

G DATA

# Security Software



# Índice de materias

<b>Primeros pasos</b>	<b>4</b>
+ ServiceCenter	
+ Instalación	
<b>Centro de seguridad</b>	<b>7</b>
+ Indicaciones de estado	
+ Licencia	
+ Módulos de software	
<b>Protección antivirus</b>	<b>12</b>
+ Comprobación de virus	
+ Archivos en cuarentena	
+ Soporte de arranque	
<b>Cortafuegos</b>	<b>14</b>
+ Estado	
+ Redes	
+ Conjuntos de reglas	
<b>Copia de seguridad</b>	<b>19</b>
+ Guardar y restaurar	
<b>Administrador de contraseñas</b>	<b>25</b>
+ Utilización del complemento para el navegador	
<b>Optimizador de sistema</b>	<b>27</b>
+ Restaurar	
+ Browser Cleaner	
<b>Protección infantil</b>	<b>29</b>
+ Crear nuevo usuario	
+ Contenidos prohibidos	
+ Contenidos permitidos	
+ Supervisar tiempo de uso de Internet	
+ Supervisar tiempo de uso del PC	
+ Filtros propios	
+ Ajustes: Registro	
<b>Cifrado</b>	<b>32</b>
+ Crear nueva caja fuerte	
+ Crear caja fuerte móvil	
+ Abrir caja fuerte móvil	
<b>Administrador de autoarranque</b>	<b>36</b>
+ Propiedades	
<b>Control de dispositivos</b>	<b>37</b>

---

<b>Ajustes</b>	<b>38</b>
+ General	
+ AntiVirus	
+ Cortafuegos	
+ Optimizador de sistema	
+ Control de dispositivos	
+ Copia de seguridad	
<b>Registros</b>	<b>58</b>
+ Registros de protección antivirus	
+ Registros de Cortafuegos	
+ Registros de Copia de seguridad	
+ Registros de protección antispam	
+ Registros de protección infantil	
+ Registros del control de dispositivos	
<b>FAQ: BootScan</b>	<b>59</b>
<b>FAQ: Funciones del programa</b>	<b>60</b>
+ Icono de seguridad	
+ Realizar comprobación de virus	
+ Alerta de virus	
+ Alerta de Cortafuegos	
+ Mensaje "no es un virus"	
+ Desinstalación	
<b>FAQ: Consultas sobre la licencia</b>	<b>64</b>
+ Licencias múltiples	
+ Extensión de la licencia	
+ Cambio de ordenador	
+ Copyright	

# Primeros pasos

Nos alegramos de que se haya decidido por nuestro producto y esperamos que esté totalmente satisfecho/a con su nuevo software G DATA. Si algo no funcionara correctamente en un primer momento, encontrará asistencia en nuestra documentación de ayuda. Para otras preguntas tiene a su disposición a nuestros expertos en el **ServiceCenter**.

**Nota:** Dentro del software, puede acceder en cualquier momento a la detallada ayuda del programa y obtener toda la información necesaria. Para ello, simplemente pulse dentro del programa el icono de ayuda representado.

## ServiceCenter

La instalación y el uso del software G DATA son sencillos e intuitivos. Si en algún momento se presentase algún problema, simplemente pónganse en contacto con los competentes empleados de nuestro ServiceCenter:

G DATA Latin America [www.gdatasoftware.com/latam](http://www.gdatasoftware.com/latam)

G DATA Spain [www.gdata.es](http://www.gdata.es)

## Instalación

Si su ordenador es totalmente nuevo o ha estado hasta ahora protegido por un software antivirus, puede efectuar la instalación siguiendo los pasos descritos a continuación. Pero si tiene motivos razonables para sospechar que su ordenador pudiera estar infectado, le recomendamos que antes de instalar el software lleve a cabo un análisis **BootScan**.

**Atención:** Si ha utilizado anteriormente un programa antivirus de otro fabricante, es necesario desinstalarlo por completo del ordenador. Debido a que los programas antivirus se incrustan a un nivel muy profundo en la estructura del sistema de Windows, es recomendable no conformarse únicamente con la desinstalación normal del software, sino utilizar también, si es posible, la herramienta de limpieza que el fabricante pone a su disposición en su centro de soporte online.

### Paso 1 - Comienzo de la instalación

Inicie la instalación del siguiente modo:

- **Instalación desde CD/DVD:** Para comenzar la instalación inserte el CD o DVD del programa.
- **Descarga de software:** Si ha descargado el software de Internet, para iniciar la instalación simplemente haga doble clic en el archivo descargado.

Se abrirá automáticamente una ventana de instalación.

**Nota:** Si la instalación no comienza inmediatamente: Es posible que no haya ajustado adecuadamente la función de autoarranque en su ordenador. Esta es la razón por la que el software no inicia automáticamente el proceso de instalación después de insertar el CD del programa y no se abre ninguna ventana con la que pueda instalar el software G DATA.

- Si en vez de esta ventana de instalación, se abre una de selección para la reproducción automática, haga clic en la opción **Ejecutar AUTOSTRT.EXE**.
- Si no se abre ninguna ventana de selección, busque en el Explorador de Windows el soporte de datos en el que esté el software G DATA y ejecute a continuación el archivo **Setup** o **Setup.exe**.

### Paso 2 - Selección del idioma

Ahora, seleccione el idioma con el que desea instalar su nuevo software G DATA.

### Paso 3 - Método de la instalación

Un asistente le acompañará durante la instalación del software en su ordenador. Ahora, seleccione si desea realizar una instalación estándar o una instalación definida por el usuario. Le recomendamos la instalación estándar.

**Iniciativa de información sobre malware:** En nuestro laboratorio G DATA SecurityLabs se investigan constantemente métodos y formas de proteger a los clientes de G DATA frente al malware (virus, gusanos y programas maliciosos) a los clientes de G DATA. La cantidad de información a disposición de nuestro laboratorio está en relación directamente proporcional con la efectividad de los mecanismos de protección desarrollados. No obstante, una gran cantidad de información sobre el malware se encuentra solo en los sistemas atacados o infectados. La Iniciativa de información sobre malware de G DATA tiene por objeto que también estos datos puedan tenerse en cuenta en

los análisis. Es por este motivo que, la información relativa a los programas dañinos se envía a G DATA SecurityLabs. Su participación activa es una contribución decisiva a que todos los clientes de G DATA puedan utilizar Internet con mayor seguridad. Durante la instalación del software G DATA puede decidir si desea enviar información a G DATA SecurityLabs o si prefiere no hacerlo.

**Nota:** En la instalación definida por el usuario puede seleccionar durante la instalación individualmente la ubicación de almacenamiento de los datos de programa y seleccionar o deseleccionar módulos del software (por ejemplo, la protección antispam).

## Paso 4 - Acuerdo de licencia

Lea a continuación el acuerdo de licencia y confirme que lo acepta.

## Paso 5 - Instalación definida por el usuario (opcional)

Si ha seleccionado la instalación definida por el usuario, ahora aparecerán dos ventanas de asistente en las que podrá definir el directorio de instalación del software y los módulos que desea instalar. Si ha elegido la instalación estándar, puede saltarse este paso.

- **Definido por el usuario:** Aquí podrá personalizar la instalación seleccionando los diferentes módulos del software que desee instalar (por ejemplo, antispam, etc.).
- **Completa:** Se instalan todos los módulos sin excepción.
- **Mínima:** Solo se instala el módulo AntiVirus, la protección antivirus básica del software G DATA.

**Actualizaciones:** A través de la configuración se pueden instalar en cualquier momento más módulos de programa o actualizar el software. Para ello, no tiene más que ejecutar de nuevo la instalación y seleccionar **Adaptar instalación** para ampliar o reducir los módulos. Si posee una nueva versión del programa y desea actualizar su versión, a través de la opción **Actualización definida por el usuario** puede elegir qué otros módulos desea seleccionar o deseleccionar.

## Paso 6 - Versión del software

Aquí también puede establecer si desea instalar la versión completa del programa o solo la versión de prueba. Si ha adquirido el software y posee un número de registro, debe seleccionar, por supuesto, la opción **Versión completa**. Para hacerse una idea del software G DATA de manera gratuita, puede utilizar simplemente nuestro acceso de prueba limitado.

## Paso 7 - Activación del producto

La activación del producto se realiza durante la instalación. Aquí puede activar su software.

- **Introducir nuevo número de registro:** Si instala por primera vez el software G DATA, seleccione esta opción y, a continuación, introduzca el número de registro que acompaña al producto. Dependiendo del tipo de producto encontrará este número, por ejemplo, en el dorso del manual de usuario, en el correo electrónico de confirmación al descargar el software o en el embalaje del producto.

**Nota:** Al introducir el número de registro se activa su producto y además se le envían por correo electrónico sus datos de acceso para el uso posterior.

- **Introducir los datos de acceso:** Si ya ha activado anteriormente el software G DATA, habrá recibido sus datos de acceso (nombre de usuario y contraseña). Para instalar nuevamente el software o para dar de alta otros ordenadores si ha adquirido una licencia múltiple, introduzca simplemente aquí sus datos de acceso.

**Nota:** Los datos de acceso los recibe exclusivamente por correo electrónico. En el producto no se encuentran datos de acceso.

Si no encuentra los datos de acceso o los ha olvidado, haga clic en la opción **¿Ha olvidado los datos de acceso?** en la sección de registro. Se abre una página web en la que debe introducir de nuevo su número de registro. Una vez hecho esto se le enviarán los datos de acceso a la dirección de correo que indicó en el registro. Si desde entonces hubiera cambiado su dirección de correo electrónico, diríjase a nuestro **ServiceCenter**.

- **Activar más tarde:** Si solo desea echar un vistazo al software, también podrá instalarlo sin necesidad de introducir ningún tipo de datos. Tenga en cuenta que en este caso el programa no se actualizará a través de Internet, y por tanto no le ofrecerá una protección en tiempo real contra el software malicioso. Puede introducir su número de registro o sus datos de acceso posteriormente, cuando realice una actualización.

## Paso 8 - Conclusión de la instalación

Para finalizar la instalación es necesario reiniciar el ordenador. Después ya tiene el software G DATA listo para usarlo.

## Después de la instalación

Después de la instalación podrá iniciar el software G DATA recién instalado seleccionando el icono de programa en la barra de tareas. Además, ahora tiene disponibles otras funciones de seguridad adicionales en su ordenador:



**Icono de seguridad:** El software G DATA protege permanentemente su ordenador frente al malware y los ataques de virus. Un símbolo en la barra de tareas de su ordenador le avisará de inmediato cuando el software considere necesaria una intervención por parte del usuario. Si hace clic con el botón derecho del ratón en el icono, podrá abrir la interfaz del programa G DATA. Para más información consulte el capítulo [Icono de seguridad](#).



**Destructor de datos:** Si durante la instalación seleccionó la opción del destructor de datos (no integrado en G DATA Antivirus), lo encontrará como icono en el escritorio. Los datos que mueva al destructor de datos se eliminarán de manera tal que no podrán ser restaurados ni siquiera con la ayuda de herramientas profesionales de recuperación. Para ello se sobrescriben los datos un número de veces que se puede definir libremente. Puede acceder a los ajustes haciendo clic con el botón derecho sobre el icono del destructor y abriendo las propiedades.





**Comprobación rápida:** Con la comprobación rápida se podrán analizar los archivos de manera muy sencilla sin necesidad de tener que iniciar el software. Marque simplemente los archivos o carpetas, por ejemplo, con el ratón en el Explorador de Windows. Pulse ahora el botón derecho del ratón y en la ventana de diálogo que aparece seleccione la opción **Comprobación de virus**. A continuación se lleva a cabo un examen de virus automático en el archivo correspondiente.

**Tras la instalación del software, su ordenador se inicia de manera distinta a lo usual:** Esto puede deberse a que el CD del programa aún se encuentra dentro de la unidad de disco. Retire simplemente el CD e inicie nuevamente su ordenador de la manera habitual.

# Centro de seguridad

Solo necesitará entrar en el Centro de seguridad cuando quiera acceder activamente al control antivirus o a una de las numerosas funciones adicionales del programa. La protección en sí de su ordenador frente a los virus y otras amenazas se realiza de manera permanente en segundo plano. En los casos en los que el software requiera una intervención se le recordará automáticamente mediante informaciones que figuran en la barra de tareas de su ordenador.




## Estado de seguridad

-  Si todo está marcado con una marca de verificación verde, su sistema está protegido.
-  Un signo de exclamación rojo indica que su sistema se enfrenta a un peligro inminente. En ese caso debe adoptar medidas inmediatas para asegurar que la protección de sus datos siga activa.
-  Si se muestra el icono de comodín, esto significa que no ha activado la función de seguridad correspondiente (por ejemplo, la protección antispam).
-  Un icono amarillo indica que es necesaria una pronta intervención por parte del usuario. Esto sucede, por ejemplo, cuando existe una actualización del software.

Puede utilizar todas las funciones y los áreas del programa (como por ejemplo, la **protección antivirus** o los **ajustes**), si desea profundizar en la gestión de la seguridad del sistema, pero no tiene necesariamente que hacerlo. Usted decide en qué medida quiere implicarse activamente en la protección antivirus y la salvaguardia de datos. Dispone de una extensa ayuda de uso del programa dentro del software.

## Funciones generales

Los siguientes símbolos le indican el estado de seguridad de cada una de las distintas áreas.

-  **Ajustes:** Mediante este botón situado arriba a la derecha puede acceder a todas las ventanas de diálogo de ajustes de las diferentes áreas del software. En cada área también tiene la posibilidad de seleccionar directamente la ventana de diálogo de ajustes correspondiente.
-  **Registros:** El software muestra aquí los registros actuales de todas las acciones realizadas (comprobación de virus, actualización, virus detectados, etc.).
-  En la parte superior derecha, en el encabezado del software, encontrará también las siguientes funciones:
  - Mostrar ayuda:** Puede iniciar en cualquier momento la completa ayuda del programa que ofrece el software. Para ello, simplemente pulse dentro del programa el botón de ayuda representado.
  - Actualizar programa:** Cuando hay disponibles nuevas versiones de programa las puede actualizar cómodamente con un clic, igual que las informaciones de virus. Es decir, cuando le llegue la información de que hay una actualización disponible, haga clic simplemente en Actualizar programa. Encontrará información más completa en el capítulo: [Actualizaciones](#)
  - Información:** Aquí obtendrá información sobre la versión del programa. Si contacta con el [ServiceCenter](#) estas informaciones pueden ser muy útiles.

## Indicaciones de estado

Las siguientes indicaciones de estado le informan sobre el estado de seguridad de su sistema. Pulsando estas entradas puede iniciar de inmediato medidas para mejorar el estado de seguridad:

### Protección en tiempo real

La protección en tiempo real del Vigilante de virus comprueba su ordenador constantemente en busca de virus, controla los procesos de escritura y lectura y, en cuanto un programa intenta ejecutar una función dañina o desea propagar archivos maliciosos, el Vigilante lo bloquea. ¡El Vigilante de virus es su protección más importante! Nunca debe estar desactivado.

