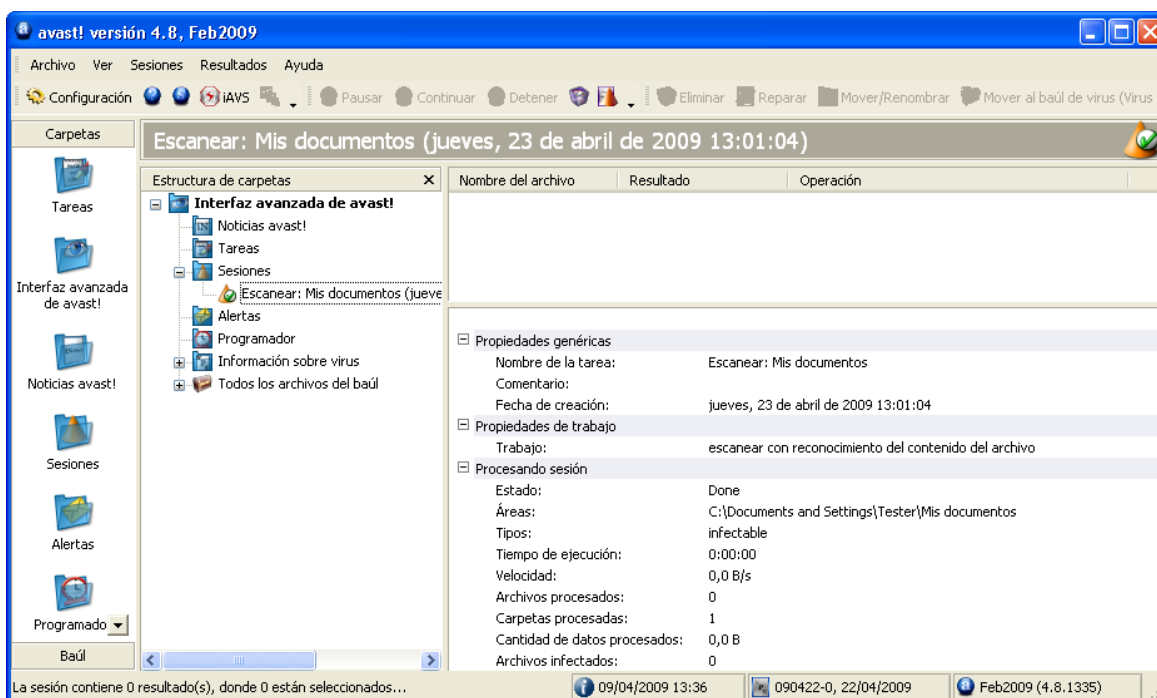
Sesiones: Ejecutar una tarea “Por demanda”

Al hacer clic en cualquier tarea enumerada en la ventana de tareas, se mostrará una descripción de la tarea en la ventana que puede ver más abajo. Haciendo doble clic en cualquier tarea en la ventana de tareas, o haciendo clic en la misma con el botón derecho del ratón y seleccionando “Ejecutar”, se ejecutará la tarea.

Tan pronto como se inicie cualquier tarea, se crea una nueva “sesión”, y el resultado del escaneo se almacena en la carpeta “Sesiones”. Para ver las sesiones individuales, haga clic en el signo “+” a la izquierda de “Sesiones” en la lista de la “Estructura de carpetas”. Hay una sesión grabada para cada tarea y haciendo clic en la sesión en particular obtendrá los resultados del escaneo en la parte derecha según se muestra más abajo. Cualquier fichero sospechoso detectado durante el escaneo se mostrará en la parte superior de la ventana, mientras que los resultados globales del escaneo se mostrarán al final de la ventana.

En la columna “Operación” puede ver qué acción se ha tomado. Si alguna acción automática fué especificada en la página de Virus al crearse la tarea, verá la confirmación

aquí de si la acción se ha realizado con éxito. Si la opción “Interactiva” fué seleccionada, verá un aviso de que ha sido detectado un virus y se le preguntará cómo quiere proceder usted – véase [página 33](#). Puede tomar la acción deseada inmediatamente, o si usted decide dejarlo para más tarde, haciendo clic en el fichero sospechoso aparecerán las opciones disponibles en la parte superior de la pantalla. Cualquier acción manual que tome usted ahora o después también se mostrará en esta pantalla en la columna “Operación”.

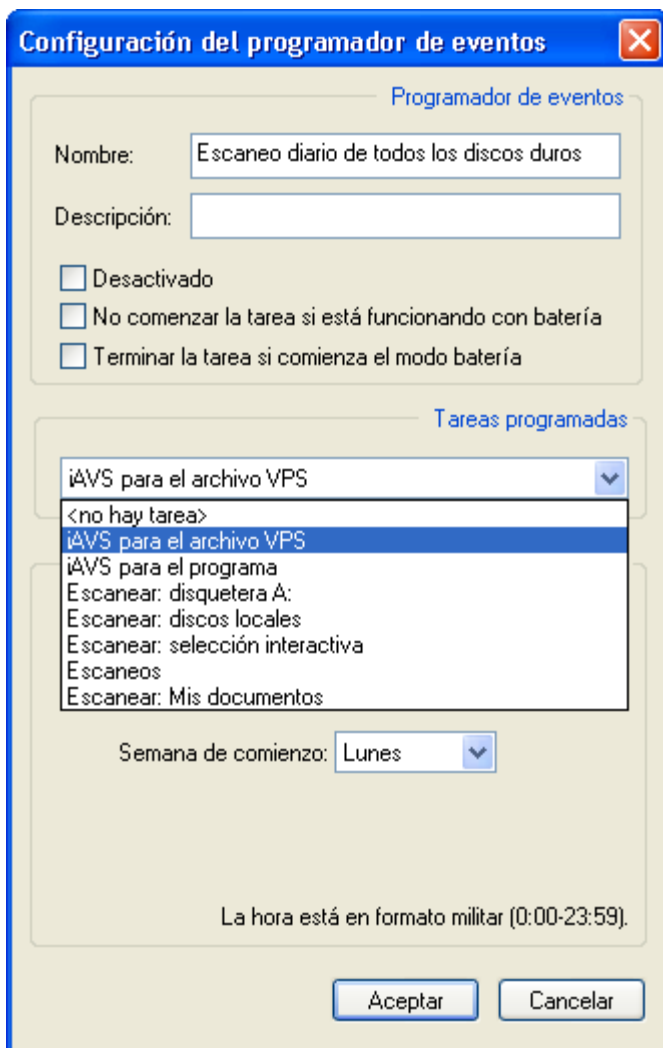


Si se creó un informe al ajustar la tarea, se puede visualizar haciendo clic en “Sesiones” y después en “Mostrar informe”.

Programar tareas/actualizaciones existentes

El programador en la Interfaz Avanzada de Usuario se puede utilizar para programar cualquier tarea que ha sido creada. También se puede utilizar para programar actualizaciones del programa y de la base de datos de virus.

Si quiere programar una tarea, por ejemplo una actualización de la base de datos de virus, primero haga clic en la carpeta “Programador”. Después haga clic en el icono “Nuevo” o haga clic en “Programar” en la parte superior de la pantalla y a continuación haga clic en “Crear evento”. En la pantalla que aparece, introduzca el nombre para el evento programado y, si fuera necesario, una descripción. Las siguientes tres casillas han sido previamente explicadas en la sección Crear una nueva tarea “Por demanda”. Después seleccione el evento que quiere programar de la lista de tareas disponibles haciendo clic en flecha azul que señala hacia abajo según se muestra a continuación.



Finalmente, ajuste la frecuencia de la tarea, lo cual se describe en la sección anterior, y a continuación haga clic en “Aceptar”.

La tarea ahora está programada y cuando haga clic en “Programador” en la lista de Carpetas o en lista estructurada de carpetas, aparecerá como una tarea programada. Tan pronto como se inicie la tarea programada, se creará una nueva sesión y usted podrá ver los resultados del escaneo en cualquier momento haciendo clic en la sesión apropiada en la carpeta “Sesiones”.

Para editar posteriormente un evento programado, haga clic en dicho evento con el botón derecho del ratón y seleccione “Propiedades”. Para borrar un evento, haga clic en “Eliminar”.

Al programar un escaneo en su ordenador, recuerde que si la opción “interactiva” fué seleccionada al crear la tarea, si se detecta un virus el escaneo se suspenderá hasta que usted especifique qué acción se debería llevar a cabo. Véase [página 60](#). En esta situación, se aconseja crear y programar una nueva tarea en la que usted puede especificar que se lleve a cabo una acción diferente si se detecta un virus, tal como mover el fichero al baúl de virus.

Nota – el programa y la base de datos de virus se pueden actualizar en cualquier momento haciendo clic tanto en “Archivo” como en “Actualización de iAVS” para actualizar la base de datos de virus, o “Actualización del programa” para actualizar el programa en sí mismo. La base de datos de virus también se puede actualizar haciendo clic en el icono “iAVS” en la parte superior de la pantalla.

Programar un escaneo al inicio

Para programar un escaneo al inicio de su ordenador, primero haga clic en la carpeta “Programador”. Después haga clic en “Programar” en la esquina superior izquierda de la pantalla y seleccione “Programar escaneo al inicio del sistema”, o haga clic en el icono del lápiz que aparece debajo un pequeño triángulo verde, que se encuentra en la parte superior de la pantalla. Aparecerá una nueva ventana en el centro de la pantalla, que se describe en la [página 39](#).

El baúl de virus

Usted puede ver todos los archivos almacenados actualmente en el baúl de virus haciendo clic en la carpeta “Todos los archivos del baúl”. Haciendo clic en “Baúl” en la esquina inferior izquierda de la pantalla, y después haciendo clic en uno de los cuatro iconos, usted puede visualizar de forma separada los archivos infectados, archivos de sistema o archivos de usuario. También puede visualizar estos ficheros haciendo clic en el signo “+” a la izquierda de la carpeta “Todos los archivos del baúl” y a continuación seleccionando la sub-carpeta requerida.

Para llevar a cabo una acción respecto a un archivo específico, haga clic en el mismo y los iconos grises en la parte superior de la pantalla cambiarán a otro color diferente. Estos iconos se pueden utilizar para llevar a cabo varias acciones, las cuales se describen en la [página 48](#) de este manual. Alternativamente, haga clic en “Baúl” en la parte superior de la pantalla, o haga clic con el botón derecho del ratón en cualquier archivo y se presentarán todas las opciones en una lista, de las cuales la opción requerida puede ser seleccionada.