- **Desactivar el Vigilante de virus:** Si, de todos modos, desea desactivar alguna vez el Vigilante de virus, lo puede hacer aquí. Si su objetivo es optimizar el rendimiento de su ordenador desactivando el Vigilante, no deje de comprobar si no puede obtener el mismo resultado modificando la configuración. Al desactivar el Vigilante de virus tiene la opción de acceder a las modificaciones

correspondientes de la configuración. Pulse [Cambiar seguridad / rendimiento](#) y siga las indicaciones del capítulo con el mismo título de la ayuda. De todas maneras siempre le queda la alternativa de desactivar completamente el Vigilante de virus.

- **Desactivar supervisión de conducta:** La supervisión de conducta consiste en un sistema inteligente de reconocimiento del malware desconocido que ofrece una protección adicional independiente de las firmas de virus. Conviene tener siempre activada la supervisión de conducta.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiVirus | Protección en tiempo real](#).

## Último escaneo en modo reposo

Aquí se muestra la última vez en que su ordenador fue examinado en su totalidad para detectar posibles virus. Cuando esta entrada está marcada en rojo significa que debe realizar lo antes posible una comprobación de virus.

- **Comprobar PC:** Si tiene tiempo y durante unas horas no va a usar el ordenador para trabajar, puede iniciar aquí directamente una comprobación completa del ordenador. Puede seguir usando el ordenador durante este intervalo, pero puede ser que otras aplicaciones reaccionen más despacio porque la comprobación de virus se realiza con este ajuste con el máximo rendimiento. Encontrará más información sobre este aspecto en el capítulo [Comprobación de virus](#).
- **Iniciar ahora escaneo en modo reposo:** El escaneo en modo reposo se inicia automáticamente en las fases en las que su ordenador está inactivo y, de este modo, realiza un análisis de todo el ordenador de forma automática en intervalos regulares. Si desea iniciar el escaneo en modo reposo antes de la próxima fecha fijada automáticamente, seleccione la opción **Iniciar ahora escaneo en modo de reposo**. Si no desea que el software G DATA inicie automáticamente el escaneo en modo reposo durante sus pausas de trabajo, puede desactivar esta función en la opción **Desconectar el escáner en modo reposo** (no se recomienda).

## Cortafuegos

Un Cortafuegos protege su ordenador del *espionaje* desde el exterior. Examina los datos y los programas que llegan a su ordenador procedentes de Internet o de la red y los datos que su PC transfiere al exterior. En cuanto encuentra algún indicio de que se van a grabar o descargar datos de modo ilícito en su ordenador, el Cortafuegos le alerta sobre este hecho y bloquea el intercambio de datos no autorizado. Este módulo está disponible en las versiones del programa G DATA Internet Security y G DATA Total Security.

- **Desactivar Cortafuegos:** En caso de necesidad también se puede desactivar el Cortafuegos. Su ordenador sigue conectado a Internet y otras redes, pero el Cortafuegos ya no le sirve de escudo frente a los ataques o intentos de espionaje (no se recomienda).
- **Desactivar piloto automático:** Por regla general, es conveniente tener el Cortafuegos funcionando en modo **Piloto automático**. El programa se ejecuta, como si dijéramos, en segundo plano y le protege sin que tenga que llevar a cabo grandes ajustes. Cuando emplee el Cortafuegos sin el piloto automático, en los casos de duda aparecerá una ventana de diálogo en la que podrá optimizar el Cortafuegos adaptándolo poco a poco a su entorno de sistema. Para los usuarios experimentados, ésta es una función muy útil. Normalmente, no se recomienda desconectar el piloto automático.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | Cortafuegos | Automaticidad](#).

## Protección Web

En esta área puede activar y desactivar la protección Web. La protección Web es un módulo que durante la navegación en Internet y las descargas reconoce automáticamente las amenazas y, en caso de ser necesario, las neutraliza. Sirve como apoyo útil al Vigilante de virus y bloquea las páginas Web y descargas dañinas, antes de que puedan ser abiertas.

Si el software G DATA detecta que una página de Internet es una amenaza y la bloquea, la página no se carga y en su lugar se visualiza una página informativa de G DATA en el navegador.

- **Desactivar protección Web:** Si desactiva la Protección Web puede obtener por ej., una ventaja en el tiempo de descarga de grandes paquetes de datos de una fuente segura. Fundamentalmente, su ordenador está protegido también sin la protección Web por medio del Vigilante de virus. No obstante, sólo debería prescindir de la protección Web en casos excepcionales.
- **Definir excepciones:** La protección web se encarga de evitar que caiga víctima de páginas web infectadas o engañosas. En raras ocasiones puede ocurrir que la página web no se visualice correctamente aunque provenga de un proveedor seguro. En estos casos, puede agregar la URL a la Lista blanca, es decir puede definirla como excepción, con lo que la protección web ya no bloqueará más este sitio. Lea en el capítulo [Definir excepciones](#) cómo se realiza esto.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiVirus | Protección Web](#).

## Comprobación de correo electrónico

La comprobación de correo electrónico le permite explorar los emails entrantes y salientes y sus archivos adjuntos y eliminar directamente



las posibles infecciones. Cuando el software encuentra un virus, puede borrar directamente los archivos adjuntos o reparar los archivos infectados.

- **Desactivar la comprobación de correo electrónico:** Si no desea que el software G DATA compruebe su correo electrónico, desactive esta opción. Desactivar esta función, no obstante, representa un alto riesgo para la seguridad y sólo debería realizarse en casos excepcionales.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiVirus | Comprobación de correo](#).

**Microsoft Outlook:** Aquí, los emails se escanean mediante un plugin. Esta función proporciona la misma protección que la protección basada en POP3/IMAP que se encuentra en las opciones de AntiVirus. Después de instalar este plugin encontrará la función **Comprobar carpeta** en el menú Herramientas de Outlook. Con esta función puede revisar cada una de sus carpetas de correos para detectar si tienen virus.

## Protección antispam

Promociones, publicidad, newsletter: la avalancha de correos electrónicos no deseados sigue creciendo. ¿Está su buzón lleno a rebosar por culpa de las enormes cantidades de correo electrónico no deseado? El software G DATA le protege de forma segura contra los correos basura (spam), bloquea eficientemente los remitentes fraudulentos y evita las falsas alarmas gracias a la combinación de los más modernos criterios de verificación de spam. Este módulo está disponible en las versiones G DATA Internet Security y G DATA Total Security.

- **Registro: Spam:** Aquí encontrará una lista detallada de los correos que el software G DATA ha definido como spam. Con el botón **Actualizar** puede consultar el estado actual de datos y con el botón **Borrar** puede eliminar todas las entradas marcadas hasta el momento. Los correos electrónicos que hayan entrado en su programa de correo naturalmente no se borrarán. El botón **En lista blanca** le permite incluir en la lista blanca un correo marcado, excluyendo así la dirección de correo correspondiente de los futuros análisis antispam. El botón **En lista negra** le permite incluir en la lista negra un correo marcado, cuya dirección de correo electrónico pasará a analizarse siempre y de modo especial para detectar elementos de spam.
- **Registro: Sin spam:** Aquí encontrará una lista detallada de los correos que el software G DATA no ha definido como spam. Con el botón **Actualizar** puede consultar el estado actual de datos y con el botón **Borrar** puede eliminar todas las entradas marcadas hasta el momento. Los correos electrónicos que hayan entrado en su programa de correo naturalmente no se borrarán. El botón **En lista blanca** le permite incluir en la lista blanca un correo marcado, excluyendo así la dirección de correo correspondiente de los futuros análisis antispam. El botón **En lista negra** le permite incluir en la lista negra un correo marcado, cuya dirección de correo electrónico pasará a analizarse siempre y de modo especial para detectar elementos de spam.
- **Editar lista blanca:** Mediante la lista blanca puede excluir de forma explícita de la sospecha de spam determinadas direcciones de remitentes o dominios. Simplemente, pulse el botón **Nuevo** e indique en el campo **Remitente / dominio del remitente** la dirección de correo electrónico (p. ej., newsletter@paginainformativa.es) o el dominio (p. ej., paginainformativa.es) que desea excluir de la sospecha de spam, y el software G DATA considerará que los correos electrónicos de este remitente o dominio del remitente no son spam. Con el botón **Importar** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista blanca. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **Exportar** también puede exportar la lista blanca como archivo de texto.
- **Editar lista negra:** Mediante la lista negra puede categorizar determinadas direcciones de remitentes o dominios explícitamente como sospechosos de spam. Simplemente, pulse el botón **Nuevo** e introduzca en el campo **Remitente / dominio del remitente** la dirección de correo (p. ej., newsletter@megaspam.de.vu) o el dominio (p. ej., megaspam.de.vu) que desea considerar bajo sospecha de spam, y el software G DATA tratará, por norma general, los correos electrónicos de este remitente o dominio como correos con probabilidad muy alta de spam. Con el botón **Importar** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista negra. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **Exportar** también puede exportar la lista negra como archivo de texto.
- **Desactivar protección antispam:** Aquí puede desactivar la protección antispam de su ordenador, en caso de ser necesario, por ej. si no ha instalado ningún programa de correo en su ordenador.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiSpam | Filtro antispam](#).

## Última actualización

Aquí se muestra la última vez que su ordenador recibió firmas de virus procedentes de Internet. Cuando esta entrada está marcada en rojo significa que debe realizar lo antes posible una actualización de virus. Simplemente haga clic en la entrada y a continuación seleccione la opción **Actualizar firmas de virus**.

- **Actualizar firmas de virus:** Normalmente, las actualizaciones de las firmas de virus se realizan de manera automática. Si desea

obtener una actualización inmediatamente, entonces haga clic sobre este botón.

- **Desactivar actualizaciones automáticas:** Si no desea que el software G DATA se ocupe de manera automática de actualizar las firmas de virus a su estado más actual, desactive esta opción. Desactivar esta función, no obstante, representa un alto riesgo para la seguridad y sólo debería realizarse en casos excepcionales.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiVirus | Actualizaciones](#).

## Próxima actualización

En esta entrada podrá ver cuándo se realizará la próxima actualización. Si desea realizar inmediatamente una actualización, simplemente haga clic en la entrada y a continuación seleccione la opción **Actualizar firmas de virus**.

- **Actualizar firmas de virus:** Normalmente, las actualizaciones de las firmas de virus se realizan de manera automática. Si desea obtener una actualización inmediatamente, entonces haga clic sobre este botón.
- **Desactivar actualizaciones automáticas:** Si no desea que el software G DATA se ocupe de manera automática de actualizar las firmas de virus a su estado más actual, desactive esta opción. Desactivar esta función, no obstante, representa un alto riesgo para la seguridad y sólo debería realizarse en casos excepcionales.
- **Otros ajustes:** Encontrará más información en el capítulo [Configuración | AntiVirus | Actualizaciones](#).

## BankGuard

Los troyanos bancarios se están convirtiendo en una amenaza cada vez más grave. En cuestión de horas, los cibercriminales desarrollan nuevas variantes de malware (por ejemplo, Zeus, SpyEye) para robarle su dinero. Los bancos se ocupan de la seguridad del tráfico de datos en Internet, pero estos datos se descodifican en el navegador y justo aquí es donde atacan los troyanos bancarios. La tecnología puntera de G DATA BankGuard asegura las transacciones bancarias desde el principio y las protege inmediatamente allí donde se produce el ataque. G DATA BankGuard comprueba la autenticidad de las bibliotecas de red usadas, asegurando así que ningún troyano bancario llegue a manipular el navegador de Internet. Se recomienda dejar activada la protección de G DATA BankGuard.

## Protección frente a keyloggers

La protección frente a keyloggers vigila también, independientemente de las firmas de virus, si en su sistema se están espiando las pulsaciones de teclado. De esta forma se evita que los atacantes puedan también registrar sistemáticamente la introducción de contraseñas. Esta opción debe permanecer siempre activada.

## Exploit Protection

El llamado exploit aprovecha las vulnerabilidades de las aplicaciones habituales y, en el peor de los casos, puede llegar a tomar el control de su ordenador sirviéndose de estas vulnerabilidades. Los exploits pueden atacar incluso si se actualizan regularmente las aplicaciones (como p. ej. lector de PDF, navegador, etc.). Exploit Protection le protege contra estos accesos, y también de forma proactiva contra ataques hasta ahora desconocidos.

## Licencia

Debajo del campo **Licencia** situado en la parte izquierda de la interfaz del programa se ve el periodo de validez que le queda a su licencia para realizar actualizaciones de virus. No hay ningún otro software donde las actualizaciones muy frecuentes sean tan importantes como en el software antivirus. Por eso, antes de que caduque su licencia, el software le recuerda automáticamente que la renueve. Lo mejor, más cómodo y sencillo es hacerlo vía Internet.

## Mostrar información sobre la licencia

Si en el área de licencia hace clic sobre el campo de información, aparece un cuadro de diálogo en el que puede visualizar su nombre de usuario o clave de licencia. Si alguna vez tiene alguna pregunta acerca de su licencia, con esta información podemos ayudarle en el [Centro de servicios G DATA](#) de forma más precisa. Si alguna vez olvida su contraseña, usando este cuadro de diálogo también puede generar de forma rápida y sencilla una contraseña nueva.

# Módulos de software

Tiene disponibles los siguientes módulos, en función de la versión de software instalada:



**Centro de seguridad:** Su centro de seguridad personal. Aquí obtendrá toda la información necesaria para proteger su ordenador frente al malware, para que pueda reaccionar de forma idónea frente a las amenazas.



**Protección antivirus:** En este área obtendrá información sobre cuándo fue la última vez en que se comprobó si su ordenador estaba infectado y si el Vigilante de virus le está protegiendo ahora de las infecciones. Además podrá comprobar directamente si el ordenador o soporte de datos está infectado con software dañino, tratar los archivos infectados en la cuarentena y crear un soporte de arranque.



**Cortafuegos:** Un Cortafuegos protege su ordenador del espionaje desde el exterior. Examina los datos y los programas que llegan a su ordenador procedentes de Internet o de la red y los datos que su PC transfiere al exterior. En cuanto encuentra algún indicio de que se van a grabar o descargar datos de modo ilícito en su ordenador, el Cortafuegos le alerta sobre este hecho y bloquea el intercambio de datos no autorizado. Este módulo de software está disponible en las versiones del programa G DATA Internet Security y G DATA Total Security.



**Copia de seguridad:** Con el avance de la digitalización de la vida diaria, la utilización de servicios de música en línea, cámaras digitales y correo electrónico, cada vez es más importante garantizar la seguridad de los datos personales. Ya sea debida a errores de hardware, a un descuido o a un daño causado por virus o ataques de hackers: sus documentos privados deben guardarse de forma regular. El módulo de Copia de seguridad se encarga de esta tarea y protege tanto documentos como archivos importantes sin que usted tenga que preocuparse constantemente de ello. Este módulo de software está disponible en la versión del programa G DATA Total Security.



**Optimizador de sistema:** Con este optimizador de sistema tiene a mano una herramienta que hace que su sistema Windows sea bastante más rápido y fácil de comprender con recordatorios automáticos para las actualizaciones de Windows, la desfragmentación periódica programada o la eliminación con regularidad de las entradas de registro innecesarias y los archivos temporales. Este módulo de software está disponible en la versión del programa G DATA Total Security.



**Protección infantil:** Con la protección infantil puede regular las pautas de navegación en Internet y el uso del PC por parte de sus hijos. Este módulo de software está disponible en las versiones del programa G DATA Internet Security y G DATA Total Security.



**Cifrado:** El módulo de cifrado actúa como una caja fuerte de un banco para proteger los datos sensibles. Se puede utilizar una caja fuerte, por ejemplo, adicional, como otra partición de disco duro, y es muy fácil de operar. Este módulo de software está disponible en la versión del programa G DATA Total Security.



**Administrador de autoarranque:** Con el Administrador de autoarranque se pueden administrar los programas que arrancan automáticamente al iniciarse Windows. Normalmente, estos programas se cargan directamente al iniciar el sistema. Si se pueden administrar con el Administrador de autoarranque, pueden también iniciarse con demora o en función del grado de ocupación del sistema o del disco duro. Esto permite un arranque más rápido del sistema, mejorando así el rendimiento del ordenador.



**Control de dispositivos:** Mediante esta opción puede limitar el uso de dispositivos, como soportes de datos intercambiables, unidades de CD/DVD y unidades de disquete, para determinados usuarios de su ordenador. De este modo puede impedir, por ejemplo, la exportación o importación no deseada de datos o la instalación de software. Ahora también con USB KeyboardGuard. Puede encontrar más información sobre este tema en el capítulo Control de dispositivos.

# Protección antivirus

Con este módulo puede examinar selectivamente si su ordenador o los soportes de datos seleccionados están infectados con malware. Esta operación se recomienda si recibe, por ejemplo, de amigos, familiares o compañeros CDs o memorias USB de grabación casera. La comprobación de virus también está indicada al instalar nuevos programas y en las descargas de Internet.

**Atención:** La comprobación del ordenador o del soporte de datos seleccionados constituye una protección complementaria. En términos generales, el escaneo en modo reposo de G DATA y el Vigilante de virus de G DATA, que permanece siempre activo en segundo plano, le protegen perfectamente del software dañino. Una comprobación de virus encontraría también virus que se hayan copiado en su ordenador antes de instalar en él el software G DATA o que entraron cuando el Vigilante de virus no estaba activo.

## Comprobación de virus

Seleccione aquí el área de su ordenador o el soporte de datos que desea comprobar de forma selectiva:



**Analizar PC (todos los discos duros locales):** Si desea revisar su ordenador mediante el escaneo en modo reposo, independientemente de la comprobación automática (por ejemplo, porque sospecha momentáneamente de un virus en concreto), sólo tiene que pulsar esta entrada. A continuación, el programa examina su ordenador para detectar una infección por virus. Para más información consulte también el siguiente capítulo: [Realizar comprobación de virus](#)



**Comprobar memoria y autoinicio:** Mediante esta función se escanean los archivos de programa y las DLL (bibliotecas de programa) para todos los procesos en ejecución. De este modo, los programas maliciosos se pueden eliminar directamente de la memoria y del área de autoarranque. Los virus activos se pueden eliminar directamente, sin tener que comprobar todo el disco duro. Esta función sirve como operación adicional y no reemplaza la exploración de virus regular de los datos almacenados.



**Analizar los directorios/archivos:** Esta opción permite escanear los discos, directorios o ficheros seleccionados en busca de virus. Si hace clic en esta acción, se abre una selección de directorios y archivos. Aquí puede comprobar si existen virus en ciertos archivos y también en directorios completos. Si hace clic en los signos "más" del árbol de directorios, podrá seleccionar y abrir directorios, y en la vista de archivos pueden visualizarse sus contenidos. A continuación, el software procederá a escanear los directorios y archivos que haya marcado.

Si en un directorio no se comprueban todos los archivos, aparecerá marcado con una marca de verificación gris.



**Analizar soportes intercambiables:** Con esta función puede comprobar si hay virus en discos CD-ROM o DVD-ROM, tarjetas de memoria o lápices USB. Al hacer clic en esta acción, se comprueban todos los soportes intercambiables que estén conectados al ordenador (también los CD y tarjetas de memoria insertados, los discos duros conectados vía USB o los lápices USB). Tenga en cuenta que el software no podrá eliminar los virus de los soportes que no permitan un acceso de escritura (p. ej., discos CD-ROM grabados). En este caso, los virus encontrados se listan en un registro.



**Comprobar la existencia de rootkits:** Los rootkits intentan soslayar los métodos convencionales de detección de virus. Con esta opción puede buscar específicamente virus rootkits sin tener que realizar una comprobación completa del disco duro y de los datos guardados.

## Archivos en cuarentena

Hay varios modos de tratar los virus detectados durante una exploración. Una opción es poner en cuarentena el archivo infectado. La cuarentena es una zona segura del software donde los archivos son cifrados y almacenados para que no puedan transferir el virus a otros archivos.



**Visualizar cuarentena:** Al pulsar este botón se abre el área de cuarentena.

Los archivos en cuarentena se almacenan en el mismo estado en el que el software G DATA los encontró y más tarde podrá decidir qué hacer con ellos.

- **Actualizar:** Si, en alguna ocasión, dejase la ventana de diálogo de la cuarentena abierta durante un tiempo y en este intervalo se detecta un virus y se mueve a la cuarentena (por ejemplo, el Vigilante se encarga de ello automáticamente), con este botón puede actualizar la vista.
- **Enviar:** En ciertos casos, un archivo infectado que no haya podido desinfectar, puede enviarlo vía Internet a G DATA. El contenido de este archivo se tratará por supuesto de forma totalmente confidencial. Los resultados de su examen sirven para mejorar y

actualizar las firmas de virus y el software.

**Iniciativa de información sobre malware:** En nuestro laboratorio G DATA SecurityLabs se investigan constantemente métodos y formas de proteger del malware (virus, gusanos y programas maliciosos) a los clientes de G DATA. La cantidad de información a disposición de nuestro laboratorio está en relación directamente proporcional con la efectividad de los mecanismos de protección desarrollados. No obstante, una gran cantidad de información sobre el malware se encuentra solo en los sistemas atacados o infectados. La Iniciativa de información sobre malware de G DATA tiene por objeto que estos datos también puedan tenerse en cuenta en los análisis. Es por este motivo que, la información relativa a los programas dañinos se envía a G DATA SecurityLabs. Su participación activa es una contribución decisiva a que todos los clientes de G DATA puedan utilizar Internet con mayor seguridad.

- **Desinfectar:** Muchas veces no es demasiado tarde para salvar los archivos infectados. En esos casos, el software elimina los componentes del virus del archivo y reconstruye el archivo original libre de virus. Si el proceso de desinfección tiene éxito, el archivo será restaurado automáticamente en la ubicación donde estaba almacenado antes de realizar la exploración de virus y estará disponible de nuevo.
- **Recuperar:** Hay ocasiones en que puede ser necesario sacar de la cuarentena un archivo infectado que no sea posible desinfectar y devolverlo a su lugar de origen. La recuperación puede hacerse, p. ej., para salvar datos. Esta función sólo debe ejecutarse en casos excepcionales y adoptando medidas de seguridad estrictas (por ejemplo, desconectar el ordenador de Internet o de la red, hacer una copia de seguridad previa de los datos no infectados, etc.).
- **Eliminar:** Si ya no necesita el archivo infectado, puede simplemente borrarlo de la cuarentena.

## Soporte de arranque

El soporte de arranque es una herramienta muy útil cuando se trata de limpiar de virus los ordenadores ya infectados. Justo en los ordenadores que no tuvieran ningún antivirus antes de instalar el software G DATA se recomienda utilizar un soporte de arranque. La forma de usar el **soporte de arranque** se explica en el capítulo [BootScan](#).



Para crear un soporte de arranque solo tiene que pulsar el botón **Crear soporte de arranque** e ir siguiendo las instrucciones del asistente de instalación. Aquí tiene la posibilidad de descargarse las firmas de virus actuales, para que su soporte de arranque esté al día. Además, puede elegir si quiere grabar un CD o DVD como soporte de arranque o si quiere usar una memoria USB para este fin.

**Restauración de copia de seguridad:** Si usa la versión del programa G DATA Total Security, con un soporte de arranque puede restaurar una copia de seguridad de la unidad de disco también en el volumen en que se encuentra actualmente el sistema. También es posible restaurar una copia de seguridad de una unidad o un archivo en otros destinos. Para ello, inserte el soporte de arranque y seleccione la función **G DATA Backup (restaurar)**.


# Cortafuegos

Un Cortafuegos protege su ordenador del *espionaje* desde el exterior. Examina los datos y los programas que llegan a su ordenador procedentes de Internet o de la red y los datos que su PC transfiere al exterior.

En el módulo de Cortafuegos tiene tres áreas disponibles:

- **Estado:** En el área de estado del Cortafuegos encontrará información básica sobre el estado actual del sistema y del Cortafuegos.
- **Redes:** En el área de redes figura una lista de las redes (por ej. LAN, acceso telefónico a redes, etc.) con las que está conectado su ordenador.
- **Conjuntos de reglas:** En este área puede crear reglas especiales para diferentes redes, con el fin de optimizar la forma de reaccionar de su Cortafuegos.

El cortafuegos le alerta tan pronto encuentra algún indicio de que se van a grabar o descargar datos de modo ilícito en su ordenador y bloquea el intercambio de datos no autorizado.

 **Ajustes:** Mediante este botón situado arriba a la derecha puede acceder a todas las ventanas de diálogo de ajustes del Cortafuegos.

## Estado

En el área de estado del Cortafuegos encontrará información básica sobre el estado actual del sistema y del Cortafuegos. Esta información se encuentra a la derecha de la entrada correspondiente como indicación textual o numérica. Además, el estado de los componentes se representa también gráficamente. Haciendo doble clic en una entrada se pueden seleccionar directamente acciones a realizar o se puede navegar al área de programa correspondiente.

En cuanto haya optimizado los ajustes de un componente que muestre un símbolo de advertencia aparecerá de nuevo la marca de verificación verde en el área de estado.

- **Seguridad:** Mientras utiliza su ordenador en su trabajo diario, el Cortafuegos va aprendiendo continuamente qué programas utiliza para el acceso a Internet, cuáles no y qué programas suponen un riesgo para la seguridad. Dependiendo de la profundidad de sus conocimientos acerca de la tecnología del Cortafuegos, puede variar la configuración de esta herramienta, de manera que le ofrezca una buena seguridad básica sin realizar muchas preguntas, o bien configurar una protección profesional, que se adapte perfectamente a sus hábitos de uso del ordenador, pero que le exigirá al mismo tiempo ciertos conocimientos como usuario. Aquí se puede ajustar el estado de seguridad: [Configuración | Cortafuegos | Modo automático](#).

- **Modo:** Aquí puede informarse de la configuración básica con la que está operando su Cortafuegos. Se puede elegir entre una creación manual de reglas o el modo automático (piloto automático).

**Piloto automático:** Aquí el Cortafuegos trabaja de modo totalmente autónomo y mantiene automáticamente el ordenador doméstico resguardado de los peligros. Este ajuste ofrece prácticamente una protección total y se recomienda en la mayor parte de los casos. El piloto automático debería estar activado normalmente.

**Creación manual de reglas:** Si desea configurar su Cortafuegos de modo personalizado, o hay alguna aplicación que no interactúa con el modo de piloto automático, puede adaptar totalmente la protección del Cortafuegos a sus necesidades mediante la creación manual de reglas. Encontrará información más detallada en el capítulo: [Configuración | Cortafuegos | Modo automático](#).

- **Redes:** Aquí se pueden visualizar las redes en con las que está conectado su ordenador. En el siguiente capítulo encontrará más información: [Cortafuegos | Redes](#).
- **Ataques rechazados:** En cuanto su Cortafuegos detecta un ataque al ordenador, lo bloquea y lo registra aquí. Puede obtener más información haciendo clic en el elemento de menú.
- **Radar de aplicaciones:** Este cuadro de diálogo muestra los programas bloqueados en este momento por el Cortafuegos. Si desea autorizar una de estas aplicaciones bloqueadas para el uso de la red, basta con seleccionarla y hacer clic en el botón **permitir**.

## Redes

En el área de redes figura una lista de las redes (por ej. LAN, acceso telefónico a redes, etc.) con las que está conectado su ordenador. Aquí también se indican las reglas (véase el capítulo [Conjuntos de reglas](#)) que protegen a la red correspondiente. Cuando se quita la marca de verificación delante de la red correspondiente entonces se la excluye de la protección del Cortafuegos. Debería quitar la protección sólo en casos individuales justificados. Cuando marque una red con el ratón y haga clic en el botón **editar**, podrá ver o modificar la configuración del Cortafuegos para esa red.

## Editar red

En este resumen se muestran las siguientes informaciones y posibilidades de ajuste para la red seleccionada:

- **Información de red:** Aquí obtendrá información sobre la red y, si estuvieran disponibles, datos sobre la dirección IP, la máscara de subred, la puerta de enlace estándar, el servidor DNS y el servidor WINS.
- **Cortafuegos activo en esta red:** El Cortafuegos para la red se puede desactivar aquí, pero solo debería hacerlo en casos especiales justificados.
- **Uso compartido de la conexión a Internet:** En el caso de conexiones directas a Internet podrá establecer si todos los ordenadores de la red van a tener acceso a Internet a través de un ordenador conectado a Internet o no. Por regla general, esta autorización de conexión a Internet (ICS) puede activarse para una red doméstica.
- **Permitir configuración automática (DHCP):** Al conectarse su ordenador con la red se genera una dirección IP dinámica (mediante el DHCP = Dynamic Host Configuration Protocol). Si está conectado con la red mediante esta configuración estándar, debe dejar la marca de verificación puesta.
- **Conjunto de reglas:** Aquí puede cambiar muy rápidamente entre reglas preestructuradas y determinar de esta manera si con arreglo a los criterios de monitorización del Cortafuegos se trata, por ejemplo, de una red fiable, no fiable o que debe bloquearse. Con el botón **Editar conjunto de reglas** también tiene la posibilidad de configurar los conjuntos de reglas individualmente. Para más información consulte el capítulo [Crear conjuntos de reglas](#).