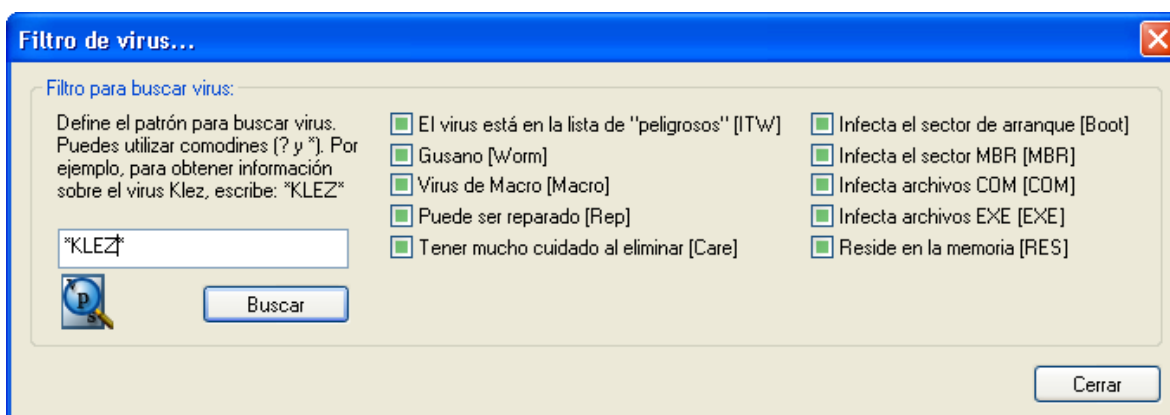
Tenga en cuenta que para utilizar las opciones de “Actualizar” y “Añadir”, puede ser necesario tener que hacer clic en la ventana en la que aparecerán los archivos.

Cómo buscar la Base de Datos de Virus

La base de datos de virus es accesible desde la Interfaz Avanzada de Usuario haciendo clic en la carpeta “Información sobre virus”

Las características de cada virus se indican mediante una marca de selección. Las características se explican por individual en la [página 48](#).

Para buscar un virus en particular, o tipo de virus, haga clic en “Información sobre virus” en la parte superior de la pantalla y después en “Filtro”, y le aparecerá la siguiente pantalla.



Los virus de la lista se pueden buscar por muchos parámetros. Si usted sabe el nombre del virus, simplemente escriba el nombre en la casilla y haga clic en la pestaña Buscar. Si usted sabe sólo parte del nombre, puede escribir “?” en lugar de un carácter desconocido (letra o número) o “*” en lugar de muchos caracteres desconocidos.

Ejemplo: Suponga que está buscando el virus “Klez”. Su nombre actual en la base de datos es Win32:Klez-H [Wrm]. Escriba: *klez*. Todos los virus que contengan la palabra "klez" serán encontrados.

Para restringir la búsqueda, también puede utilizar las casillas próximas a la descripción de cada virus. Para buscar por una característica en concreto, marque la casilla haciendo clic dos veces en la misma. Al hacer clic en cualquier casilla una vez, con lo que cambia a una casilla de color gris, significa que no debe tener dicha característica. Si se deja alguna casilla sin marcar pero figura en verde, significa que no importa si el virus tiene esa característica o no.

Visor de Informes

La información contenida en el Visor de Informes and how para buscar registros concretos se describe en la [página 51](#).

Para acceder al Visor de Informes via la Interfaz Avanzada de Usuario, haga clic en “View” then on “Show Log Files”.

Limpiador de virus

El Limpiador de Virus “avast! Virus Cleaner” es un programa diseñado para eliminar cualquier rastro de infección de virus de su sistema. Repara archivos infectados (donde sea posible) y borra los cuerpos de virus, con lo que no es necesario reinstalar su sistema o restaurarlo con las copias de seguridad. También elimina ítems de virus del sistema de registro, repara los archivos de configuración corruptos, y borra los archivos creados temporalmente por los virus (tales archivos no contienen ningún código de virus, con lo que no se reconocen como archivos sospechosos – pero ocupan espacio en su disco duro).

El Limpiador de Virus está integrado directamente en el programa y si se detecta un virus que puede ser completamente eliminado por el Limpiador de Virus, una pestaña adicional – “Eliminar el virus completamente del sistema” – aparecerá en la casilla de aviso del virus. Si esta opción está disponible, se recomienda utilizarla.

El Limpiador de Virus también se puede ejecutar directamente desde la Interfaz Avanzada de Usuario haciendo clic en “Archivo” y después en “Iniciar el Limpiador de virus avast! Una vez iniciada, hará lo siguiente:

- Escaneará la memoria del sistema operativo y, si se encuentra algún virus, se terminará el proceso afectado – evitando de este modo la propagación. Si no es posible terminar el proceso afectado, el virus será desactivado en la memoria para detener su propagación.
- Escaneará sus discos duros locales.
- Escaneará los “ítems de inicio” (tales como el registro de sistema, Carpeta(s) de inicio, etc.). Se eliminarán o arreglarán las referencias a ficheros infectados encontrados en la memoria o en el disco.
- Se eliminarán o arreglarán (según sea necesario) los ficheros infectados, identificados en el punto 2.
- Se eliminarán los archivos temporales adicionales creados por los virus identificados.

Si se necesita reiniciar el ordenador para finalizar el proceso de desinfección (e.g. si no se ha podido eliminar un archivo debido a que estaba actualmente en uso, o si el proceso de virus desactivado aún está presente en la memoria), se le preguntará si el sistema debería ser reiniciado inmediatamente.

Al ejecutar el limpiador de virus, se recomienda no iniciar ninguna otra aplicación, pues algunos virus o gusanos se iniciarán automáticamente al iniciarse otra aplicación. Los

procesos de virus activos serán terminados/desactivados sólo al inicio del proceso de desinfección; si posteriormente se activa un virus en el proceso (al iniciar otra aplicación, tal como Notepad, Explorer, etc.), probablemente no se eliminará de su ordenador!

Para trabajar correctamente, el Limpiador de Virus requiere privilegios de administrador al ejecutarse en los sistemas operativos Windows NT/2000/XP/2003/Vista/2008, de lo contrario algunos virus podrían no ser detectados o completamente eliminados!

Instalación Silenciosa

Esta opción, dirigida principalmente a los administradores de red, hace posible (y fácil) instalar avast! en una serie de ordenadores, sin tener que involucrar a los usuarios. El programa se puede instalar con ciertos ajustes y tareas predefinidos.

Para crear la instalación silenciosa:

- Primero instale el programa en un ordenador.
- Modifique los ajustes exactamente como quiere que figuren en los demás ordenadores.
- Ajuste los parámetros requeridos de las tareas.
- Si fuera necesario, establezca la contraseña de acceso a los ajustes de la protección residente.
- En la Interfaz Avanzada de Usuario, seleccione “Archivo” después “Crear una instalación silenciosa”.

A continuación, ajuste los parámetros de la instalación silenciosa:

- Modo silencioso – Durante la instalación en los ordenadores de destino, sólo se mostrarán los mensajes de error.
- Modo muy silencioso – Durante la instalación en los ordenadores de destino, no se mostrarán ningunos mensajes.
- Ruta de instalación – Insertar la carpeta donde se deberían instalar los archivos del programa (la carpeta por defecto es Program files\Alwil Software\Avast4).
- No reiniciar – El ordenador necesita ser reiniciado después de la instalación. Si usted selecciona esta opción, no se pedirá reiniciar.
- Preguntar por reiniciar - Al finalizar la instalación, se le pedirá al usuario que reinicie su ordenador.
- Si no se seleccionan ni “No reiniciar” ni “Preguntar por reiniciar”, el sistema se reiniciará automáticamente cuando la instalación haya finalizado.
- Hacer clic en la pestaña Crear.

Finalmente, seleccione una carpeta compartida donde deberían almacenarse los archivos necesarios para la instalación silenciosa. Los archivos admin.ini y tasks.xml se guardarán en la carpeta seleccionada. El archivo admin.ini contiene los ajustes del programa avast!, el archivo tasks.xml contiene los ajustes de las tareas particulares. Si se había establecido una

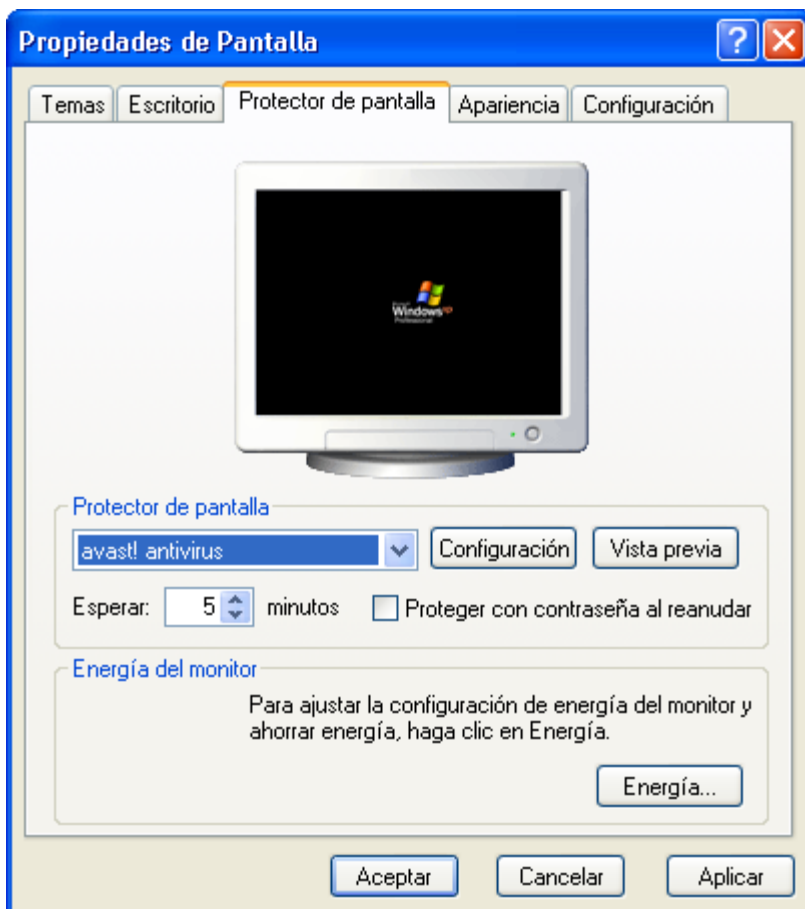
contraseña en los ajustes de la protección residente, habrá un tercer archivo en la carpeta final: aswResp.dat; la cual contiene la contraseña cifrada.

El fichero de instalación de avast! también se debería copiar a esta carpeta, desde donde debería ejecutarse en cada uno de los ordenadores finales.