## Conjuntos de reglas

En este área se pueden definir reglas específicas para diferentes redes. Estas reglas se agrupan posteriormente en un conjunto de reglas. Por defecto hay conjuntos de reglas para una conexión directa con Internet, redes inseguras, redes seguras, y redes que deben ser bloqueadas. En la vista general se muestra el correspondiente conjunto de reglas con su nombre. Con la ayuda de los botones **nuevo**, **borrar** y **editar** se pueden modificar conjuntos de reglas existentes o añadir otros conjuntos de reglas.

No pueden borrarse los cuatro conjuntos de reglas predefinidos para la **conexión directa con Internet**, **redes seguras**, **redes no seguras** y **redes que se deben bloquear**. Los conjuntos de reglas que haya definido Ud. mismo puede borrarlos en el momento que desee.

## Crear conjuntos de reglas

Puede asignar a cada red un conjunto de reglas propio (es decir, una compilación de reglas especialmente adaptadas). De esta forma, puede proteger con el Cortafuegos de forma selectiva redes con distintos niveles de peligrosidad. Así, una red doméstica privada necesitará seguramente menos protección (y con ello menos inversión en administración) que una red de transmisión de archivos remotos que está en contacto directo con Internet.

Además, aquí puede crear con el botón **nuevo** sus propios conjuntos de reglas para redes. Haga clic en el área de Conjuntos de reglas en el botón **Nuevo** y defina los siguientes parámetros en la ventana de diálogo que se abre a continuación:

- **Nombre del conjunto de reglas:** Introduzca un nombre explicativo para el conjunto de reglas.
- **Crear un conjunto de reglas vacío:** Aquí puede crear un conjunto de reglas completamente vacío y equiparlo exclusivamente con reglas definidas por Ud.
- **Crear un conjunto de reglas que contenga algunas reglas lógicas:** Esta opción le permite decidir si en el nuevo conjunto de reglas deben predefinirse algunas reglas básicas para redes inseguras, seguras o que deben ser bloqueadas. Partiendo de estas preconfiguraciones pueden realizarse modificaciones individuales.

El Cortafuegos contiene tres conjuntos de reglas predefinidos para los siguientes tipos de red:

- **Conexión directa con Internet:** Este epígrafe comprende las reglas que regulan el acceso directo a Internet.
- **Redes inseguras:** En este grupo se incluyen normalmente redes abiertas como, por ejemplo, redes de transmisión de archivos

remotos.

- **Redes seguras:** Normalmente, son seguras las redes domésticas y de empresas.
- **Redes que deben ser bloqueadas:** Si tuviera que bloquear temporalmente o de forma duradera el contacto del ordenador con una red, puede utilizar esta configuración. Esto es útil, p.ej., en caso de conexión con redes externas cuyo nivel de seguridad no le conste de modo fiable (p.ej., en eventos con LAN públicas, redes de empresas desconocidas, puestos de trabajo públicos para portátiles, etc.).

El nuevo conjunto de reglas aparece ahora en el área conjuntos de reglas bajo el nombre correspondiente del conjunto de reglas (por ejemplo, *nuevo conjunto de reglas*) de la lista. Pulsando **editar** y en función del ajuste que haya hecho en [Configuración | Otros](#) (consultar el capítulo correspondiente), se abre el Asistente para reglas o el Modo de edición avanzado para la edición de las distintas reglas de este conjunto de reglas. Para consultar cómo se definen nuevas reglas en los conjuntos de reglas, consulte los capítulos [Utilizar asistente para reglas](#) o bien [Utilizar el modo de edición avanzado](#).

Además de la introducción directa de reglas, tiene también la posibilidad de crear reglas a través de la ventana de información de la alerta del Cortafuegos. El proceso de aprendizaje del Cortafuegos se detalla en el capítulo [Alerta de Cortafuegos](#).

## Utilizar asistente para reglas

Con el Asistente para reglas puede definir determinadas reglas adicionales para el conjunto de reglas correspondiente o modificar las reglas ya existentes. Precisamente para los usuarios con escasos conocimientos acerca de la tecnología de Cortafuegos, se recomienda elegir el asistente para reglas en vez del modo de edición avanzado.

Con el asistente para reglas se modifican una o varias reglas del conjunto de reglas seleccionado. Es decir, se crea siempre una regla dentro de un conjunto que ya contiene distintas reglas.

En función del conjunto de reglas que se haya definido para una red determinada, una aplicación puede estar bloqueada en un conjunto de reglas (p.ej., para redes no fiables) y en otro conjunto de reglas tener pleno acceso a la red (p.ej., para redes seguras). De esta manera, se puede, p.ej., limitar el acceso de un navegador con distintas reglas de tal forma que pueda acceder perfectamente a algunas páginas, p.ej., de su red doméstica privada, pero que no tenga ninguna posibilidad de acceder a contenidos de la red de transmisión de archivos remotos.

El asistente para reglas pone a su disposición las siguientes reglas básicas:

- **Autorizar o bloquear aplicaciones:** Con esta función puede seleccionar una aplicación (un programa) en su disco duro y autorizarle o denegarle explícitamente el acceso a la red definida por el conjunto de reglas. Para ello seleccione en el asistente el programa deseado (**ruta de programa**) e indique en **dirección**, si el programa debe ser bloqueado para las conexiones entrantes, las conexiones salientes o las conexiones de ambos tipos. De esta forma, por ejemplo, puede impedir que el software de su reproductor de MP3 transmita datos sobre sus gustos musicales (conexiones salientes) impedir que se realicen actualizaciones automáticas del programa (conexión entrante).
- **Autorizar o bloquear servicios de red: "Puerto"** se denomina a los ámbitos de direcciones específicas que transmiten datos automáticamente a través de una red, en un determinado protocolo y, por esta vía, a un determinado software. Así, las páginas Web normales se transmiten a través del puerto 80, los correos electrónicos se envían mediante el puerto 25 y se recogen por el puerto 110, etc. Sin Cortafuegos, todos los puertos de su ordenador están abiertos por norma general, aunque la mayoría de los usuarios normales no los necesitan en absoluto. Bloqueando uno o varios puertos se pueden cerrar por tanto rápidamente brechas, que de otra forma podrían ser utilizadas por los hackers para realizar ataques. En el asistente tiene la posibilidad de cerrar completamente los puertos o hacerlo únicamente para una aplicación determinada (p.ej., su software para reproducción de MP3).
- **Uso compartido de impresoras y archivos:** Si autoriza el acceso, tendrá la posibilidad de acceder en su red local a carpetas e impresoras de uso compartido. Simultáneamente, también otros equipos y usuarios de su red local podrán acceder a los usos compartidos que haya establecido.
- **Autorizar o bloquear servicios de dominio:** Un dominio es un tipo de índice de clasificación para equipos en una red y permite una administración centralizada de los ordenadores conectados en red. La autorización para servicios de dominio en redes no fiables debe denegarse como norma general.
- **Uso compartido de la conexión de Internet:** En el caso de conexiones directas con Internet podrá establecer si todos los ordenadores de la red van a tener acceso a Internet a través de un ordenador conectado a Internet o no. Por regla general, esta autorización de conexión a Internet puede activarse para una red doméstica.
- **Autorizar o bloquear servicios de VPN:** VPN son las siglas de "virtual private networks" (redes privadas virtuales) y designa la forma de acoplar ordenadores de forma exclusiva para establecer una conexión casi directa entre ellos. Para que los servicios de VPN puedan funcionar, hay que autorizarlos en el Cortafuegos.



- **Editor avanzado de conjuntos de reglas (modo experto):** Aquí puede cambiar del asistente para reglas al modo de edición avanzado. Encontrará información sobre el modo de edición avanzado en el capítulo [Utilizar el modo de edición avanzado](#).

## Utilizar el modo de edición avanzado

En el modo de edición avanzado podrá definir (contando con ciertos conocimientos acerca de seguridad de redes) reglas estrictamente individuales para la red correspondiente. Por supuesto, puede crear aquí todas las reglas que se pueden definir con el asistente para reglas, pero también se pueden realizar ajustes más avanzados.

Están disponibles las siguientes posibilidades de configuración:

- **Nombre:** Aquí puede modificar el nombre del conjunto de reglas actual si fuera necesario. El conjunto de reglas aparecerá con este nombre en la lista del área de **Conjuntos de reglas** y puede ser combinado con las redes allí identificadas por el Cortafuegos.
- **Modo sigilo:** Con el modo sigilo (del inglés "stealth": oculto, secreto) no se responde a las consultas que reciba el ordenador sobre la verificación de la accesibilidad de los puertos correspondientes. Esta actuación dificulta que los hackers puedan obtener información sobre el sistema.
- **Acción a realizar si no se cumple ninguna regla:** Aquí se puede determinar si se permite o deniega el acceso general a la red o si debe consultarse. Si mediante la función de aprendizaje del Cortafuegos se definen reglas especiales para algunos programas, éstas, por supuesto, se respetarán.
- **Modo adaptativo:** El modo adaptativo le protege en aplicaciones que utilizan la denominada tecnología de canal de retorno (p.ej. FTP y muchos juegos online). Estas aplicaciones se conectan con un ordenador remoto y negocian con él un canal de retorno en el que el ordenador remoto se *reconecta* con su aplicación. Si está activo el modo adaptativo, el Cortafuegos reconoce este canal de retorno y le permite la conexión sin más consultas.

## Reglas

En la lista de reglas encontrará todas las reglas que se han definido para el conjunto de reglas en cuestión. De esta manera, p.ej., pueden permitirse numerosos accesos a la red a programas seleccionados, aunque la red en sí haya sido definida como no fiable. Las reglas aplicables aquí se pueden crear de distintas maneras:

- Con el [Asistente para reglas](#)
- Directamente con el [Modo de edición avanzado](#) mediante el botón **Nuevo**
- A través del diálogo de la ventana de información que aparece con una [Alerta de Cortafuegos](#).

Cada conjunto de reglas dispone de una lista propia con reglas.

Puesto que las reglas del Cortafuegos se activan en parte jerárquicamente, es importante tener en cuenta para algunos casos el orden jerárquico de las reglas. De esta forma puede ocurrir que una autorización para un puerto vuelva a ser bloqueada después por la denegación de un acceso de protocolo. Puede cambiar el orden del rango de una regla marcándola con el ratón y desplazándola hacia arriba o hacia abajo mediante las flechas en el **rango** de la lista.

Si crea una nueva regla mediante el modo de edición avanzada o si cambia una regla existente con el diálogo **Editar** aparece el cuadro de diálogo **Editar regla** con los siguientes ajustes posibles:

- **Nombre:** En las reglas preconfiguradas y generadas automáticamente, aquí se encuentra el nombre del programa para el que se aplica la regla correspondiente.
- **Regla activa:** Puede dejar inactiva una regla quitando la marca de verificación, sin tener que borrarla en ese momento.
- **Comentario:** Aquí puede averiguar cómo ha sido creada una regla. En las reglas preconfiguradas para el conjunto de reglas se indica "regla por defecto", en las reglas creadas a partir del diálogo proveniente de la [Alerta de Cortafuegos](#) se indica "generado en respuesta a una consulta" y en las reglas que haya creado usted mismo a través del modo de edición avanzado, puede introducir un comentario.
- **Dirección de conexión:** Con la dirección se define si en este caso se trata de una regla para conexiones entrantes, salientes o de ambos tipos.
- **Acceso:** Aquí se determina si para el programa correspondiente dentro de este conjunto de reglas se permite o se rechaza el acceso.
- **Protocolo:** Aquí puede seleccionar a qué protocolos de conexión desea permitir o rechazar el acceso. Para ello, tiene la posibilidad de bloquear o habilitar protocolos en general o de vincular el uso del protocolo al empleo de una o varias aplicaciones determinadas

(**asignar aplicaciones**). Del mismo modo, puede definir exactamente los puertos deseados o no deseados con el botón **Asignar servicio de Internet**.





- **Periodo de tiempo:** Puede configurar el acceso a los recursos de red también en función del tiempo y de esta forma garantizar que un acceso se realice solo en estas horas y no fuera de ellas.
- **Espacio de direcciones IP:** Especialmente en redes con direcciones IP fijas es aconsejable regular el uso restringiendo el rango de direcciones IP. Un rango de direcciones IP claramente definido reduce considerablemente el peligro de un ataque de hackers.

# Copia de seguridad


Con el avance de la digitalización de la vida diaria, la utilización de servicios de música en línea, cámaras digitales y correo electrónico, cada vez es más importante garantizar la seguridad de los datos personales. Deben hacerse copias de seguridad periódicas de los documentos personales, para prevenir en caso de que se produzca un error de hardware, un descuido o un daño causado por un virus o por ataques de hackers. El software G DATA se encarga de esta tarea y protege tanto documentos como archivos importantes sin que usted tenga que preocuparse constantemente de ello.

## Guardar y restaurar

Cuando se crea una orden de copia de seguridad con la función **Nueva orden** la puede editar y controlar directamente con los siguientes iconos:



-  **Restaurar:** Con esta opción se devuelven al sistema los datos archivados en la copia de seguridad. La forma en que se produce la restauración se explica en el capítulo [Restaurar copia de seguridad](#).
-  **Copia de seguridad:** Con esta opción se inicia el proceso de copia de seguridad para la orden de copia de seguridad definida, de forma inmediata y no programada, es decir, independientemente del horario programado para esa copia de seguridad.
-  **Configuración:** Aquí se pueden modificar los ajustes para la orden de copia de seguridad correspondiente que se configuraron al crear por primera vez la orden en [Nueva orden de copia de seguridad](#).
-  **Registros:** Aquí se ve un resumen de todos los procesos realizados con esta orden de copia de seguridad. Figuran entradas sobre los procesos manuales o programados de copia de seguridad, información sobre posibles restauraciones y los mensajes de error que haya, por ej. si no quedaba espacio en el directorio de destino para la copia de seguridad prevista.

## Nueva orden de copia de seguridad

-  Para asignar una nueva orden de copia de seguridad, haga clic en el botón **Nueva orden**.

## Selección de archivos / Discos duros / Particiones

El asistente de copia de seguridad le pregunta ahora qué clase de copia de seguridad desea realizar.

-  **Copia de seguridad de archivos:** Se trata de una copia de seguridad de los archivos y carpetas que haya seleccionado en un archivo comprimido.  
  
Solo tiene que seleccionar en la vista de directorio los archivos y carpetas que desee guardar. Por norma general, se recomienda guardar en la copia de seguridad archivos personales, no archivos de los programas instalados. Si hace clic en los símbolos de más del árbol de directorios, podrá abrir y seleccionar directorios y en la vista de archivos se puede visualizar su contenido. A continuación, el software procederá a usar para la copia de seguridad los directorios y archivos que haya marcado. Si en un directorio no se usan todos los archivos y las carpetas para la copia de seguridad, el directorio estará marcado con una marca de verificación gris.
-  **Copia de seguridad de la unidad de disco:** Se trata de una copia de seguridad completa de los discos duros o particiones en un archivo comprimido.