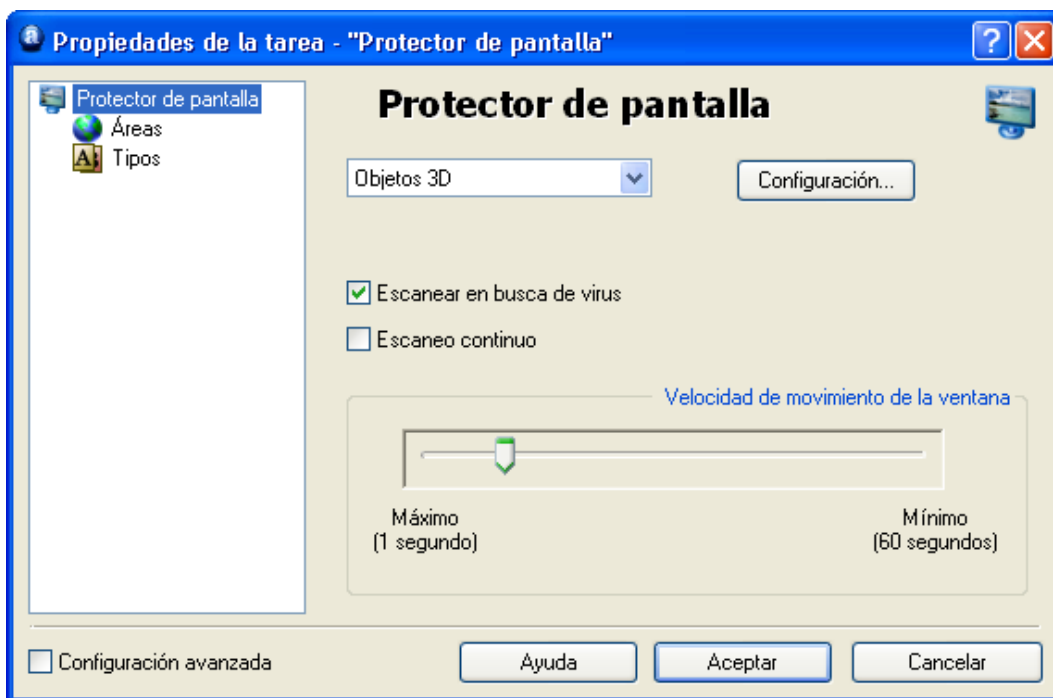
Cómo activar el protector de pantalla avast! antivirus

Avast! antivirus puede escanear su ordenador de potenciales infecciones de virus durante periodos en los que el ordenador no está en uso y el protector de pantalla está activado. Durante este tiempo, aparecerá una pequeña casilla en el protector de pantalla que le informará sobre el progreso del escaneo.

Para activar el protector de pantalla avast! antivirus, haga clic en la pestaña “Inicio” en la esquina inferior izquierda de su pantalla y seleccione “Configuración”. Después haga clic en “Panel de control” y haga doble clic en “Pantalla”. En la casilla que aparece, haga clic en “Protector de pantalla” y después en la primera flecha que indica hacia abajo para mostrar las opciones disponibles. Haga clic en “avast! antivirus”. En la casilla abajo, también puede cambiar el número de minutos después de los cuales se activa el protector de pantalla, utilizando las flechas azules que indican hacia arriba y hacia abajo, y si es necesario introducir su contraseña para continuar.



Haciendo clic en “Configuración” en esta pantalla, usted puede seleccionar el protector de pantalla normal en el cual aparecerá la casilla del mensaje avast! que le avisa sobre el estado del escaneo – véase página siguiente.



Si usted quiere escanear su ordenador siempre que el protector de pantalla esté activado, marque la casilla “Escanear en busca de virus”. Si no se marca esta casilla, el protector de pantalla funcionará sólo como un protector de pantalla normal.

Marcar la casilla “Escaneo continuo”, asegurará que el escaneo se inicie de nuevo una vez se hayan escaneado todas las áreas definidas.

Cambiar la velocidad del movimiento de la ventana, afectará a la frecuencia a la que se actualizará la posición de la casilla que marca el progreso del escaneo.

Haciendo clic otra vez en “Configuración”, le permitirá establecer los ajustes del protector de pantalla normal.

Al hacer clic en “Áreas” y “Tipos”, usted puede especificar qué áreas de su ordenador y qué archivos deberían ser escaneados según se describe en la [página 56](#).

Si usted marca la casilla “Configuración avanzada”, es posible especificar una serie de ajustes adicionales, según se describe en la sección [Crear una nueva tarea “Por demanda”](#).

Ajustes de la Protección Residente

1. Mensajería Instantánea

Programas

Aquí puede especificar para qué programas IM (Mensajería Instantánea) deberían escanearse los archivos. Si usted utiliza Windows 95/98/ME y desea proteger el programa Trillian, usted deberá introducir la ruta a su fichero de configuración, talk.ini (para esto, puede utilizar la pestaña Examinar). Algunos programas se pueden proteger sólo si usted está utilizando Windows NT, 2000, XP, 2003, Vista o 2008.

Compresores

Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Virus

En esta página usted puede especificar de antemano qué acción llevar a cabo en relación a cualquier archivo infectado. Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 60](#).

2. Correo de Internet

En las páginas “POP”, “SMTP”, “IMAP” y “NNTP” usted puede especificar si los e-mails entrantes y/o salientes y novedades (News) deberían escanearse. Si se detecta un virus, se insertará un mensaje en el mensaje pertinente. También puede especificar que se inserte una nota en mensajes limpios confirmando que no contienen ningún virus o ninguna infección.

Redirigir

Esta página hace posible establecer un escaneo transparente de los e-mail. Cualquier e-mail que pase a través de puertos especificados, será escaneado. Esta característica está sólo disponible en sistemas operativos basados en NT (Windows NT/2000/XP/2003/Vista/2008).

- Puertos redirigidos.

Los puertos por defecto son los números de puerto estándar para los cuatro protocolos de e-mail básicos: Si usted utiliza un puerto diferente (o puertos), deberían ser introducidos aquí. Los valores múltiples deberían ser separados por comas.

- Direcciones ignoradas.

Aquí puede introducir las direcciones de servidores de correo o puertos específicos que quiere excluir del escaneo. Esta característica puede ser útil cuando usted quiere que avast! escanee solamente mensajes a o desde una cuenta particular (e ignorar el resto). Por ejemplo, si usted introduce smtp.server.com, avast! no escaneará los mensajes salientes (SMTP) para la cuenta correspondiente.

- Ignorar comunicación local.

Normalmente, se debería marcar esta opción. Si se desmarca, avast! escaneará incluso la comunicación local (lo cual es generalmente seguro), puede ralentizar un poco su ordenador. Nota: No introduzca ningún número de puerto que no sea aquel que usted realmente utiliza para el tráfico de e-mail. De lo contrario, podrían surgir problemas inesperados.

Avanzado

- Mostrar detalles sobre la acción realizada.

Si se marca esta opción, en la esquina inferior derecha de la pantalla, se mostrará la información sobre los archivos que se están analizando actualmente.

- Modo silencioso.

Si la acción especificada en la página de Virus es la acción por defecto i.e. la opción interactiva, y el modo silencioso seleccionado, cualquier archivo infectado se tratará automáticamente según las siguientes reglas:

- Si se selecciona “con respuesta general Sí (OK)”, cualquier fichero infectado adjunto a un email se borrará automáticamente.
- Si se selecciona la segunda opción “con respuesta general No (Cancel)” cualquier archivo infectado se moverá automáticamente al baúl de virus.

Si la acción especificada en la página de Virus es la acción por defecto y esta casilla se ha dejado sin seleccionar, la ventana de alerta normal de virus se mostrará preguntando cómo quiere tratar usted con el archivo infectado.

Si se especifica cualquier otra acción, i.e. una acción que no sea la opción interactiva por defecto, se quedará sin efecto al seleccionar esta casilla.

Tenga en cuenta que si también se ha especificado una acción que no sea la acción por defecto para la Protección Estándar, esto anulará la acción especificada por el módulo Correo de Internet!

- Tiempo de espera para la comunicación con Internet.

Este es el tiempo en segundos de espera por una respuesta del servidor de correo. Usted puede especificar si la conexión debería ser cerrada en el caso de no recibir una respuesta durante este tiempo o si debería pedirle primero una confirmación.

- Mostrar icono cuando se procesa el correo

Si se marca esta casilla, aparecerá un pequeño icono en la barra de tareas en la esquina inferior derecha de la pantalla de su ordenador para indicar que el escaneo está en progreso.

Heurísticas

avast! no sólo puede escanear el correo entrante, sino que también puede controlar mensajes utilizando análisis heurísticos y probablemente mostrar un virus que aún no está presente en la base de datos de virus. Usted puede modificar los ajustes del análisis heurístico en esta página.

- Sensibilidad - Baja.
 - Comprobación de adjuntos básica.
Los archivos adjuntos se verifican de acuerdo con el nombre y si el nombre de uno de ellos contiene dos extensiones, e.g. "Patch.jpg.exe", se tratará como uno potencialmente peligroso. avast! también analiza si la extensión del archivo adjunto corresponde al tipo de fichero actual e.g. si el archivo "Pamela.jpg" es una foto, lo cual se esperaría, o un fichero renombrado COM.
 - Comprobar secuencia de espacios en blanco.
Algunos virus añaden espacios (u otros caracteres "blancos" que no se pueden visualizar) al final de la extensión de un archivo, seguido por una segunda, extensión real que es peligrosa. Debido a la longitud del nombre del fichero, el usuario puede no ver la segunda extensión sin embargo el análisis heurístico puede descubrir esta trampa. El número de espacios consecutivos en blanco permitidos son cinco. Si hay más de cinco, aparecerá un mensaje de aviso.
- Sensibilidad – Media (además de lo anterior).
 - Comprobación de adjuntos exhaustiva.
Así como la comprobación de adjuntos básica, también aparecerá un mensaje de aviso si el adjunto tiene una extensión ejecutable simple (EXE, COM, BAT etc.). No todos esos archivos son peligrosos y este nivel de sensibilidad, por consiguiente, generará más alertas de falsos-positivos que la comprobación de adjuntos básica.

- Sensibilidad - Alta. (además de lo anterior)
 - Comprobación de la parte HTML.
Algunos virus pueden aprovecharse de los fallos en algunos programas de correo (especialmente inseguros MS Outlook y Outlook Express) que hacen posible iniciar el virus simplemente visualizando el mensaje en el panel de vista previa. avast! comprueba si el código HTML del mensaje contiene una etiqueta que permite la trampa. En caso afirmativo, aparecerá un mensaje de aviso.
 - Mensajes salientes – Tiempo de comprobación.
La mayoría de los virus se propagan por e-mail y se envían por sí mismos a direcciones almacenadas en el libro de direcciones de Windows. En un periodo de tiempo muy breve, los mensajes se envían a un gran número de direcciones, con el mismo título y/o adjunto. avast! monitoriza el número de mensajes en un periodo dado de tiempo y también puede controlar el título y/o los adjuntos. Todos estos parámetros se pueden ajustar en la página Heurísticas (Avanzada).
 - Mensajes salientes – Mensajes en masa.
Los virus también se pueden propagar enviándose por sí mismos sólo en un mensaje a muchos destinatarios. avast!, por consiguiente, monitoriza el número total de destinatarios de los mensajes. El número total de destinatarios permitido se puede ajustar en la página de Heurística (Avanzada).

- Sensibilidad - Personalizada

Haciendo clic en “Personalizar” usted puede seleccionar cuál de los componentes del análisis de heurística quiere utilizar.

Usted puede adicionalmente seleccionar “Comprobar asunto y estructura”. Si se selecciona esta opción, los encabezamientos del título de los e-mail se analizará para números largos de caracteres sin sentido e.g. si el título contiene la secuencia "<?*&\$^*(^%#\$%* _())", aparecerá un aviso.

- URLs permitidas

Haciendo clic en “URLs permitidas”, usted puede definir cualquier URLs que se considere seguro, el cual será entonces ignorado por el análisis heurístico. Para añadir un URL, haga clic en “Añadir” y después escriba manualmente el nombre del URL. Para eliminar un URL, haga clic una vez en el mismo para seleccionarlo, y después haga clic en “Eliminar”

- Modo silencioso

En esta página, también puede especificar qué acción se debería llevar a cabo si se detecta un mensaje infectado.