## Seleccionar destino

Aquí puede definir el destino, es decir, determinar la ubicación en la que el software G DATA creará la copia de seguridad de los archivos y carpetas o de los discos duros y particiones. Puede ser una unidad de CD o DVD-ROM, otro disco duro, un lápiz USB, otros soportes intercambiables o un directorio de la red.

**Nombre del archivo comprimido:** Aquí se puede dar un nombre explicativo al archivo comprimido que se va a crear, como por ej. *Copia de seguridad semanal de Mis documentos*, *Copia de seguridad de MP3* o similar.

**Nueva carpeta:** Si desea crear una nueva carpeta para la copia de seguridad, seleccione en la vista de directorios la ubicación deseada y pulse luego el botón **Nueva carpeta**.

**Nota:** Asegúrese de que la copia de seguridad no se realice en el mismo disco duro en que ya estén los datos de origen. Porque

entonces si este disco se estropease, se perderían los datos de origen y los de seguridad. Lo mejor es conservar una copia de seguridad en una ubicación separada físicamente de los archivos de origen, por ejemplo en otra habitación en un disco duro USB, en red en un servidor FTP o grabada en un CD / DVD-ROM.

**Crear un archivo comprimido en un servidor FTP:** Si tiene acceso a un servidor FTP, también puede guardar su copia de seguridad online en este servidor FTP. Para ello, solo tiene que iniciar sesión con los datos de acceso para su servicio FTP, y así queda ya vinculado el archivo comprimido de copia seguridad con su servidor FTP. En su software de G DATA puede gestionar también los archivos comprimidos de copia de seguridad mediante el [Navegador FTP](#) integrado.

**Crear archivo comprimido en la Nube:** Simplemente, utilice los servicios en la Nube habituales, como por ejemplo, Microsoft Dropbox, OneDrive\* o Google Drive, para guardar allí su copia de seguridad. Para ello, solo tiene que iniciar sesión con los datos de acceso para su servicio en la Nube, y así queda ya vinculado el archivo comprimido de copia seguridad con la Nube.

**Nota:** Al realizar la copia de seguridad en la Nube debe asegurarse especialmente de que los datos de su copia de seguridad estén cifrados. En el área [Opciones](#) con la opción [Nueva orden de copia de seguridad](#) puede activar y desactivar el cifrado de los datos.

**(\* Nota sobre OneDrive:** Puede utilizar OneDrive si ha integrado este servicio como unidad virtual en Windows Explorer. En este caso, el archivo comprimido se crea de la forma habitual a través del directorio de archivos, y no mediante la función **Crear archivo comprimido en la Nube**.

## Horario

Aquí podrá programar cuando se debe realizar una copia de seguridad de los datos seleccionados. Además puede establecer el tipo de copia de seguridad a ejecutar. Se puede elegir entre una copia de seguridad completa, en la que se guardan los datos seleccionados en su totalidad o, una copia de seguridad parcial, en la que se guardan solo los cambios desde la última copia de seguridad.

Si selecciona **manual**, la copia de seguridad no se realizará automáticamente, sino que tiene que iniciarla desde la interfaz del programa. En la opción **Diariamente** puede especificar bajo Días de la semana que su ordenador, p. ej., ejecute la copia de seguridad sólo en los días hábiles o sólo cada dos días o durante el fin de semana, cuando no se utiliza para trabajar. Además puede definir copias de seguridad semanales y mensuales.

**No ejecutar en modo batería:** Para que un proceso de copia de seguridad en un portátil no se interrumpa repentinamente al agotarse el acumulador del portátil, puede definir que las copias de seguridad solo se realicen cuando el portátil esté conectado a la red eléctrica.

## Ejecutar copia de seguridad completa

En **Ejecutar copia de seguridad completa** simplemente debe especificar la frecuencia con que debe realizarse la orden de copia de seguridad, en qué días y a qué hora. En el intervalo especificado se realizará forma automática una copia de seguridad de todos los datos que haya seleccionado en [Selección de archivos / Discos duros / Particiones](#).

**Atención:** La copia de seguridad programada no funciona con CD-ROM o DVD-ROM, ya que en este caso se requiere una intervención del usuario en caso puede ser necesaria la intervención del usuario para cambiar el disco virgen.

En la sección **Eliminar archivos comprimidos obsoletos** puede determinar cómo debe proceder el software G DATA en caso de que ya existan copias de seguridad. El software G DATA comprime cada vez los datos en un solo archivo con la extensión ARC. Conservar copias de seguridad existentes y no sobrescribirlas aumenta el grado de seguridad de sus datos, ya que, incluso en el caso de que el archivo comprimido actual estuviera dañado, se dispone aún de un archivo comprimido anterior, con lo que no todos los datos están perdidos. No obstante, los archivos comprimidos suelen requerir mucho espacio en los soportes de datos, con lo que debería procurar que no se acumulen demasiados archivos comprimidos. Por ello resulta muy útil la opción **Conservar las copias de seguridad completas**, ya que ahí puede especificar la cantidad máxima de copias de seguridad que se guardará en el soporte de copia de seguridad. De esta forma, el archivo comprimido más antiguo será substituido por el actual.

Si activa la marca de verificación en **Crear copia(s) de seguridad parciales**, el software ejecuta solamente copias de seguridad parciales después de la primera copia de seguridad completa. Estas copias parciales son bastante más rápidas al crearse pero puede que se tarde más cuando haya que restaurar una copia de seguridad completa a partir de ellas. Otro inconveniente de la copia de seguridad parcial es que, en comparación, se necesita más espacio de almacenamiento, ya que no se pueden borrar directamente los datos que ya no se necesitan de la copia de seguridad completa. No obstante, después de la siguiente copia de seguridad completa, se reúnen los datos de la copia de seguridad completa y parcial, y la cantidad de datos vuelve a ser la de una copia de seguridad completa.

## Ejecutar copias de seguridad parciales

Las copias de seguridad parciales sirven para acelerar el respaldo de datos. En lugar de utilizar todos los datos para una copia de seguridad, la copia de seguridad parcial se basa en una copia de seguridad completa previa y guarda sólo los datos que hayan cambiado o se hayan creado nuevos desde la última copia de seguridad. De esta manera, obtendrá una copia de seguridad completa de todos sus datos, pero el proceso de copia de seguridad en sí es mucho más rápido.

**Diferencial/incremental:** En el caso de la copia de seguridad diferencial se guardan todos los datos que se han modificado o se han agregado desde la última copia de seguridad completa. Se incorpora siempre a la última copia de seguridad completa guardada. Frente a una nueva copia de seguridad completa se ahorra tiempo y espacio. La copia de seguridad incremental va un nivel más allá y, entre dos copias de seguridad parciales, guarda los archivos que se han modificado entre una copia de seguridad parcial y otra. La desventaja en este caso es que en el caso de una restauración de los datos se necesitan varios archivos.

## Opciones

En el área de opciones puede modificar las opciones generales de los archivos de copia de seguridad. Por lo general, no hace falta que modifique nada, porque las opciones estándar de G DATA ya cubren la mayor parte de los casos en la práctica.

### Opciones generales de archivos comprimidos

En las opciones generales de archivos comprimidos cuenta con las siguientes posibilidades de configuración:

- **Limitar el tamaño del archivo comprimido:** Si guarda archivos comprimidos en CD, DVD-ROM u otros soportes de escritura es importante que el software G DATA limite el tamaño de los archivos comprimidos. Aquí dispone de una selección de tamaños estándar que le posibilita guardar con posterioridad los archivos comprimidos en CD, DVD o discos blu-ray. El archivo comprimido se divide al alcanzar el tamaño máximo indicado y la información de Copia de seguridad se reparte en dos o más archivos comprimidos.
- **Crear CD/DVD multisesión:** Si selecciona esta opción, creará CDs o DVDs de copia de seguridad que se puede grabar varias veces. Pero el contenido guardado anteriormente no se borra, sino que se complementa con el nuevo contenido.
- **Eliminar archivos comprimidos temporales:** Esta opción debe, como norma general, permanecer activada. Los archivos comprimidos temporales ocupan mucho espacio en su disco duro tras un número determinado de procesos de copia de seguridad y, en realidad, ya no son necesarios después de su uso temporal.
- **Copiar archivos de programa de restauración:** Si activa esta función, además de los archivos comprimidos, se instala en el lugar de almacenamiento de la copia de seguridad un programa con el que puede restaurar sus datos sin tener instalado el software G DATA. Para ello inicie desde el CD/DVD-ROM el programa **AVKBackup** y/o **AVKBackup.exe**.

El programa de restauración se copia solo en el CD/DVD-ROM. Pero éste no es el caso en copias de seguridad de soportes intercambiables (lápiz USB, disco duro externo).

Cuando haya instalado el software G DATA en el ordenador en el que se realizará la restauración, no ejecute la restauración con el programa de restauración en el CD/DVD-ROM, sino mediante la función [Importar archivos comprimidos](#).

- **Comprobar los archivos por si tienen virus antes de comprimirlos:** Cuando está instalado el módulo AntiVirus, puede examinar los archivos por si tienen virus antes de que sean guardados en el archivo comprimido de copia de seguridad.
- **Comprobar el archivo comprimido después de crearlo:** Esta función sirve para comprobar la integridad y ausencia de errores en el archivo comprimido tras su creación.
- **Cifrar el archivo comprimido:** Si desea proteger sus archivos guardados frente al acceso de un extraño puede dotarlos de una contraseña. En ese caso, la restauración de los archivos sólo será posible con esta contraseña. Deberá acordarse bien de la contraseña o anotarla en un lugar seguro. Sin la contraseña, no podrá restaurar sus archivos comprimidos.
- **Prueba de integridad en una copia de seguridad diferencial:** Esta función sirve para comprobar de nuevo la integridad y ausencia de errores de una copia de seguridad parcial tras su creación.
- **Prueba de integridad al restablecer el disco duro:** Esta función se utiliza para comprobar que los datos se han restaurado correctamente. El **Directorio de archivos temporales** es una ubicación de almacenamiento para los datos que el software G DATA escribe solo de forma temporal en su disco duro. En caso de que no haya espacio suficiente en su partición estándar, puede cambiar aquí la partición y la ubicación temporal de estos archivos.
- **Usar el servicio shadow copy de Windows:** Si esta opción está desactivada, no se puede crear una imagen de la partición del sistema con el sistema en funcionamiento.

### Datos del usuario

Para poder realizar copias de seguridad programadas, deberá marcar aquí la opción **Ejecutar tarea como** y especificar los datos de acceso de su cuenta de usuario de Windows. Estos datos también son necesarios para que la copia de seguridad se pueda realizar según planificación horaria cuando Ud. no tenga abierta sesión.

## Comprimir

En el área comprimir puede definir si sus archivos comprimidos van a tener un alto o un bajo grado de compresión.

- **Mayor nivel de compresión:** Los datos para la copia de seguridad se comprimen al máximo. De este modo se ahorra espacio de memoria, pero la copia de seguridad en sí misma tarda más tiempo.
- **Compresión equilibrada:** La copia de seguridad no se comprime en tan alto grado, pero se realiza con mayor rapidez.
- **Ejecución rápida:** Los datos no se comprimen, la copia de seguridad se realiza con gran rapidez.

## Excluir archivos

En general, el software G DATA guarda archivos sobre la base de su formato de archivo. En el sistema de su ordenador se encuentran los formatos de archivo correspondientes también en áreas que se administran automáticamente y no son relevantes para una copia de seguridad, ya que los archivos en cuestión sólo se han guardado temporalmente (p.ej. para acelerar la visualización de páginas de Internet). Para que el software G DATA no guarde innecesariamente estos archivos, puede excluirlos marcando la casilla correspondiente.

- **Directorios temporales con archivos:** En caso de haber activado esta opción, las carpetas temporales, así como las subcarpetas y archivos que allí se encuentren, se excluirán en el momento de guardar los datos.
- **Directorios temporales de Internet con archivos:** En caso de haber activado esta opción, las carpetas para el almacenamiento de páginas de Internet, así como las subcarpetas y archivos que allí se encuentren, se excluirán en el momento de guardar los datos.
- **Thumbs.db:** Si se selecciona esta opción, en la copia de seguridad no se incluirán los archivos thumbs.db creados automáticamente por Windows Explorer. Estos archivos sirven p.ej. para administrar vistas en miniatura para presentaciones de diapositivas y se crean automáticamente a partir de las imágenes de origen.
- **Archivos temporales (atributo de archivo):** Si se selecciona esta opción, en la copia de seguridad no se incluirán los archivos con el atributo temporal asignado por el sistema.
- **Archivos del sistema (atributo de archivo):** Si se selecciona esta opción, en la copia de seguridad no se incluirán los archivos con el atributo de archivo de sistema asignado por el sistema.
- **Excluir tipos de archivo:** Con esta función puede definir las extensiones de archivo que no se deben tener en cuenta en su copia de seguridad. Para ello proceda del siguiente modo: Introduzca en **Tipo de archivo** (por ejemplo, \*.txt) la extensión de archivo o el nombre de archivo que desee excluir. Ahora haga clic en **aceptar**. Repita el proceso para todos los tipos y nombres de archivos que desee excluir, por ejemplo, picasa.ini, \*.ini, \*bak, etc. Puede utilizar el asterisco y la interrogación como comodines. El funcionamiento de los comodines es el siguiente:

El signo de interrogación (?) representa caracteres sueltos.

El signo de asterisco (\*) representa una secuencia completa de caracteres.

Para comprobar, por ejemplo, todos los archivos con la extensión exe, introduzca \*.exe. Para comprobar, por ejemplo, ficheros de distintos formatos de hojas de cálculo (p.ej. \*.xlr, \*.xls), introduzca simplemente \*.xl?. Para comprobar archivos de diferentes tipos cuyo nombre coincide al inicio, introduzca por ejemplo text\*.\*.

## Restablecer opciones estándar actuales

Haciendo clic sobre este botón restaurará las opciones que fueron definidas como opciones estándar para el software G DATA. Si introduce accidentalmente opciones erróneas al crear la copia de seguridad y no sabe cómo repararlas, haga clic en el botón **Restablecer opciones estándar actuales**.

## Restaurar copia de seguridad



Aquí puede restaurar los datos originales a partir de la copia de seguridad tras una pérdida de datos. Para ello, haga clic en el botón **Restaurar**.

Se abre ahora una ventana de diálogo en la que figuran todos los procesos almacenados de copia de seguridad para la orden correspondiente.

Seleccione aquí la copia de seguridad deseada (por ej. la última realizada, si desea restaurar documentos borrados por error poco antes) y pulse luego el botón **Restaurar**.

Ahora tiene la posibilidad de establecer la forma de restauración que desee:

- **Restaurar la copia de seguridad completa:** Se restablecerán todos los archivos y carpetas que haya respaldado con esta copia de seguridad.
- **Restablecer sólo archivos y particiones seleccionados:** Aquí aparece una vista del directorio de su copia de seguridad, en la que puede elegir los archivos, carpetas o particiones que desea restaurar y los que no. Si hace clic en los símbolos de más del árbol de directorios, podrá seleccionar y abrir directorios y en la vista de archivos se puede visualizar sus contenidos. A continuación, se restaurarán de la copia de seguridad los directorios o archivos que haya marcado con una marca de verificación. Si no se seleccionan todos los archivos de un directorio, ese directorio aparecerá marcado con una marca de verificación gris.

Al final puede definir si los archivos se restauran o no a sus directorios de origen. Si desea guardar los archivos en otro lugar distinto, puede seleccionar en **Nueva carpeta** una carpeta donde almacenarlos. Introduzca en **contraseña** la contraseña de acceso, en caso de que haya comprimido su copias de seguridad de datos protegiéndola mediante contraseña al guardarla.

Si desea restaurar archivos a los directorios de origen, tiene las siguientes opciones para recuperar solo los archivos modificados:

- **Sobrescribir siempre:** En este ajuste se considera siempre que los archivos de la copia de seguridad de datos son más importantes que los datos que se encuentran en el directorio original. Si activa esta opción, se sobrescribirán completamente los datos que haya con los datos que se encuentren en el archivo comprimido.
- **Cuando haya cambiado el tamaño:** Con este ajuste, se sobrescriben los datos existentes del directorio original sólo cuando haya cambiado el archivo original. Los archivos que no hayan cambiado de tamaño se saltarán. De este modo, la restauración de datos será posiblemente más rápida.
- **Cuando la fecha de modificación del archivo comprimido sea más actual:** Se reemplazan los archivos del directorio original siempre que la copia del archivo comprimido sea más actual que los datos del archivo. Aquí también puede ser más rápida la restauración de datos, ya que de este modo no se tienen que restaurar todos los archivos, sino sólo los datos modificados.
- **Cuando la fecha de modificación haya cambiado:** Se reemplazarán los datos del directorio original sólo cuando haya cambiado algo en la fecha en comparación con los archivos guardados.

Pulse al final el botón **Concluir proceso** para ejecutar la restauración con los ajustes que haya especificado.

## Acciones

En este área pueden realizarse otras acciones de edición y mantenimiento de sus copias de seguridad de datos.

Aquí tiene a su disposición las siguientes utilidades:

## Actualizar archivos online

Para asegurar los datos más importantes en línea en un servidor FTP, el software G DATA necesita, lógicamente, los datos de acceso correspondientes. Al hacer clic por primera vez en esta función se puede indicar aquí el nombre del servidor, el puerto, el nombre de usuario, la contraseña y el directorio que se le proporcionaron al registrarse en el servidor de actualización G DATA.

## Navegador FTP

Introduzca simplemente sus datos de acceso FTP para acceder a su servidor FTP. En el Navegador FTP ahora puede llevar a cabo las siguientes acciones:



**Conectar:** En caso de que se cancele la conexión con el Navegador FTP, puede volver a activarla aquí.



**Desconectar:** Aquí puede cancelar la conexión al Navegador FTP.




**Nueva carpeta:** Si desea guardar sus copias de seguridad en diferentes carpetas (por.ej. sólo carpetas especiales para las copias de seguridad de música), puede crear una carpeta con esta función en la memoria FTP.





**Eliminar:** Con esta función puede borrar las carpetas o archivos que ya no necesite.



**Actualizar:** Si durante el uso del Navegador FTP ha llevado a cabo otra actualización, puede visualizar los nuevos datos con el botón Actualizar.

 **Descarga:** Aquí podrá copiar con el ratón los archivos marcados del Servidor FTP en la ubicación de almacenamiento de su ordenador que desee.

 **Carga:** Así puede guardar posteriormente con el software G DATA los archivos creados en su servidor FTP.

 **Ayuda:** Con esta opción se abre la ayuda del programa.

## Grabar archivo comprimido en CD / DVD con posterioridad

Los archivos de copia de seguridad los puede grabar posteriormente en CD o DVD. Para ello, en la ventana que se abre busque el proyecto que desee grabar y haga clic en el botón **Continuar**.

Seleccione luego en qué unidad de disco desea grabar la copia de seguridad.

Tiene a su disposición las siguientes opciones:

- **Comprobar datos después de la grabación:** Si activa la marca de verificación, se comprobarán los datos después del proceso de grabación. Por lo general dura más que un proceso de grabación sin comprobación pero es recomendable.
- **Copiar archivos de programa de restauración:** Si activa esta función, además de los archivos comprimidos, se instala en el lugar de almacenamiento de la copia de seguridad un programa con el que puede restaurar sus datos sin tener instalado el software G DATA. Para ello inicie desde el CD/DVD-ROM el programa **AVKBackup** y/o **AVKBackup.exe**.

Haga clic en el botón **Grabar** para iniciar el proceso de grabación. Tras el proceso de grabación se expulsa automáticamente el CD / DVD de copia de seguridad.

**Nota:** Los datos de copia de seguridad no se borran del soporte de datos original tras el proceso de grabación. La grabación con posterioridad en CD / DVD es una medida de seguridad adicional.

## Importar archivos comprimidos

Para restaurar archivos comprimidos y copias de seguridad de datos que no se encuentran en una unidad gestionada por el software G DATA, utilice la función **Importar archivos comprimidos**. Se abrirá un cuadro de diálogo en el que podrá buscar un archivo con la extensión **ARC** en un CD, DVD o la red, por ejemplo. Cuando haya encontrado el archivo comprimido deseado, active la marca de verificación y haga clic en el botón **Aceptar**. Una ventana informativa le indicará que el archivo comprimido se ha importado con éxito. Si desea utilizar este archivo comprimido para la restauración de datos, diríjase al área **Restaurar** del software G DATA, seleccione la copia de seguridad deseada e inicie la restauración.

**Nota:** Los archivos comprimidos creados por el software G DATA tienen la extensión **ARC**.

## Crear soporte de arranque

Para poder restaurar copias de seguridad sin tener el software G DATA instalado, puede crear un CD/DVD o una memoria USB conteniendo un software especial con el que podrá realizar la restauración de los datos. Para poder restaurar así copias de seguridad, inicie el soporte de arranque y seleccione el programa **AVKBackup** o **AVKBackup.exe**. Ahora podrá seleccionar las copias de seguridad deseadas e iniciar la restauración.

**Nota:** Para saber como crear un soporte de arranque, consulte el capítulo **Soporte de arranque**. El soporte de arranque cumple dos cometidos en el software G DATA. Puede realizar restauraciones de copias de seguridad y comprobar con **BootScan** antes del arranque de Windows si su ordenador está infectado.



# Administrador de contraseñas

Mediante el gestor de contraseñas puede gestionar las contraseñas cómodamente y utilizarlo como complemento en su navegador.

El gestor de contraseñas admite los siguientes navegadores, siempre en su versión más actual:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

Nota: tenga en cuenta que, dependiendo de los ajustes de su navegador (p. ej., configuración de privacidad), la funcionalidad del gestor de contraseñas puede estar limitada.

Cree primero una caja fuerte para contraseñas y después instale el complemento para el navegador que elija. Por supuesto, también puede instalar la caja fuerte para contraseñas en todos los navegadores compatibles.


## Crear una caja fuerte nueva e instalar el complemento

Haga clic en la opción **Caja fuerte para contraseñas**. A continuación se abre un cuadro de diálogo en el que puede crear una caja fuerte nueva seleccionando **Crear nueva caja fuerte**.

Indique una contraseña, confírmela, haga clic en **Crear caja fuerte**, y se creará la caja fuerte. El indicio de contraseña puede ayudarle a recordar una contraseña olvidada.


Una vez haya creado la caja fuerte, en la parte derecha de la ventana del programa puede seleccionar el navegador en el que desea instalar el complemento del gestor de contraseñas. Para ello, simplemente haga clic en el nombre del navegador correspondiente y el complemento se instalará.

La siguiente vez que abra el navegador es posible que se le pregunte si desea utilizar el nuevo complemento. Debe confirmar el uso para el G DATA Password Manager.

-  Ahora podrá encontrar el siguiente icono en la barra de tareas de su navegador. Haciendo clic en este icono puede utilizar el gestor de contraseñas.






Para ello, introduzca su contraseña en el diálogo que aparece y haga clic en **Desbloquear**. El uso del complemento para el navegador se explica en el siguiente [capítulo](#).

## Utilización del complemento para el navegador

-  Haciendo clic en el siguiente icono de la barra de tareas del navegador puede utilizar el gestor de contraseñas.


Nota: tenga en cuenta que, dependiendo de la configuración de privacidad (p. ej., guardar el historial), es posible que el gestor de contraseñas no se pueda utilizar. Por tanto, si hay problemas con el complemento, compruebe primero los ajustes de su navegador.


Para ello, introduzca su contraseña en el diálogo que aparece y haga clic en **Desbloquear**. Ahora estarán disponibles las siguientes áreas:

-  **Favoritos:** mediante esta función puede visitar rápidamente las páginas web protegidas mediante contraseña que utilice con regularidad.
-  **Login:** aquí puede gestionar los login para las páginas web protegidas mediante contraseña.
-  **Contactos:** con ayuda de los datos de contacto introducidos aquí puede rellenar formularios como, por ejemplo, direcciones de entrega, de forma automática.
-  **Notas:** aquí puede guardar notas adicionales protegidas mediante contraseña.
-  **Configuración:** para volver a cerrar el gestor de contraseñas, haga clic en **Bloquear**. Al hacer clic sobre Configuración puede

gestionar cómodamente los Favoritos, Login, Contactos y Notas utilizando cuadros de diálogo. Mediante el generador de contraseñas puede crear automáticamente una contraseña segura y utilizarla directamente a través del portapapeles.

En la administración del gestor de contraseñas puede añadir, editar y borrar entradas de la siguiente forma:

 Nueva entrada: haciendo clic en este botón puede crear una entrada nueva e introducir todos los datos necesarios en los cuadros de diálogo correspondientes a Login, Contactos o Notas.





 Guardar entrada: haciendo clic en este botón se guarda la entrada, y esta se mostrará en la selección rápida del complemento del navegador.

 Borrar entrada: con este botón puede borrar las entradas que ya no necesite.

# Optimizador de sistema

El tuner es una herramienta muy útil para hacer su sistema Windows mucho más rápido y más manejable con recordatorios automáticos para las actualizaciones de Windows, la desfragmentación periódica programada o la eliminación con regularidad de las entradas de registro innecesarias y los archivos temporales.




Puede optimizar el rendimiento de su ordenador o bien manualmente pulsando un botón o de forma programada con órdenes periódicas de optimización.

- 
**Último proceso de optimización del sistema:** Aquí se muestra cuando se optimizó por última vez el sistema. Para iniciar una nueva optimización, pulse la entrada **Ejecutar ahora el proceso de optimización del sistema**. En cuanto inicie el proceso de optimización, la barra de progreso le indicará el estado actual de la optimización.
- 
**Proceso automático de optimización del sistema:** Si desea que la optimización de su ordenador se lleve a cabo automáticamente, puede pulsar la entrada **Activar proceso automático de optimización del sistema** para generar la correspondiente orden programada. Para configurar el proceso automático de optimización, seleccione la opción **Ajustes avanzados**.
- 
**Configuración:** En este [Área](#) puede seleccionar todos los módulos que debe utilizar el optimizador del sistema para realizar un proceso de puesta a punto. Los módulos seleccionados se iniciarán bien a través de una acción automática programada (véase el capítulo [Planificación horaria](#)) o manual. Para activar un módulo, simplemente haga doble clic en él. Las siguientes áreas de Tuning se pueden optimizar aquí de manera individual:
  - *Seguridad:* Muchas funciones que descargan posterior y automáticamente datos de Internet, le benefician únicamente al proveedor y no a usted. Con frecuencia, estas funciones son la puerta de entrada de software malicioso. Con estos módulos Ud. protege su sistema y lo mantiene en el nivel más actualizado.
  - *Rendimiento:* Los archivos temporales, como por ej. copias de seguridad que ya no se necesitan, archivos de registro o datos de instalación que, una vez realizada la instalación, sólo ocupan espacio en el disco duro, lo ralentizan y consumen valiosa memoria. Además, los procesos y vínculos de archivos superfluos ralentizan el sistema notablemente. Con los módulos enumerados aquí puede librar a su ordenador de este lastre innecesario, acelerando así la velocidad de operación.
  - *Protección de datos:* Aquí se agrupan los módulos que se ocupan de la protección de los datos. Aquí se borran los rastros que se dejan involuntariamente al navegar o al utilizar el ordenador y que desvelan mucha información sobre los hábitos del usuario o incluso datos importantes y contraseñas.
- 
**Restaurar:** El software crea un punto de restauración cada vez que ejecuta una modificación. Si uno de los cambios aplicados tiene efectos indeseados, puede deshacer esas modificaciones y restaurar su sistema al estado anterior a la modificación. Lea también el capítulo [Restaurar](#).
 

**Browser Cleaner:** G DATA Browser Cleaner puede bloquear o eliminar componentes de programa o complementos no deseados. Estos programas a menudo se instalan junto con el software gratuito, y pueden modificar la configuración del navegador o incluso espiar datos. Lea también el capítulo [Browser Cleaner](#).

## Restaurar

El software crea un punto de restauración cada vez que ejecuta una modificación. Si uno de los cambios aplicados tiene efectos indeseados, puede deshacer esas modificaciones y restaurar su sistema al estado anterior a la modificación.

- 
**Seleccionar todos:** Si desea desechar todos los cambios realizados por el optimizador del sistema, seleccione aquí todos los puntos de restauración y pulse luego el botón **Restaurar**.
- 
**Restaurar:** Si desea descartar determinados cambios realizados por el optimizador del sistema, solo tiene que seleccionar los puntos de restauración deseados y pulsar luego el botón **Restaurar**.
- 
**Borrar los seleccionados:** Con este botón puede eliminar los puntos de restauración que ya no necesite.

# Browser Cleaner

G DATA Browser Cleaner puede bloquear o eliminar componentes de programa o complementos no deseados. Estos programas a menudo se instalan junto con el software gratuito, y pueden modificar la configuración del navegador o incluso espiar datos. Con Browser Cleaner puede visualizar estos programas no deseados ("PUP" = potentially unwanted programs) para los navegadores Internet Explorer, Firefox y Google Chrome, y determinar usted mismo si desea solo desactivarlos o eliminarlos por completo. La desactivación de los complementos se puede deshacer en cualquier momento.