Heurísticas (Avanzada)

Esta página le permitirá modificar los ajustes del análisis heurístico para el correo saliente. Los ajustes se utilizan sólo cuando la sensibilidad de "Heurística" se establece en alta o personalizada (y se pueden modificar sólo con el ajuste de sensibilidad personalizada).

- Tiempo comprobado.

avast! contará los mensajes salientes durante el tiempo dado. Los ajustes por defecto son 5 mensajes en 30 segundos. Significa que si se envían más de 5 mensajes en medio minuto, con el mismo título y/o conteniendo el mismo adjunto, aparecerá un mensaje.

- Contador de advertencias.

Este es el número de mensajes permitidos sin ningún aviso, donde los mensajes tienen el mismo título y/o contienen el mismo adjunto. Cuando se excede este número, aparecerá un aviso.

- Comprobar asuntos.

Si se establece este ajuste, los mensajes en masa se identificarán según el tema o título del email.

- Comprobar adjuntos.

Si se selecciona este ajuste, los mensajes en masa serán identificados según el adjunto.

- Recuento absoluto.

Este es el número máximo total de destinatarios del mensaje, i.e. las direcciones en los campos Para, Carbon Copy (CC) y Blind Carbon Copy (BCC) ajustada a 10 por defecto. Si se excediera, aparecerá un aviso.

Compresores

Esta página sólo se muestra cuando se accede a los ajustes de la tarea de protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Virus

En esta página usted puede especificar de antemano qué acción llevar en relación a cualquier archivo infectado. Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario, y se describe en la [página 60](#).

3. Escudo de Red

El Escudo de Red protege su ordenador de los ataques de gusanos en Internet. Funciona de forma similar a un cortafuegos, pero no es un sustituto.

Configuración

- Mostrar mensajes de aviso

Si se selecciona esta casilla, aparecerá un mensaje en la esquina inferior derecha de la pantalla siempre que sea detectado un ataque de un gusano de internet.

- Registro

Si se selecciona esta casilla, se grabará el historial de los ataques de gusanos y se mostrará en la página “Últimos ataques”. Para ver esta página, es necesario acceder directamente a los ajustes de la protección residente i.e. haciendo clic con el botón derecho del ratón en el icono de avast!; No se puede ver al acceder a los ajustes de la protección residente a través de la tarea de la protección residente en la interfaz avanzada de usuario.

Últimos ataques

En esta página se mostrarán los 10 últimos ataques de gusanos si en la página anterior se ha seleccionado la casilla “Registro”. Incluirá la fecha y hora del ataque, tipo de ataque y la dirección IP y puerto de dónde se ha originado

4. Outlook/Exchange

Escáner

Aquí puede especificar qué tipo de mensajes se deberían escanear y si los cuerpos de los mensajes también deberían ser escaneados, así como los adjuntos.

Correo entrante

Aquí puede especificar qué se debería hacer si se detecta un mensaje entrante infectado, por ejemplo, puede ser entregado, descartado (borrado), o redirigido a una carpeta de correo diferente. También puede especificar si se debería insertar una nota en los mensajes limpios y/o infectados, y el formato de la nota i.e. TXT o HTML. Cualquier fichero infectado adjunto o contenido en un mensaje será tratado de acuerdo a los ajustes en las páginas “Almacenamiento de Virus” y “Avanzado”.

Correo saliente

Aquí puede especificar si se debería insertar una nota en los mensajes limpios, y el formato de la nota, según se indica más arriba. Los mensajes infectados no serán enviados en ningún caso. También puede especificar que los adjuntos deberían ser escaneados en el momento en el que se adjuntan en lugar de cuando son enviados.

Firmas

Utilizando firmas, es posible reducir considerablemente el número de mensajes que necesitan ser escaneados. Las firmas son pequeños "sellos" que se adjuntan a los mensajes no infectados para confirmar que no contienen virus. Toda firma contiene la fecha y hora del escaneo.

Las firmas de MS Outlook/Exchange son completamente compatibles con aquellas de e.g. avast! Exchange Server Edition. Por lo tanto, los mensajes son testados por Exchange Server no serán analizados de nuevo por Outlook/Exchange, logrando de este modo un tiempo de transferencia más rápido.

- **Insertar firmas en los mensajes limpios.**

Esta opción se debería seleccionar si quiere que las firmas se añadan a los mensajes limpios.

- **Aceptar siempre mensajes firmados.**

Si se selecciona esta casilla, los mensajes correctamente firmados siempre serán fiables y no serán escaneados, sin importar lo antigua que sea la firma (a menos que la casilla "Siempre ignorar las firmas más antiguas que las actuales en la base de datos" sea seleccionada).

- **Aceptar mensajes firmados sólo hasta X días.**

Aquí puede ajustar la edad máxima de las firmas para que sean fiables. El valor ajustado aquí podría ser anulado por la opción " Siempre ignorar las firmas más antiguas que las actuales en la base de datos " – véase más abajo.

- **Ignorar todas las firmas (no aceptar).**

Si se selecciona esta casilla, todos los mensajes serán escaneados independiente de si contienen una firma válida o no.

- **Siempre ignorar las firmas más antiguas que las actuales en la base de datos.**

Si se selecciona esta casilla, los mensajes que tengan una firma válida serán analizados, si la firma es más antigua que la base de datos de virus actual. Esto podría ser útil, pues un mensaje podría contener un nuevo virus que fué añadido a la base de datos de virus después del escaneo original. Si el mensaje es fiable, no será escaneado y el virus no sería detectado.

Almacenamiento de virus

En esta pantalla, usted puede especificar que una copia de un adjunto infectado se guarde en una carpeta específica en el disco duro de su ordenador. Usted puede utilizar el botón Examinar para ubicar y seleccionar la carpeta requerida. Si marca la casilla “Sobreescribir archivos existentes”, cualquier archivo con el mismo nombre será reemplazado por el nuevo archivo.

Avanzado

- **Modo silencioso**

Si la acción especificada en la página de Virus es la acción por defecto, i.e. la opción interactiva, seleccionando esta casilla moverá automáticamente cualquier archivo infectado al baúl de virus.

Si la acción especificada en la página de Virus es la acción por defecto y esta casilla se ha dejado sin marcar, la pantalla normal de alerta de virus se mostrará preguntando cómo desea usted tratar con el archivo infectado.

Si se especifica alguna otra acción, i.e. cualquier otra acción que no sea la opción interactiva, marca esta casilla no tendrá ningún efecto.

- **Mostrar información detallada en la acción tomada**

If this box is checked, information about the files currently being tested will be displayed in the bottom right corner of the screen.

- **Mostrar un icono en la barra de tareas cuando se escanea el correo**

Si se selecciona esta casilla, aparecerá un pequeño icono en la bandeja del sistema en la esquina inferior derecha de la pantalla de su ordenador para indicar que hay un escaneo en progreso.

- Mostrar la pantalla de inicio cuando se carga el módulo

Si se selecciona esta casilla, la pantalla de avast! aparecerá siempre que se inicie el módulo de correo.

Finalmente, si especifica su perfil MAPI y contraseña, serán utilizados para visualizar la estructura de su carpeta de correo cuando haga clic en el botón Examinar en la página de Correo Entrante.

Heurísticas

Los ajustes en esta página son los mismos que para el Correo de Internet

Heurísticas (Avanzada)

Los ajustes en esta página son los mismos que para el Correo de Internet, pero con dos ajustes adicionales:

- Recuento relativo

Este es el número permitido de destinatarios de un mensaje expresado como un porcentaje del número total de direcciones en el libro de direcciones de correo. Si se excede este porcentaje, aparecerá un mensaje de aviso.

- Recuento mínimo

Este es el número mínimo de destinatarios actuales, correspondientes al cómputo relativo, bajo el cual el aviso no se mostrará. En otras palabras, si se excede el cómputo relativo, el aviso no se mostrará si el número actual de destinatarios es inferior que el cómputo mínimo. Ejemplo: Cómputo relativo = 20%, Cómputo mínimo = 10. Si el número de direcciones es 40 y se envía un mensaje a 9 destinatarios, se excederá el cómputo relativo pero no se mostrará el mensaje de aviso, puesto que el número actual es inferior que el cómputo mínimo.

Compresores

Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Virus

En esta página usted puede especificar de antemano qué acción tomar en relación a cualquier archivo infectado. Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 60](#).

5. Protección P2P

Programas

En esta página usted puede especificar los programas para los cuales los archivos recibidos deberían ser escaneados. Algunos programas sólo pueden ser protegidos en Windows NT, 2000, XP, 2003, Vista ó 2008.

Compresores

Esta página sólo se muestra al acceder a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Virus

En esta página usted puede especificar de antemano qué acción llevar a cabo en relación a cualquier fichero infectado. Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 60](#).

6. Bloqueo de Scripts

Programas protegidos

En esta página usted puede seleccionar los navegadores que deben ser protegidos por el módulo de bloqueo de scripts.

Avanzado

- Mostrar pantalla flotante al inicio

Si se selecciona esta casilla, la pantalla de avast! se mostrará siempre que se inicie el navegador.

- Mostrar información detallada en la acción ejecutada

Si se selecciona esta casilla, la información referente a los archivos que están siendo actualmente analizados, se mostrará en la esquina inferior derecha de la pantalla.

- Modo silencioso

Si se selecciona esta casilla, y se detecta un script sospechoso, se bloqueará el acceso a la página web.

Virus

En esta página usted puede especificar de antemano qué acción tomar en relación a cualquier archivo infectado que trate de instalarse en su ordenador. Esta página sólo se muestra al acceder a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 60](#).

7. Protección Estándar

Escáner (Básico)

En esta página usted pueden especificar los objetos que deben ser escaneados por este módulo. Se recomienda seleccionar todas las casillas en esta página, lo cual permitirá la detección de los tipos más comunes de virus.

Escáner (Avanzado)

En esta página usted puede especificar que se escaneen otros archivos de acuerdo a su extensión, incluso cuando están abiertos, o cuando son creados o modificados.

- Escanear archivos cuando se abren.

Las extensiones de los archivos adicionales a ser escaneados deberían separarse mediante una coma. Usted puede utilizar el comodín "?" (e.g. si usted quiere que se escaneen todos los archivos abiertos .htm y .html, introduzca "htm", "html" o utilice el comodín - "ht?"; en el caso siguiente, sin embargo, todos los ficheros con extensiones que empiezan por "ht", tales como "htt", serán escaneados).

- Siempre escanear archivos de script WSH.

Esta opción asegura que todos los ficheros de script (Windows Scripting Host) sean analizados.

- No escanear bibliotecas del sistema.

Las librerías de sistema fiables no serán escaneadas al abrirse, sólo se llevará a cabo un análisis rápido para validar la autenticidad. Esta opción puede acelerar un poco el inicio del sistema.

- Escanear archivos creados/modificados.

Si se selecciona esta casilla, se escanearán los archivos en el momento en el que son creados o modificados. Usted puede especificar si esto debería ser aplicado a:

- Todos los archivos, o
- Sólo archivos con las extensiones seleccionadas

Si se selecciona la casilla “Juego de extensiones por defecto”, sólo aquellos archivos cuyas extensiones que generalmente son consideradas como "peligrosas" serán escaneados – haga clic en “Mostrar” para ver la lista de extensiones por defecto. Usted también puede especificar las extensiones a ser escaneadas.

Bloqueador

En esta página usted puede especificar qué operaciones particulares están bloqueadas por archivos con extensiones específicas. Esto se puede aplicar al “Juego de extensiones por defecto” – haga clic en “Mostrar” para ver la lista de extensiones por defecto, pero usted también puede especificar extensiones adicionales para las cuales las operaciones se deberían bloquear.

Usted puede especificar las operaciones que deberían ser bloqueadas para los tipos de archivos dados i.e. al abrir, renombrar, borrar o reformatar.

Finalmente, usted puede especificar qué se debería hacer si una operación es una de aquellas que debería ser bloqueada, pero que avast! no es capaz de obtener una confirmación i.e. si la operación debería ser aceptada o denegada.

Avanzado

- Mostrar información detallada en las acciones ejecutadas

Si se selecciona esta casilla, la información sobre los archivos que están siendo testados actualmente, se mostrarán en la esquina inferior derecha de la pantalla.

- Modo silencioso

Si la acción especificada en la página de Virus es la acción por defecto i.e. la opción interactiva, y se selecciona el modo silencioso, cualquier fichero infectado se tratará automáticamente de acuerdo a las siguientes normas:

- Si se selecciona “Con una respuesta general Sí (OK)”, no se llevará a cabo ninguna acción en relación al fichero infectado
- Si se selecciona la segunda opción “Con una respuesta general No (Cancelar)”, cualquier archivo infectado será movido automáticamente al baúl de virus.

Si la acción especificada en la página de Virus es la acción por defecto y esta casilla se deja sin seleccionar, la pantalla normal de alerta de virus se mostrará preguntando cómo quiere usted tratar con el archivo infectado.

Si se especifica cualquier otra acción, i.e. cualquier acción que no sea la opción interactiva por defecto, seleccionar esta casilla no tendrá ningún efecto.

Finalmente, puede modificar la lista de lugares que no serán procesados por este módulo. Tenga en cuenta que las ubicaciones que han sido excluidas del escaneo por todos los módulos no se muestran en esta lista.

Compresores

Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Virus

En esta página usted puede especificar de antemano qué acción llevar a cabo en relación con cualquier fichero infectado. Esta página sólo se muestra cuando se accede a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario descrita en la [página 60](#).

8. La Protección Web

La Protección Web funciona como un servidor proxy local. En sistemas operativos NT (Windows NT/2000/XP/2003/Vista/2008) la protección es completamente transparente y no suele ser necesario ajustar ninguno de los ajustes normales. Si usted está utilizando Windows 95/98/ME, es necesario modificar los ajustes en las Opciones de Internet – en concreto, la dirección y puerto del proxy local según se indica a continuación:

Si utiliza una red de área local (LAN):	Si utiliza una conexión dial-up (módem):
Iniciar Internet Explorer.	Iniciar Internet Explorer.
Seleccione Herramientas y después Opciones... del menú principal.	Seleccione Herramientas y después Opciones de Internet... del menú principal.
Cambie a la página de Conexiones	Cambie a la página de Conexiones.
Haga clic en los Ajustes LAN	Seleccione su conexión dial-up de la lista y haga clic en “Configuración”.
Seleccione la opción “Utilizar un servidor proxy para su LAN”	Seleccione la opción “Utilizar un servidor proxy para esta conexión”.
Escriba “localhost” en el campo disponible para la Dirección (alternativamente, usted puede insertar la dirección de IP 127.0.0.1, la cual es la misma que el localhost). Introduzca 12080 en el campo Puerto.	Escriba “localhost” en el campo disponible para la Dirección (alternativamente, usted puede insertar la dirección de IP 127.0.0.1, la cual es la misma que el localhost). Introduzca 12080 en el campo Puerto.
Confirme haciendo clic en Aceptar.	Confirme haciendo clic en Aceptar.

Nota: Si usted utiliza múltiples conexiones, es necesario ajustar la dirección y puerto del proxy local para cada conexión por separado.

Simple

- Activar el escaneo de la web

Desmarcando esta casilla, puede apagar el escaneo web sin afectar al bloqueo URL, que permanecerá activo.

- Usar el escaneo inteligente

Si se selecciona esta casilla, los archivos que se descarguen serán escaneados casi en tiempo real. Los datos se escanean según van llegando – y los siguientes datos se descargan sólo cuando se ha verificado que los anteriores no contienen ningún virus. Si se desmarca esta opción, todos los ficheros se descargarán primero a una carpeta temporal, y serán escaneados después.

Las otras opciones en esta página no están disponibles en Windows 95, 98, y Millennium:

- Puerto(s) HTTP redirigido(s).

Este ajuste es importante si usted utiliza algún tipo de servidor proxy para acceder a Internet y quiere escanear la comunicación entre el servidor y su ordenador. Si usted se conecta a un servidor proxy utilizando e.g. el puerto 3128, inserte este número en la casilla. De lo contrario, avast! esperará que la comunicación tenga lugar en el puerto 80 (por defecto) y todo lo demás será ignorado. Nota: No introduzca ningún otro puerto que no sea HTTP (tales como los puertos para ICQ, DC++, etc.). Múltiples números de puertos deberían ser separados por comas.

- Direcciones ignoradas.

Aquí usted debería introducir los nombres de los servidores o direcciones de IP que no serán redirigidas a la Protección Web. Múltiples direcciones deberían ser separadas por comas.

- Ignorar comunicación local.

Si se marca esta opción, toda la comunicación local - i.e. comunicación entre los programas ejecutándose en su ordenador, será ignorada.

Escaneo de la web

En esta página, usted puede especificar qué archivos deberían ser escaneados cuando se descargan de Internet. Usted puede especificar que todos los ficheros deben ser escaneados, o sólo aquellos con extensiones concretas. Si usted elige esto último, deberá introducir las extensiones de los ficheros a ser escaneados, separándolos por comas. Usted también puede insertar los tipos de ficheros MIME que deberían ser escaneados. En ambos casos, los comodines pueden ser utilizados.

Excepciones

Aquí usted puede especificar los objetos que no serán escaneados por la Protección Web. Esto puede ser útil al descargar un gran número de ficheros desde una única ubicación (fiable!)

- URLs a excluir

Utilice el botón de Añadir para introducir las direcciones URL que deberían ser ignoradas. Si usted quiere bloquear sólo una página, es necesario introducir la ruta completa e.g. si usted añade `http://www.yahoo.com/index.html`, sólo la página `index.html` será excluida del escaneo. Si usted introduce `http://www.yahoo.com/*`, sin embargo, ninguna página que empiece por `http://www.yahoo.com` será escaneada. De igual modo, si usted quiere excluir un archivo en concreto de ser escaneado, e.g. archivos con una extensión `".txt"`, simplemente introduzca `*.txt`.

- Tipos MIME a excluir

Aquí usted puede especificar los tipos/subtipos MIME a ser excluidos del escaneo.

Bloqueo de URLs

La Protección Web también se puede utilizar para bloquear el acceso a ciertas páginas web. So apaga por defecto, sin embargo, se puede utilizar para prevenir el acceso a páginas web "no recomendadas" (e.g. conteniendo pornografía, software ilegal, etc.). Si el navegador web solicita dicha página bloqueada, aparecerá un mensaje anunciando que el acceso a la página ha sido bloqueado por avast! antivirus.

La casilla "Activar el bloqueo de URLs" primero debe ser seleccionada y usted entonces podrá introducir las direcciones a ser bloqueadas haciendo clic en el botón "Añadir", y a continuación insertar la URL correspondiente. Se pueden utilizar los comodines (i.e. `?` y `*`), por ejemplo, si usted inserta `http://www.penthouse.com/*`, no se mostrará ninguna página que empiece por `http://www.penthouse.com`

Las direcciones de URL introducidas serán completadas de acuerdo a las siguientes reglas:

Si la dirección no empieza por http:// o los comodines * o ?, avast! añade el prefijo http:// al principio de la dirección y añade un asterisco al final. Por tanto, si usted introduce www.yahoo.com, será modificado por http://www.yahoo.com*.

Avanzado

- Mostrar información detalla en las acciones ejecutadas

Si se selecciona esta casilla, la información sobre los ficheros que están siendo testados actualmente se mostrará en la esquina inferior derecha de la pantalla.

Modo silencioso

Si se marca esta casilla, la conexión será terminada siempre que se encuentre un virus

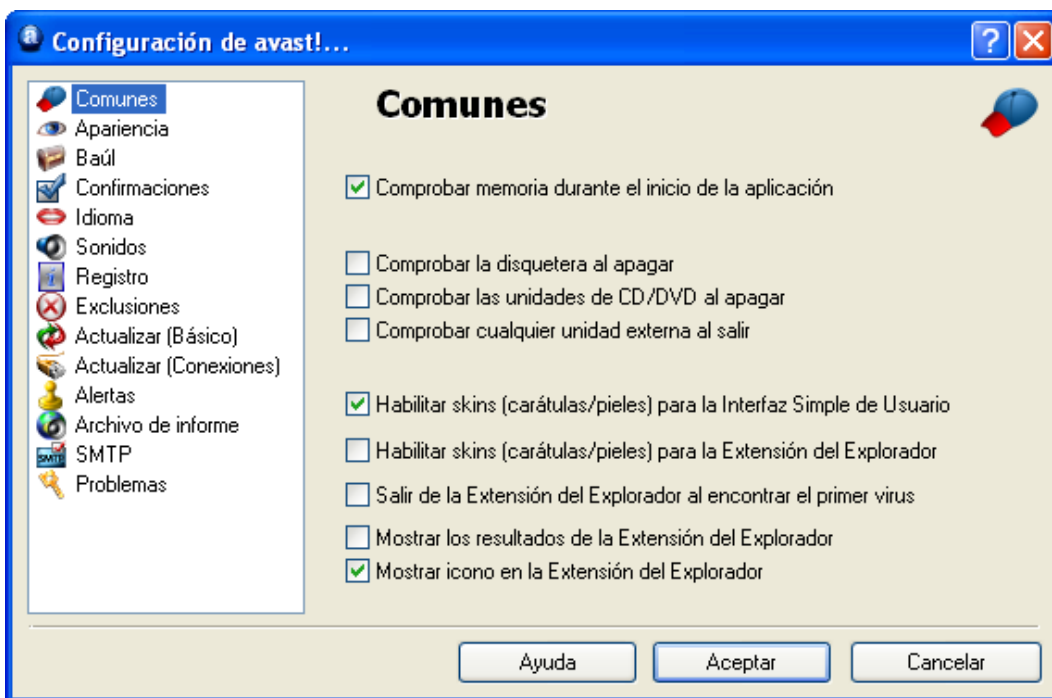
Compresores

Esta página sólo se muestra al acceder a los ajustes de la tarea de la protección residente en la Interfaz Avanzada de Usuario y se describe en la [página 61](#).

Otros ajustes avast!

Muchas otras partes del programa avast! son capaces de ser modificadas de acuerdo con sus requisitos o preferencias personales. Algunos de ellos ya han sido descritos en las secciones anteriores.