**Nota:** G DATA Browser Cleaner es compatible con Microsoft Internet Explorer, Mozilla Firefox y Google Chrome y permite una administración extremadamente fácil de todos los complementos de navegador instalados. Con un clic del ratón se pueden desactivar o eliminar todos los plugins de la lista para librar al navegador de complementos no deseados. Mediante una opción, la herramienta muestra todos los plugins clasificados como seguros, para poder diferenciarlos rápida y fácilmente de los complementos no seguros o no deseados. G DATA Browser Cleaner se incluye en la solución de seguridad integral G DATA Total Security y está siempre a disposición de los usuarios de este software.

# Protección infantil

Con la protección infantil puede regular las pautas de navegación en Internet y el uso del PC por parte de sus hijos.

Seleccione en **Usuario** un usuario registrado en su ordenador y ajuste luego las limitaciones que le correspondan. Con el botón [Crear nuevo usuario](#) puede también crear directamente nuevas cuentas en su ordenador (por ej. para sus hijos).

- **Protección infantil para este usuario:** Aquí se puede activar o desactivar la protección infantil para el usuario seleccionado arriba.
- **Contenidos prohibidos:** En esta área se abre una ventana de diálogo en la que puede bloquear contenidos especiales de Internet para el usuario que se muestra actualmente. Haga clic en [Editar](#) para definir los contenidos prohibidos para el usuario correspondiente.
- **Contenidos permitidos:** Al pulsar en esta área se abrirá una ventana de diálogo en la que puede autorizar el acceso a contenidos especiales de Internet para el usuario activo. Haga clic en [Editar](#), para definir los contenidos permitidos para el usuario correspondiente.
- **Supervisar tiempo de uso de Internet:** Desde aquí puede determinar el tiempo y las horas en las que el usuario seleccionado puede acceder a Internet. Haga clic en [Editar](#) para definir los tiempos de uso para el usuario correspondiente.
- **Supervisar tiempo de uso del PC:** Desde aquí puede determinar el tiempo y las horas durante las cuales el usuario seleccionado puede utilizar el ordenador. Haga clic en [Editar](#) para definir los tiempos de uso para el usuario correspondiente.

Ajustes: aquí podrá modificar la configuración básica para el funcionamiento de la protección infantil y adaptarla a las necesidades individuales.

## Crear nuevo usuario

Haga clic sobre el botón **Crear nuevo usuario**. Se abre una ventana de diálogo en la que puede introducir el nombre de usuario y la contraseña.

**Nota:** Una contraseña debe tener por razones de seguridad, 8 caracteres como mínimo e incluir mayúsculas, minúsculas y cifras.

Entonces aparecerá en **Usuario** el nombre de usuario que acabamos de crear y al mismo tiempo creará una cuenta de usuario de Windows para ese usuario. Esto significa que la protección infantil se activará automáticamente con la configuración que corresponda para la persona que se haya registrado con ese nombre de usuario al iniciar Windows. Haga ahora doble clic con el ratón en el área de configuración que vaya a parametrizar para ese usuario, es decir, por ej. el veto de los **Contenidos prohibidos** o la disponibilidad exclusiva de los **Contenidos permitidos**, o bien defina para ese usuario el **Tiempo de utilización de Internet** o **Tiempo de utilización del PC** que vayan a monitorizarse.

## Contenidos prohibidos

En esta área se abre una ventana de diálogo en la que puede bloquear contenidos especiales de Internet para el usuario que se muestra actualmente. Para ello seleccione las categorías que desea bloquear marcándolas. Después haga clic en **aceptar** y las páginas web que cumplan los criterios de bloqueo quedarán bloqueadas.

Si hace clic en el botón **nuevo**, se abrirá una ventana de diálogo en la que podrá definir sus propios criterios de bloqueo (también denominados listas negras). Introduzca en primer lugar el nombre y, si lo desea, un texto informativo sobre el filtro personal creado.

Si hace clic en **aceptar**, se abre una nueva ventana en la que puede resumir los contenidos que desea prohibir mediante ese filtro.

Para ello introduzca en **Filtro** el término que desee bloquear y en **Lugar de la búsqueda** el área de la página web en la que luego se realizará la búsqueda.

Aquí tiene algunos criterios de selección:

- **URL:** Si marca esta opción, el texto que se quiera bloquear se buscará en la dirección web. Si, p. ej., desea bloquear sitios con nombres de tipo *www.chatcity.no*; *www.crazychat.co.uk*, etc., sólo tiene que introducir **chat** como *filtro*, marcar la opción **URL** y hacer clic en el botón **agregar**. A continuación se bloquearán todos los sitios que utilicen en sus nombres de dominio, es decir, en una dirección de Internet, la sucesión de caracteres *chat*.
- **Título:** Si marca esta opción, el texto que se quiera bloquear se buscará en el título de la página web. Este campo es el que aparece cuando se desea guardar una página en su lista de favoritos en forma de marcador. Si, p. ej., desea bloquear webs con nombres de tipo *Chat City Detroit* o *Teenage Chat 2005* entre otros, sólo tiene que introducir **chat** como *filtro*, marcar la opción **título** y hacer clic en el botón **agregar**. Entonces se bloquearán todos los sitios que contengan en sus títulos la sucesión de caracteres *chat*.

- **Meta:** los denominados Metatags son entradas ocultas de texto de las páginas web que sirven para que éstas aparezcan en motores de búsqueda de forma razonable o simplemente con más frecuencia. Términos de búsqueda como *sexo* o *chat* se utilizan a menudo para aumentar el acceso a las páginas. Si desea prohibir el acceso a páginas en las que entre los metatags aparezca la palabra *chat*, sólo tiene que introducir **chat** como *filtro*, seleccionar la opción **Meta** y hacer clic en **agregar**. A continuación se bloquearán todos los sitios que contengan en sus metatags la sucesión de caracteres *chat*.
- **En todo el texto:** Si desea analizar todo el contenido de texto de una página buscando el contenido que desea bloquear, introduzca simplemente el término que desea bloquear (p. ej., *chat*), marque la opción **En todo el texto** y haga clic en el botón **Agregar**. Entonces se bloquearán todos los sitios que contengan en alguna parte del texto visible la sucesión de caracteres *chat*.

No obstante, puede autorizar explícitamente páginas que entren por equivocación en el campo del filtro mediante la función de excepciones. Solo tiene que pulsar el botón **Excepciones** e indicar página correspondiente.

**Nota:** En el área **Filtros propios** puede crear y borrar sus propios filtros como desee. Para obtener más información consulte el capítulo [Filtros propios](#).

## Contenidos permitidos

Al pulsar en este área se abrirá una ventana de diálogo en la que puede autorizar el acceso a contenidos especiales de Internet por el usuario activo. Para ello, seleccione las categorías para las que desea autorizar el acceso. Después haga clic en **aceptar** y las páginas web que cumplan los criterios deseados quedarán autorizadas.

Al pulsar el botón **Nuevo** se abrirá una ventana de diálogo en la que podrá definir los contenidos autorizados por Ud. mismo (también denominados listas blancas). Introduzca en primer lugar el nombre y, si lo desea, un texto informativo sobre el filtro personal creado.

Ahora haga clic en **Aceptar**. Se abrirá una ventana en la que podrá introducir en la lista blanca los sitios web, por ejemplo, apropiados para los niños.

Introduzca en **Filtro** los componentes del nombre de dominio que desee autorizar. Si por ejemplo desea permitir el acceso a un sitio web con contenido pensado para niños, introduzca por ejemplo aquí la dirección de una página alemana para niños como es *www.fragfinn.de* con ello se permitirá el acceso a este sitio web. Introduzca ahora en **Descripción** lo que se puede encontrar en esta página, por ejemplo, *fragFINN - La Red para niños* e indique la dirección exacta del sitio en **Enlace**. La descripción y el enlace a la página serán importantes cuando el niño, por ejemplo, intente acceder a una página que no está entre las permitidas. En lugar de un mensaje de error, aparecerá entonces una página en HTML en el navegador, enumerando los sitios web incluidos en la lista blanca, incluida una descripción. De esta forma, el niño podrá acceder directamente a las páginas que tenga permitidas. Cuando haya introducido todos los datos, haga clic en **añadir** y la lista blanca se ampliará con estos datos.

**Nota:** El filtro busca segmentos en nombres de dominio. Dependiendo de los datos del filtro, los resultados pueden variar. Dependiendo de la web, será más útil utilizar otros criterios más amplios o más restringidos.

## Supervisar tiempo de uso de Internet

Desde aquí puede determinar el tiempo y las horas durante las cuales el usuario seleccionado puede acceder a Internet. Ponga para este fin una marca en **Supervisar tiempo de uso de Internet**. Ahora puede determinar cuánto tiempo al mes puede acceder el usuario a Internet, cuánto tiempo por semana y cuántas horas en determinados días de la semana. Por ejemplo, los fines de semana pueden tratarse de forma diferente para escolares que los días de entre semana. Puede introducir los intervalos correspondientes fácilmente en **días/hh:mm**, donde por ejemplo *04/20:05* indicaría un tiempo de uso de Internet de 4 días, 20 horas y 5 minutos.

**Nota:** De cara a las indicaciones para el uso de Internet cuenta siempre el menor valor. Por lo tanto, si establece un límite temporal de cuatro días al mes, pero admite cinco días en una semana, el software reduce el uso de Internet del usuario automáticamente a cuatro días.

Cuando el correspondiente usuario intenta acceder a Internet más allá del periodo autorizado, aparece en el navegador una indicación que le informa que ha excedido su cuota de tiempo.

## Bloquear horas

Con el botón **bloquear horas** puede acceder a un campo de diálogo en el que, además de limitar cuantitativamente el uso de Internet, podrá bloquear categóricamente intervalos especiales de la semana. Los periodos bloqueados se muestran en rojo, los periodos liberados, en verde. Para liberar o bloquear un periodo simplemente márkuelo con el ratón. Aparece entonces un menú contextual junto al puntero del ratón. Este menú ofrece dos posibilidades: **Autorizar tiempo** y **Bloquear tiempo**. Cuando el correspondiente usuario intenta acceder a Internet durante los periodos bloqueados, aparecerá en el navegador una pantalla que le informará que en ese momento no tiene acceso a Internet.

## Supervisar tiempo de uso del PC

Desde aquí puede determinar el tiempo y las horas durante las cuales el usuario seleccionado puede utilizar el ordenador. Para ello active la marca de **Supervisar tiempo de uso del PC**. Ahora puede determinar cuánto tiempo al mes puede acceder el usuario al ordenador, cuanto tiempo por semana y cuántas horas en determinados días de la semana. Por ejemplo, los fines de semana pueden tratarse de forma diferente para escolares que los días de entre semana. Puede introducir los intervalos correspondientes fácilmente en **días/hh:mm**. Así por ejemplo *04/20:05* indicaría un tiempo de uso de Internet de 4 días, 20 horas y 5 minutos. Con el botón **mostrar aviso antes de que expire el tiempo** podrá informar al usuario antes de que el ordenador se apague automáticamente, para darle tiempo a que pueda guardar los datos. En caso de apagarse el ordenador sin previo aviso pueden ocurrir pérdidas de datos.

**Nota:** De cara a las indicaciones para el uso del ordenador cuenta siempre el menor valor. Por lo tanto, si establece un límite temporal de cuatro días para el mes, pero admite cinco días en una semana, entonces el software reduce el uso del ordenador por el usuario automáticamente a cuatro días.

## Bloquear horas

Con el botón **bloquear horas** puede acceder a un campo de diálogo en el que, además de limitar cuantitativamente el uso del ordenador, podrá bloquear categóricamente intervalos especiales de la semana. Los periodos bloqueados se muestran en rojo, los periodos liberados, en verde. Para liberar o bloquear un periodo simplemente márkelo con el ratón. Aparece entonces un menú contextual junto al puntero del ratón. Este menú ofrece dos posibilidades: **Autorizar tiempo** y **Bloquear tiempo**.

## Filtros propios

En esta área podrá modificar las listas blancas (es decir, los contenidos permitidos) y listas negras (es decir, los contenidos prohibidos) que ha creado y crear también manualmente listas completamente nuevas.

Los siguientes tipos de listas difieren totalmente entre sí:

- **Contenidos permitidos:** Cuando seleccione para uno de los usuarios marcados arriba una lista blanca, éste podrá ver exclusivamente los sitios Web que se encuentren en ella. El administrador podrá configurar esta lista blanca según su criterio, o bien, de entre las listas blancas que haya, seleccionar la lista adecuada para cada usuario. Una lista blanca es especialmente útil para permitir a los niños más pequeños un acceso muy limitado a Internet, dándoles así la posibilidad de sacar provecho de las páginas web con contenidos pedagógicos recomendables, pero nada más.
- **Contenidos prohibidos:** Con una lista negra podrá bloquear para un usuario sitios Web seleccionados. Aparte de estas excepciones, el usuario tendría libre acceso a Internet. Tenga en cuenta que aunque a través de esta función pueden bloquearse ciertos sitios específicos, pueden permanecer disponibles, sin embargo, contenidos similares en otras páginas web. Por eso, una lista negra de direcciones de Internet nunca ofrece una protección total frente a contenidos no deseados.

Los siguientes botones le permiten editar las listas de exclusión:

- **Eliminar:** Con la función **Borrar** puede eliminar sencillamente las listas que haya seleccionado con el ratón.
- **Nuevo:** Aquí podrá crear una lista negra o una lista blanca completamente nueva. El procedimiento a seguir es el mismo que se describe en los capítulos [Contenidos prohibidos](#) y [Contenidos permitidos](#).
- **Editar:** Aquí podrá modificar el contenido de una lista existente.

## Ajustes: Registro

En este área puede modificar los ajustes básicos de las informaciones en el área de Registro. Así podrá definir si se deben protocolizar o no las violaciones contra contenidos permitidos y/o prohibidos. Cuando se lleva registro de los contenidos, puede ver los registros de los diferentes usuarios en este área.

Como los archivos de registro pueden ser muy grandes cuando se utilizan con regularidad, puede establecer que la Protección infantil le recuerde en la opción **Mostrar mensaje si el archivo alcanza \_\_\_ KB** que el archivo de registro excede ya un tamaño determinado, para que lo pueda borrar manualmente en el área de [Protocolo](#) con **Eliminar registros**.

# Cifrado

El módulo de cifrado actúa como una caja fuerte para proteger los datos sensibles. Una caja fuerte se puede utilizar por ejemplo como una unidad extra, como una partición de disco duro adicional, y es muy fácil de usar.