Si usted está utilizando la Interfaz Simple de Usuario, abra las [opciones del menú](#) (véase [página 26](#)) y hace clic en “Configuración”, aparecerá la siguiente pantalla. Si usted está utilizando la Interfaz Avanzada de Usuario, sólo necesita hacer clic en “Configuración” y también habrá una opción adicional – “Interfaz Avanzada”. Los ajustes pueden ser modificados haciendo clic en el membrete correspondiente en la parte izquierda de la pantalla:



Ajustes comunes

En esta pantalla usted puede especificar qué comprobaciones llevar a cabo al iniciar o apagar su ordenador. Aquí usted también puede modificar la apariencia del programa marcando o desmarcando la casilla “Permitir skins...”.

Extensión Explorer

Las cuatro últimas casillas de esta pantalla están relacionadas con “Extensión Explorer”. Esta es la facilidad de escanear cualquier archivo por individual haciendo clic con el botón derecho del ratón en el mismo y seleccionando la opción “Escanear <filename>”. Si se marca la última casilla, esta opción tendrá el icono de con la “a” al lado.

Apariencia

Haciendo clic en “Apariencia” usted puede especificar si el icono de avast! – la bola azul con la “a” en el medio – debería mostrarse en la esquina inferior derecha de la pantalla y también si debería ser animada (rotando) mientras se está llevando a cabo el escaneo.

Usted puede añadir un efecto translúcido a la apariencia del reproductor avast!. Estos cambios serán efectivos después de reiniciar su ordenador.

Interfaz Avanzada (sólo se muestra si se utiliza la Interfaz Avanzada de Usuario)

En esta pantalla, usted puede especificar si las tareas especiales “Extensión Explorer” (véase más arriba) y “Protector de pantalla” (véase [página 72](#)) están incluidas en la lista de tareas en el panel de tareas de la interfaz avanzada. Si se muestran aquí, pueden ser editadas del mismo modo que las demás tareas seleccionándolas y haciendo clic en “Editar”.

Marcando la casilla “Desplazar resultados de la sesión”, aparecerá la lista de archivos escaneados continuamente desplazándose hacia abajo mientras el escaneo está en progreso. Esto puede ser útil si usted quiere visualizar actualmente el progreso del escaneo. Si desmarca esta casilla, usted tendrá que hacer el desplazamiento manualmente para poder ver todos los resultados del escaneo.

La última casilla en esta pantalla le permite especificar que las sesiones finalizadas deberían borrarse automáticamente después de cierto periodo de tiempo.

Confirmaciones

Esta pantalla le permite determinar si se le debería pedir la confirmación cuando usted seleccione cierto tipo de acciones, y también si usted querría recibir los mensajes de confirmación después de que se hayan llevado a cabo ciertas acciones.

Las preguntas de confirmación son una característica segura de avast! antivirus que le permite cancelar una acción que ha sido seleccionada por error.

Si usted no desea recibir ningún mensaje de confirmación o pregunta en particular, simplemente desmarque la casilla correspondiente. Sin embargo, si se desmarca una pregunta de confirmación, la acción correspondiente se llevará a cabo tan pronto como la acción sea seleccionada sin opción de cancelarla.

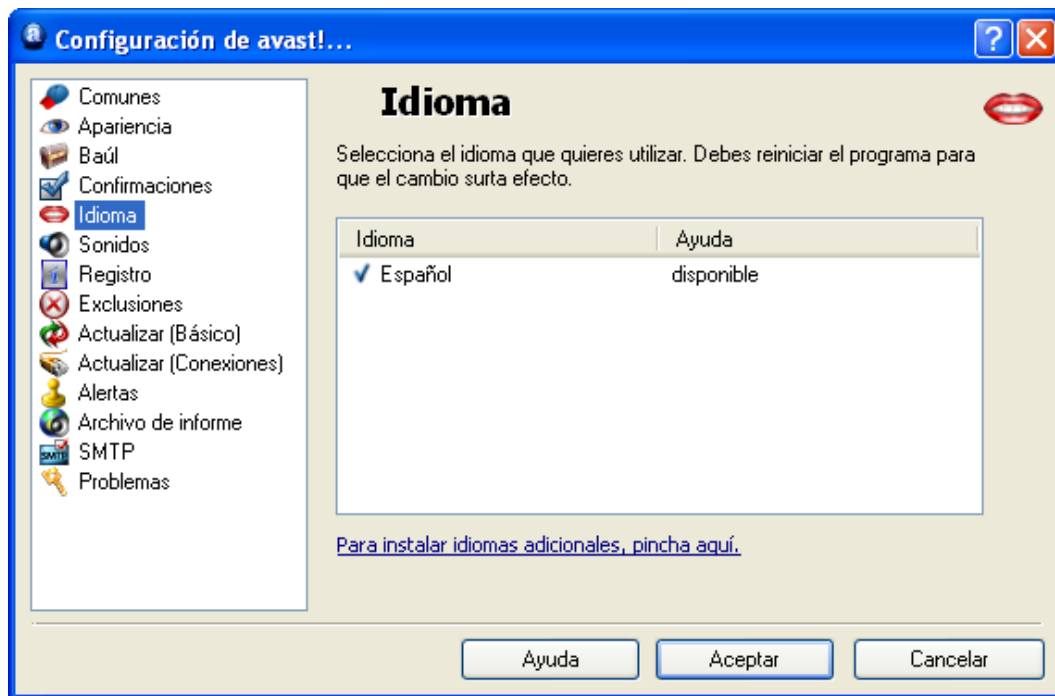
Las siguientes confirmaciones/preguntas son consideradas como estándar, pero se pueden apagar desmarcando la casilla correspondiente:

- ***Preguntar antes de cerrar la Interfaz Simple cuando un escaneo esté ejecutándose***
Si se cierra el programa mientras un escaneo está en progreso, el escaneo se terminará automáticamente en dicho momento
- ***Preguntar si persisten los cambios en el módulo de estado residente***
Este mensaje aparecerá si usted decide “Terminar” cualquiera de los módulos de protección residente – véase [página 24](#). Si su respuesta es “Sí”, el módulo particular permanecerá desactivado hasta que usted lo reactive manualmente. Si su respuesta es “No”, se reactivará la próxima vez que reinicie su ordenador.
- ***Preguntar antes de detener la protección por acceso***
Este mensaje aparecerá si usted decide “Terminate” la protección residente (o por acceso) como una unidad – véase [página 20](#). Si su respuesta es “Sí”, la protección residente se desactivará, pero se reactivará automáticamente la próxima vez que reinicie su ordenador.
- ***Preguntar antes de eliminar archivos del baúl***
Si se marca esta casilla, el programa siempre solicitará una confirmación antes de borrar cualquier archivo. Esto es para prevenir que cualquier archivo se borre accidentalmente
- ***Mensaje al concluir el procesamiento de resultados satisfactoriamente***
Esto confirma que cualquier acción que usted seleccione en relación a cualquier fichero enviado por el programa e.g. borrar, mover el fichero al baúl de virus etc ha sido completado
- ***Mensaje al ocurrir un error durante el procesamiento de resultados***
Esto le informa que la acción que usted ha seleccionado en relación al archivo enviado por el programa no debería ejecutarse.

- ***Mensaje cuando se utiliza un archivo VPS antiguo***
 Esto es para avisarle de que la base de datos de virus no está actualizada. Para asegurar que su sistema esté completamente protegido, la base de datos de virus debería ser actualizada regularmente - véase [página 38](#)
- ***Advertencia sobre la versión BETA***
 Este mensaje es para avisarle de que la versión del programa que está utilizando usted aún está en estado de análisis.
- ***Mostrar mensaje cuando se haya enviado correctamente un informe de error***
- ***Mostrar la ventana de estado en el baúl (virus chest) cuando se complete una acción***
 Si se selecciona esta casilla, recibirá un mensaje que confirma que la acción que usted ha seleccionado ha sido procesada con éxito.
- ***Mensaje cuando hay buenos resultados durante la configuración de tareas.***
 Cuando se selecciona esta casilla, usted verá un aviso si especifica “Aceptar archivos” debería incluirse en los resultados del escaneo. Nota, esto sólo se aplica a la creación de tareas en la Interfaz Avanzada de Usuario.
- ***Eliminación de fichero(s) con extensiones peligrosas***
 Este es un aviso de que puede no ser fiable borrar el archivo especificado, pues el tipo de archivo es uno que normalmente contiene datos importantes.

Modificar el idioma del programa

Si usted desea modificar el idioma del programa, haga clic en “Idioma” y aparecerá la siguiente pantalla:



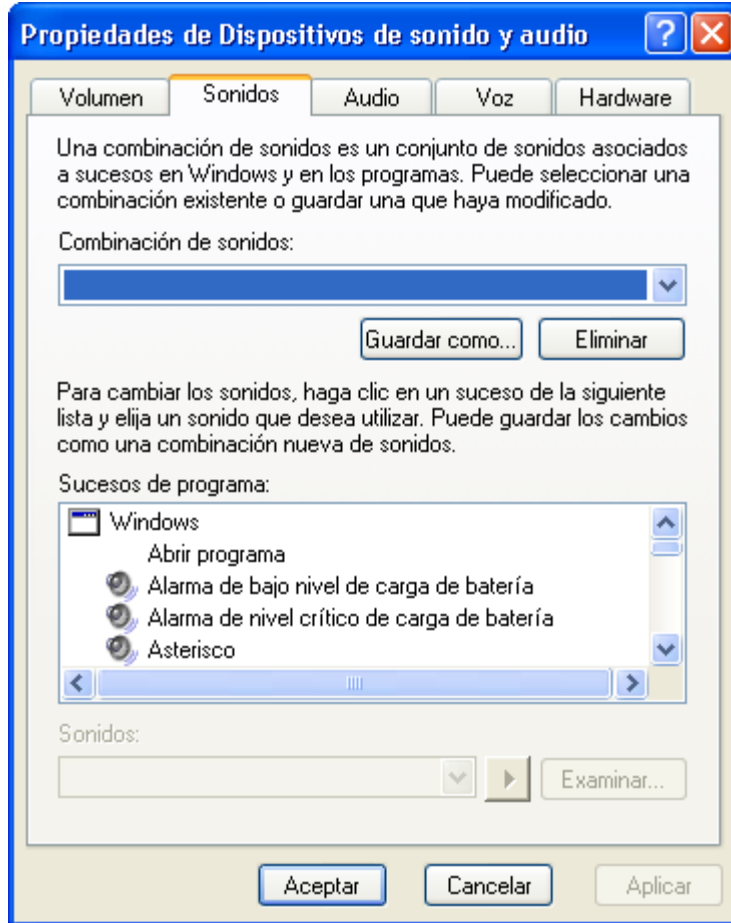
Si el idioma requerido se muestra como “disponible” en la casilla en parte derecha, haga clic en el mismo para seleccionarlo, y a continuación haga clic en “Aceptar”. Entonces deberá cerrar el programa y, la próxima vez que lo inicie, el idioma se habrá modificado.

Si el idioma deseado no se muestra como “disponible”, haga clic en “Para instalar idiomas adicionales...” Debajo de la casilla, después haga marque la casilla que aparece al lado del idioma que usted desea. Haga clic en “Siguiente” y los archivos adicionales del programa serán instalados. Cuando se haya completado, haga clic en “Finalizar”. Usted ahora puede seleccionar el idioma deseado según se describe más arriba.

Sonidos

En esta pantalla usted puede modificar los sonidos del programa o puede apagar el sonido completamente.

Si hace clic de nuevo en “Configuración”, aparecerá una pantalla en la que usted podrá modificar los ajustes de sonido para todos los programas de Windows. En la parte media inferior de la pantalla, hay una casilla llamada “Sucesos del programa” – véase más abajo.



Si hace clic en la flecha azul que indica hacia abajo en la parte derecha, a medio camino en la parte de abajo de la lista, encontrará los eventos de avast! antivirus a los que puede asignar sonidos. Si usted desea asignar un nuevo sonido a un evento, haga clic en el evento correspondiente y después en “Examinar”. De la lista de opciones disponibles, seleccione el sonido que desea y haga clic en “Aceptar”.

Después volverá a aparecer a la casilla que se muestra más arriba donde debería hacer clic en “Aplicar” y después en “Aceptar” otra vez.

Esto le llevará de vuelta a la pantalla principal de “Sonidos” donde usted debería hacer clic en “Aceptar” de nuevo para finalizar.

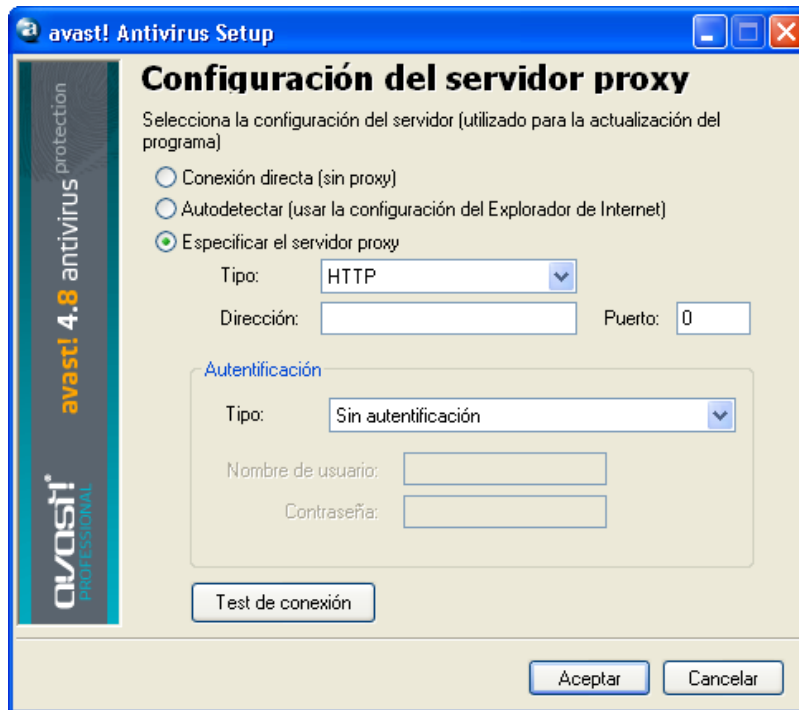
Actualizar (Conexiones)

En la pantalla, usted puede especificar el tipo de conexión a Internet marcando la casilla correspondiente i.e.

- Sólo me conecto a Internet utilizando un módem dial-up, o
- Mi ordenador está permanentemente conectado a Internet

Esto optimizará el camino en el que avast! busca nuevas actualizaciones y hará el proceso de actualización automática más fiable.

Una vez haya especificado el tipo de conexión, haga clic en el botón “Proxy”. Se abrirá una nueva ventana en la que usted podrá insertar los ajustes de su servidor proxy. Los ajustes del servidor proxy son importantes cuando avast! necesita acceder a Internet, e.g. durante las actualizaciones.



Si usted se conecta directamente a Internet (i.e. no a través de un proxy), lo cual por lo general se aplica a usuarios de dial-up, seleccione la opción “Conexión directa (sin proxy)”

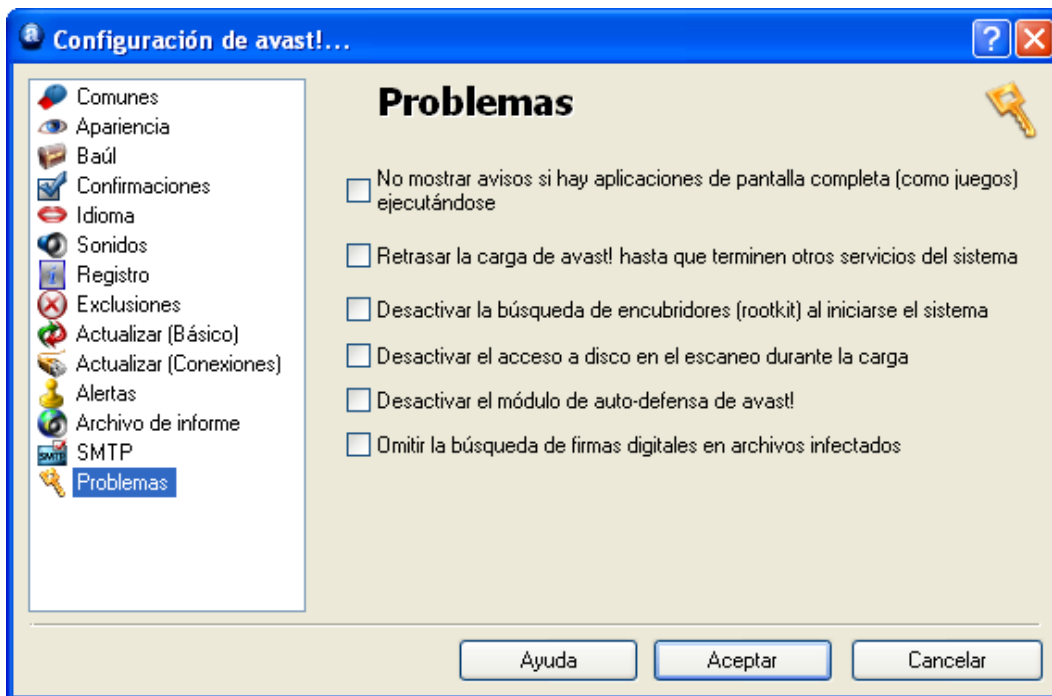
Si usted no está seguro de si su servidor es proxy, o cuál utiliza, seleccione “Autodetectar (usar la configuración del Explorador de Internet)”, o pregunte a su proveedor de Internet o administrador de red.

Si usted conoce la dirección y puerto de su servidor proxy, seleccione “Especificar el servidor proxy” e introduzca los detalles requeridos del proxy según se indica a continuación:

- **Tipo.** HTTP o SOCKS4
- **Dirección.** Introduzca la dirección de su servidor proxy.
- **Puerto.** Introduzca el puerto que utiliza su servidor proxy.
- **Autenticación.** Especifique aquí si el acceso a Internet a través de su servidor proxy requiere la autenticación del usuario, y si fuera necesario el tipo de autenticación.
- **Nombre de usuario y contraseña.** Estos datos deberían introducirse si fuesen requeridos para la autenticación.

Finalmente, haga clic en “Test de conexión” para comprobar si funciona la conexión a Internet (basada en los ajustes anteriores).

Problemas



Modificar los ajustes en esta página podría ayudar a resolver ciertos problemas específicos. Sin embargo, estos ajustes no se deberían modificar sin una buena razón. En caso de duda, por favor, póngase en contacto con avast!.

No mostrar avisos si hay aplicaciones de pantalla completa (como juegos) ejecutándose. Según su configuración de avast!, se pueden mostrar varios mensajes cuando esté utilizando su ordenador (e.g., cuando la base de datos de virus ha sido actualizada, cuando un correo entrante está siendo escaneado, etc.). Normalmente, los mensajes se muestran siempre que ocurre el evento correspondiente. Esto, sin embargo, puede dar lugar a la interrupción de aplicaciones en pantalla completa (e.g. juegos) - Windows cambia del modo

pantalla completa al modo de ventana normal cuando aparece el mensaje. Si usted selecciona esta opción, avast! intentará detectar si se está ejecutando alguna aplicación en pantalla completa antes de mostrar cualquier mensaje; si se encuentra una aplicación activa en pantalla completa, avast! no mostrará el mensaje.

Retrasar la carga de avast! hasta que terminen otros servicios del sistema.

El servicio avast! antivirus, por lo general, se inicia bastante pronto en el proceso de iniciación. Ocasionalmente, esto puede causar problemas al iniciar otros servicios del sistema - lo cual se podría manifestar e.g. como una congelación temporal (durante unos segundos o minutos) del sistema durante un corto periodo de tiempo después de haberse iniciado. Esta opción hace posible el retraso del inicio del servicio avast! antivirus hasta después de que los servicios del sistema se hayan cargado completamente.

Desactivar la búsqueda de encubridores (rootkit) al iniciarse el sistema.

avast! escanea los rootkits siempre que usted inicie el sistema operativo. Marque esta casilla si usted quiere desactivar este tipo de escaneo.

Desactivar el acceso a disco en el escaneo durante la carga.

Durante el escaneo al inicio, avast! utiliza un método especial de acceso al disco que permite al antivirus detectar incluso a aquellos virus que ocultan sus archivos. Aquí usted puede apagar esta característica - avast! utilizará el método usual de acceso al disco.

Desactivar el módulo de auto-defensa de avast!.

Algunos virus son capaces de apagar un software antivirus terminando sus procesos, borrando sus archivos críticos o modificando los mismos. avast! contiene propiedades de autodefensa que previenen estos ataques bloqueando las operaciones peligrosas. Para desactivar este módulo de autodefensa, marque esta casilla.

Omitir la búsqueda de firmas digitales en archivos infectados.

Para prevenir alertas de falsos positivos, avast! analiza si los ficheros infectados disponen de firmas digitales. Si se detecta un fichero infectado, pero también contiene una firma digital válida de una autoridad fiable (e.g. Microsoft), lo más probable es que se trate de un falso positivo - y avast! ignorará esta detección (falsa). Marcando esta casilla desactivará la selección adicional - avast! reportará todas las infecciones encontradas.

Cómo utilizar el escáner de la línea de comandos

El escáner de la línea de comandos de avast!, ashCmd.exe, normalmente se instala en el directorio C:\program files\alwil software\avast4.

Un escaneo se ejecuta desde la línea de comandos utilizando varios parámetros. Para ver una descripción de los parámetros, localice el archivo ashCmd y haga doble clic en él. Esto abrirá una nueva ventana en la que se visualizarán varios parámetros. También se puede encontrar una lista de todos los parámetros en la sección “Ayuda” de avast! en la carpeta “ashCmd Program”.

Para ejecutar un escaneo, vaya a su línea de comandos y escriba el nombre del programa ashCmd.exe seguido del área a ser escaneada y de los parámetros apropiados. Por ejemplo, para escanear todos los discos duros locales, la línea de comandos debería ser según se indica a continuación:

```
C:\Program Files\Alwil Software\Avast4 ashCmd.exe /*
```

Se pueden añadir parámetros adicionales. Para escanear un archivo concreto, escriba la ruta requerida, asegurándose de que cualquier nombre conteniendo espacios se indique entre comillas e.g.

```
C:\Program Files\Alwil Software\Avast4 ashCmd.exe c:"program files"
```

Para ejecutar una tarea particular, escriba el nombre del programa seguido de /@=<name of task>. Por ejemplo, para ejecutar una tarea llamada “Escaneo semanal”, la línea de comandos debería ser

```
C:\Program Files\Alwil Software\Avast4 ashCmd.exe /@=escaneo semanal
```

La tarea se ejecutará basándose en los parámetros establecidos para la tarea. Cualquier otro parámetro introducido en la línea de comandos, será ignorado.

Nota: si el nombre de la tarea contiene espacios, tiene que ser escrito entre comillas, por ejemplo para ejecutar una tarea llamada “Escaneo semanal de mis documentos”, la línea de comandos sería:

```
C:\Program Files\Alwil Software\Avast4 ashCmd.exe /@="Escaneo semanal de mis documentos"
```

Cuando el escaneo ha finalizado, los resultados se pueden transferir a un archivo utilizando el parámetro “/_>”. Por ejemplo, la línea de comandos: ashCmd.exe c:\windows /_> results.txt daría lugar al escaneo de la ruta c:\windows y guardaría los resultados del escaneo en un nuevo archivo llamado results.txt.

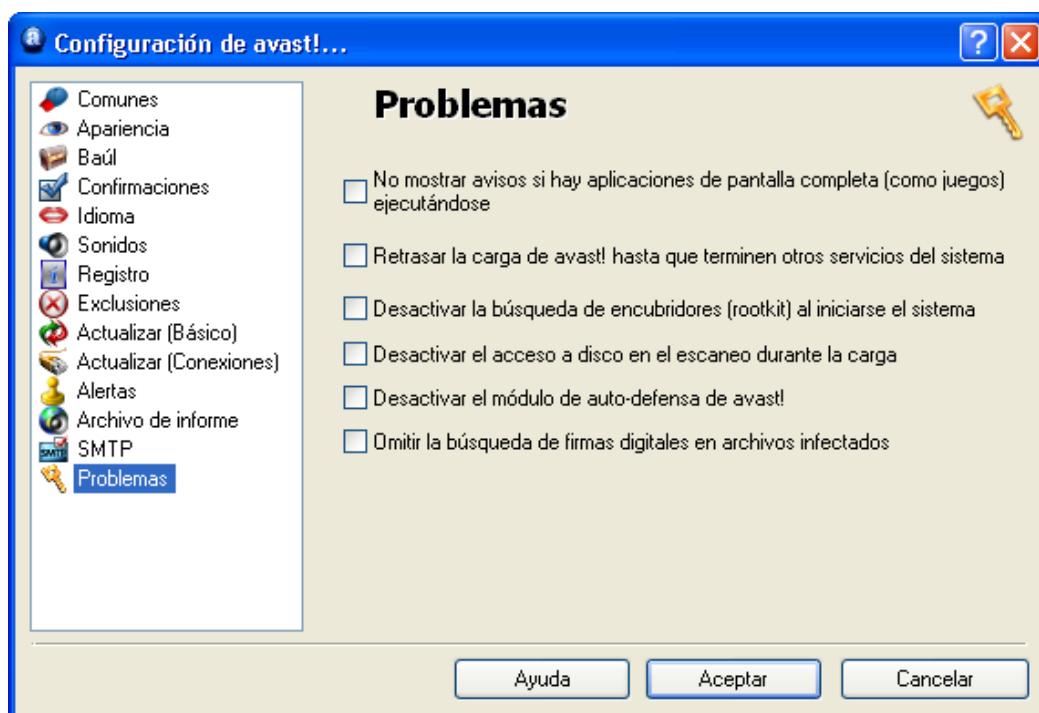
Cómo desinstalar avast! antivirus

Algunos virus están diseñados para apagar el software antivirus de un ordenador. Por lo tanto avast! antivirus ahora está protegido por un potente módulo de autodefensa (SD) que previene que sea modificado o borrado por tales virus. Sin embargo, una consecuencia de esto es que otros programas válidos también pueden encontrar más difícil cambiar o borrar avast! antivirus en comparación con las versiones anteriores. Para eliminar el programa avast! antivirus correctamente, es esencial seguir el procedimiento adecuado.

Antes de intentar desinstalar avast! antivirus, se recomienda cerrar cualquier otra aplicación que pueda estar ejecutando en su ordenador. Para desinstalar el programa avast! antivirus, el procedimiento recomendado es según se indica a continuación.

1. Apagar la Auto Defensa

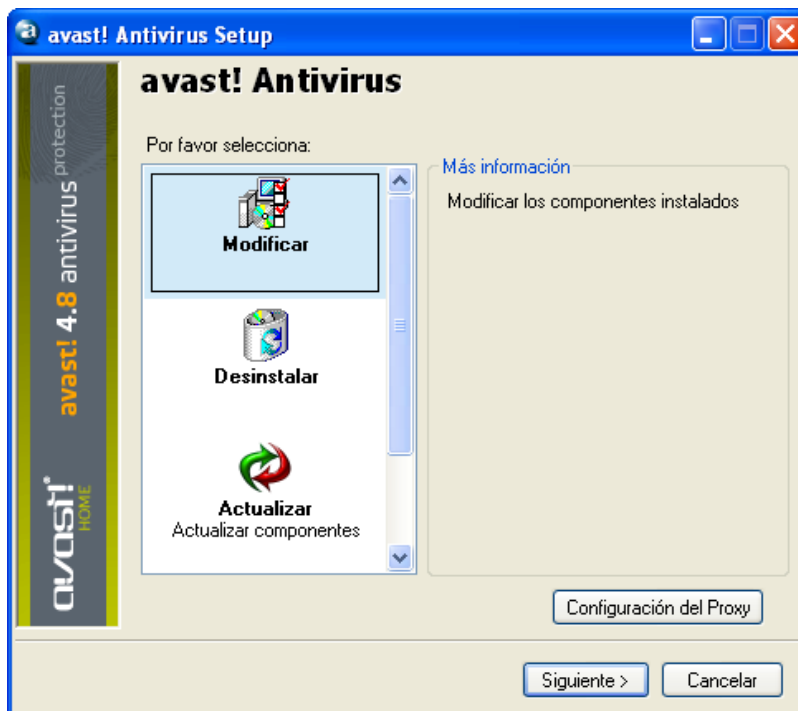
- Haga clic en el icono de la bola azul con la “a” en el medio en la esquina inferior derecha de la pantalla de su ordenador y seleccione la opción “Configuración del programa” en el menú de opciones.
- Haga clic en “Problemas” en la parte izquierda y la pantalla cambiará según se muestra más abajo



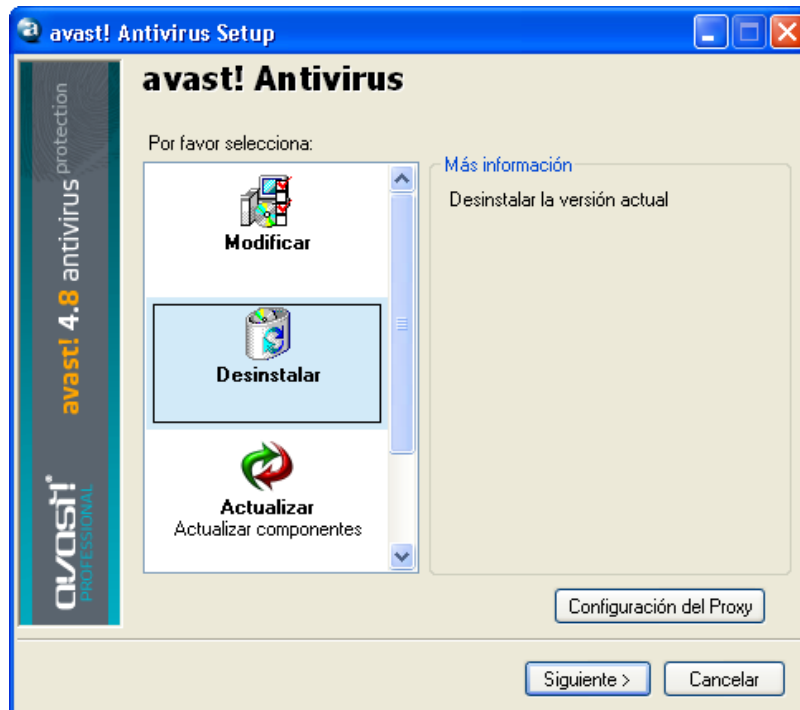
- Ahora seleccione la casilla “Desactivar el módulo de auto-defensa de avast!” y haga clic en “Aceptar”
- La auto-defensa ahora está apagada.

2. Eliminar el programa

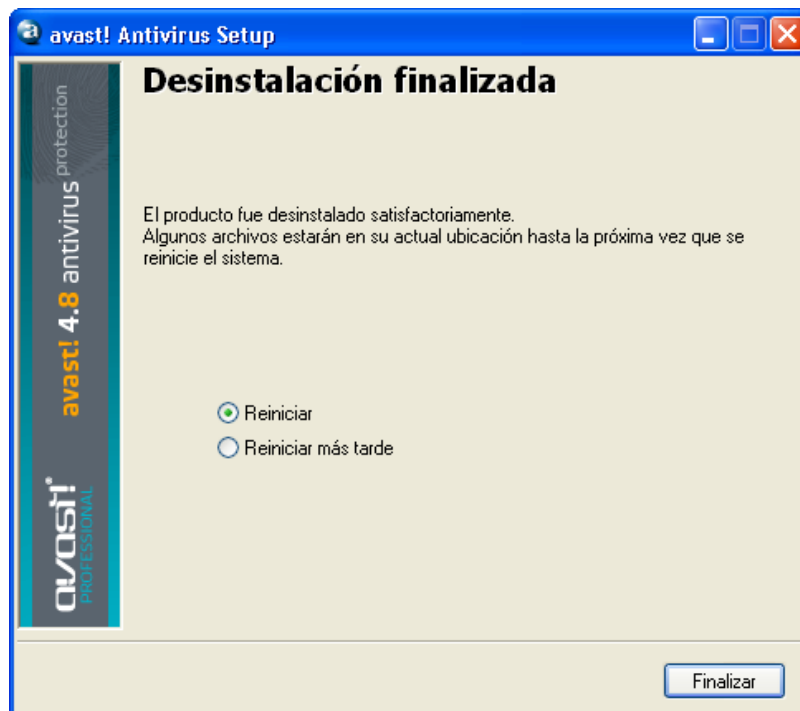
- Haga clic en “Inicio” en la esquina inferior izquierda de la pantalla de su ordenador y abra el panel de control de su ordenador. Si no puede encontrarlo en el Menú de Inicio, haga clic en Configuración y debería aparecer como una de las opciones.
- En el panel de control, haga clic en “Agregar o quitar programas”.
- Aparecerá una lista de todos los programas instalados actualmente.
- Seleccione “avast! antivirus” haciendo clic, y después haga clic en “Cambiar/Eliminar”
- Se mostrará la siguiente pantalla:



Haga clic en “Desinstalar” con lo que se seleccionará y después en “Siguiente”:



Ahora se desinstalará el programa, apareciendo la siguiente pantalla:



Para completar el proceso de desinstalación, es necesario reiniciar el ordenador. Con “Reiniciar” seleccionado, haga clic en “Finalizar” y su ordenador se reiniciará automáticamente.