Para crear y gestionar las cajas fuertes puede elegir entre las siguientes opciones:

- **Actualizar:** Si ha abierto o cerrado en algún momento cajas fuertes fuera del módulo de cifrado, se recomienda pulsar **Actualizar** para poner al día la vista de estado de las cajas fuertes que administra el módulo de cifrado.
- **Abrir/Cerrar:** Aquí puede abrir o cerrar las cajas fuertes que se encuentren en su ordenador y en los medios de almacenamiento conectados. Tenga en cuenta que para abrir la caja fuerte necesitará la contraseña que le haya asignado en el momento de crearla. Para cerrar las cajas fuertes no hace falta indicar la contraseña.
- **Crear nueva codificación:** Mediante esta función puede crear una nueva caja fuerte. Se abre un asistente que le ayuda a crear la caja fuerte. Para obtener más información consulte el capítulo [Crear nueva caja fuerte](#).
- **Crear caja fuerte móvil:** En cuanto haya creado una caja fuerte, puede convertirla en portátil, configurándola de modo que pueda usarla en una memoria USB o, incluso, enviarla por correo. Para obtener más información consulte el capítulo [Crear caja fuerte móvil](#).
- **Eliminar:** En la administración de la caja fuerte dispone de una vista general de todas las cajas fuertes que están guardadas en su ordenador y en los medios de almacenamiento conectados. Aquí también puede borrar las cajas fuertes que ya no necesite. Tenga en cuenta que aquí también puede borrar las cajas fuertes sin conocer su contraseña. Por ello, debe estar completamente seguro de que ya no necesita el contenido de la caja fuerte que quiera borrar.

## Crear nueva caja fuerte

Cuando desee crear una nueva caja fuerte, un diálogo interactivo le irá guiando. Haga clic en el botón **Siguiente**, para proseguir.

## Ubicación de almacenamiento y capacidad de la caja fuerte

Por favor, indique dónde se debe guardar la caja fuerte y qué capacidad debe tener.

**Nota:** La caja fuerte es, en realidad, un archivo protegido que funciona como una partición del disco duro cuando está abierto, es decir, mediante la ubicación de almacenamiento está creando un archivo de caja fuerte en el lugar deseado de su disco duro. Aquí, sus datos se guardan cifrados. Si tiene abierta la caja fuerte y está trabajando con ella, podrá editar, borrar, copiar y mover los archivos y directorios que contenga, igual que en un disco duro o partición normales.

### Ubicación de almacenamiento

Seleccione aquí en qué soporte (por ej. disco local (C:)) se debe crear la caja fuerte.

**Nota:** Las cajas fuertes que se crean en un directorio protegido solo se pueden ver en su ordenador si el software G DATA está instalado en el ordenador. Si tuviera que desinstalar el software, ya no será posible visualizar las cajas fuertes creadas de esta manera.

### Capacidad de la caja fuerte

Seleccione a continuación una capacidad de caja fuerte posicionando correspondientemente el control deslizante. Cuenta con todo el espacio que haya disponible en la ubicación de almacenamiento elegida. Generalmente, debería permanecer al menos 2 GB por debajo de la capacidad máxima para que su sistema no se ralentice por falta de espacio en otras áreas.

**Nota:** El botón a la izquierda del control deslizante para la capacidad de la caja fuerte le brinda la posibilidad de efectuar una selección rápida. De esta manera, puede definir allí por ej. la capacidad de la caja fuerte, aumentarla o disminuirla de tal manera que en caso de ser necesario se pueda grabar en un CD, DVD o BluRay.

Ahora haga clic en **Siguiente**.



## Parámetros de la caja fuerte

En esta ventana de diálogo puede introducir los siguientes datos y ajustes para la caja fuerte:

- **Denominación de la caja fuerte:** El nombre bajo el cual la caja fuerte es administrada por el software G DATA.
- **Descripción:** Una breve descripción adicional que contiene por ej. informaciones acerca del contenido de la caja fuerte.
- **Sistema de archivos:** Aquí puede fijar si la unidad de disco virtual, que crea la caja de seguridad, utiliza el sistema de archivos FAT o NTFS. Normalmente, debería dejar aquí el registro **Selección automática**.
- **Seleccionar automáticamente unidad de disco de caja fuerte:** La caja fuerte aparece en su ordenador como una unidad de disco duro. Aquí podrá introducir una letra de unidad de disco para la caja fuerte o permitir al sistema que elija automáticamente una. Normalmente, se recomienda en este caso la selección automática.
- **Asignar unidad:** Esta selección está disponible si no permite que el software elija automáticamente la unidad de la caja fuerte.

Ahora haga clic en **Continuar**.

## Acceso a la caja fuerte

Aquí puede introducir una contraseña para la caja fuerte. Para ello, haga clic en el botón **Agregar**.

Ahora introduzca la contraseña deseada en el cuadro de diálogo que aparece en **Contraseña y Repetir contraseña**. La contraseña solo se aceptará cuando ambas contraseñas introducidas sean idénticas. Esto le protege, por ej. de introducir una contraseña distinta por error de escritura y que después no pueda restablecerla más.

Haga clic en **Agregar** para activar la contraseña y luego en **Continuar** para cerrar la configuración de la caja fuerte.

**Nota:** Al crear la caja fuerte, puede introducir varias contraseñas diferentes y, de este modo, definir diferentes permisos. De esta manera, puede crear una caja fuerte para sí mismo, en la que usted pueda leer y modificar los archivos, y a otras personas con otra contraseña les permite que puedan leer el contenido de la caja fuerte pero no modificarlo.

Si selecciona la caja fuerte después de seleccionarla y hace clic en el botón **Autorización** tendrá las siguientes posibilidades de ajustes:

- **Editar el autoarranque:** En cada caja fuerte existe un directorio llamado autoarranque. Cuando esta opción queda establecida en Sí, al abrir la caja fuerte se inician de manera automática todos los archivos ejecutables que allí se encuentran.
- **Abrir en modo "Sólo lectura":** Un usuario que abra sesión con el método de acceso solo lectura, no podrá guardar ni modificar los archivos que encuentre en la caja fuerte. Este usuario sólo podrá leerlos.
- **Abrir como soporte extraíble:** El software G DATA abre en el Explorador las cajas fuertes de datos como discos duros locales. Si desea que la caja fuerte sea visible en el sistema como soporte de datos intercambiable, active esta opción.
- **Uso compartido:** Seleccionar esta opción permite el uso compartido del directorio de la caja fuerte para otros equipos de la red. Aviso: El acceso a la caja fuerte es posible en este ajuste sin tener necesidad de introducir una contraseña. En esta situación, recomendamos una elección cuidadosa y consciente del uso compartido de la caja fuerte. El uso compartido de la caja fuerte por todos los usuarios de la red no tiene sentido en esta situación, ya que en este caso los datos son accesibles para todos.
- **Cuando el usuario cierre sesión, cerrar también la caja fuerte:** Esta opción debería estar activada habitualmente, ya que si la caja fuerte queda abierta después de cerrar la sesión de usuario, otros usuarios pueden ver el contenido de la misma.
- **Caja fuerte automática:** Todas las cajas fuertes con esta propiedad pueden abrirse con un único comando.

## Configuración de la caja fuerte

El asistente de creación de caja fuerte le informa en el último paso sobre los parámetros de configuración. Si desea modificar estos ajustes, haga clic en el botón **Atrás**. Si está de acuerdo con la configuración, pulse **Crear**.

La caja fuerte virtual y cifrada se crea en el disco duro de su ordenador. Con un último clic en el botón **Concluir proceso** se crea la caja fuerte y se abre directamente si se desea.

## Crear caja fuerte móvil

En cuanto haya creado una caja fuerte, puede convertirla en portátil, configurándola de modo que pueda usarla en una memoria USB o, incluso, enviarla por correo.

En el resumen de las cajas fuertes, seleccione una caja fuerte y pulse luego el botón **Crear caja fuerte móvil**. A continuación se abre un diálogo que le ayuda a crear una caja fuerte portátil. Pulse **Continuar** para iniciarla.

## Parámetros de la caja fuerte

Aquí tiene la posibilidad de modificar parámetros, igual que al ajustar los parámetros de las cajas fuertes estándar. Pero las cajas fuertes portátiles tienen menos posibilidades de ajuste:

- **Seleccionar automáticamente unidad de disco de caja fuerte:** La caja fuerte aparece mientras está abierta como una unidad de disco duro. Aquí podrá introducir una letra de unidad de disco para la caja fuerte o permitir al sistema que elija automáticamente una. Normalmente, se recomienda en este caso la selección automática.
- **Vincular caja fuerte con el soporte de datos:** Aquí puede determinar que la caja fuerte se use, por ejemplo, únicamente con la memoria USB o la unidad de disco duro en la que se crea. Si no vincula la caja fuerte con el soporte de datos, puede enviar, por ej., el archivo de la caja fuerte (que se reconoce por su extensión **tsnxg**) adjunto a un correo o copiarlo o moverlo a otros soportes de datos.

## Soporte

Aquí define el soporte de datos en que vaya a guardar la caja fuerte portátil. Puede tratarse, por ej., de una memoria USB, un disco duro externo o un CD/ DVD.

**Nota:** Cuando guarde una caja fuerte en un CD o DVD, ésta, claro está, solo se podrá abrir y leer. En este tipo de soportes de datos no se pueden modificar los archivos y directorios en la caja fuerte.

## Capacidad de la caja fuerte

Aquí encontrará información sobre el espacio que requiere la caja fuerte en el soporte de datos de destino. Si el espacio de memoria es demasiado grande, puede cancelar la creación de la caja fuerte portátil.

**Nota:** Además del espacio que ocupa la caja fuerte en sí misma, hay que añadir unos 6 MB del controlador, para que pueda abrir la caja fuerte en un sistema con Windows en el que no esté instalado el software G DATA.

## Finalizar

Termine de crear la caja fuerte portátil haciendo clic en el botón **Concluir proceso**. Si lo desea, ahora aparece en el navegador de archivos el archivo en que se encuentra la caja fuerte portátil en soporte de memoria deseado.

## Abrir caja fuerte móvil

Cuando desee abrir una caja fuerte portátil en un ordenador con Windows, pero sin el módulo de Caja fuerte de datos G DATA, puede acceder de todos modos a los datos fácilmente: solo tiene que seleccionar en una memoria USB, disco duro portátil o CD/DVD el archivo de programa **start.exe** o **start** en la carpeta **TSNxG\_4**. Al pulsarlo, se abre un cuadro de diálogo con el que puede abrir la caja fuerte de datos o cerrarla (si ya estaba abierta).

**Atención:** Cuando se utilice Caja fuerte de datos G DATA por primera vez en un ordenador, se cargarán los correspondientes datos de controladores y elementos del programa. A continuación es necesario efectuar un reinicio del ordenador. Después del reinicio del PC, vuelva a seleccionar la opción **inicio** o **Start.exe**.

Ahora introduzca su contraseña o utilice uno de los otros métodos de acceso a la caja fuerte.

Ahora se abrirá la caja fuerte y su contenido podrá ser utilizado.

Después de registrarse correctamente en la caja fuerte, aparecerá en el explorador de Windows, junto a las unidades de disco locales, el símbolo de la caja fuerte como unidad de disco adicional con la letra de unidad de disco correspondiente. Cualquier usuario de una caja fuerte móvil puede transferir datos de la caja fuerte al ordenador. Si se utiliza una caja fuerte móvil en un soporte de datos USB o en una memoria flash, el usuario que cuente con la autorización necesaria puede copiar los datos de la caja fuerte del ordenador a la caja fuerte.

El cierre de una caja fuerte móvil se realiza de modo similar a la apertura. Haga doble clic en la letra de la unidad de disco de la caja fuerte

---


o seleccione un comando adecuado en el menú contextual (clic derecho del ratón).


**Atención:** Se recomienda cerrar la caja fuerte una vez que acabe de trabajar con ella, antes de sacar el soporte de datos extraíble. Vaya al soporte de datos extraíble, abra el directorio de G DATA y pulse Start.exe. Se abre una ventana de diálogo en la que se puede cerrar la caja fuerte.

# Administrador de autoarranque

Con el Administrador de autoarranque se pueden administrar los programas que arrancan automáticamente al iniciarse Windows. Normalmente, estos programas se cargan directamente al arrancar el sistema. Si se pueden administrar con el Administrador de autoarranque, pueden también iniciarse con demora o en función del grado de ocupación del sistema o del disco duro. Esto permite un arranque más rápido del sistema, mejorando así el rendimiento del ordenador.

Al abrir el Administrador de autoarranque, podrá ver en el lado izquierdo una lista de todos los programas de autoarranque instalados en su ordenador. Normalmente se inician sin demora, es decir, directamente al arrancar Windows, lo que puede ocasionar que su ordenador arranque muy despacio.

 Solo tiene que seleccionar con el icono de flecha los programas de autoarranque que desee iniciar con demora, aligerando así el proceso de arranque de Windows. Con esta medida, su sistema operativo Windows arrancará y estará operativo notablemente más rápido.

 Pero si desea posteriormente que un programa de autoarranque vuelva a iniciarse sin demora, solo tiene que sacarlo de nuevo de la carpeta **Autoarranque con demora** y llevarlo a la carpeta **Autoarranque sin demora**.

## Ajustar demora

Si tiene un programa en la carpeta Autoarranque con demora, puede determinar con toda facilidad los minutos que se demorará el inicio de este software. Solo tiene que pulsar el programa y seleccionar en la columna de demora el intervalo deseado.

Aquí tiene a su disposición las siguientes entradas:

- **No iniciar:** La aplicación está administrada por el Administrador de autoarranque, pero no arrancará también la próxima vez que se inicie el sistema. Permanece inactiva.
- **1 - 10 minutos:** La aplicación se inicia más tarde, tantos minutos como se haya seleccionado aquí.
- **Inicio automático:** La aplicación se inicia automáticamente en función de la carga del disco duro o CPU. Esto significa que otra aplicación de autoarranque no se iniciará hasta que no remita la carga del sistema causada por el arranque de otras aplicaciones de autoarranque u otros procesos.

## Propiedades

Haciendo doble clic en la entrada de un programa en las listas del Administrador de autoarranque, obtendrá información detallada sobre el software administrado.

# Control de dispositivos

Con el control de dispositivos podrá definir para su ordenador los soportes de memoria que se permiten para leer o grabar datos. Así puede impedir, por ejemplo, que se copien datos privados en una memoria USB o en un CD. Además, podrá definir exactamente en cuales soportes de datos intercambiables, como memorias o discos duros USB, se pueden descargar datos. Así por ej. puede usar su propio disco duro USB para salvaguardar datos, pero dejar sin acceso a otros discos duros.

En esta vista general puede ver cómo afectan los ajustes del control de dispositivos al usuario correspondiente. Mediante el botón "Editar reglas" puede adaptar los ajustes para el dispositivo y el usuario según sus preferencias.

**USB Keyboard Guard:** Nuestro software ahora le protege también contra una nueva amenaza: Memorias USB infectadas que se hacen pasar por teclados frente al sistema operativo, y así pueden introducir software dañino subrepticamente. El software le informa cuando su sistema da por sentado que se trata de un teclado nuevo al introducir un dispositivo USB, y usted puede confirmar si esto es así o no mediante la introducción de un PIN. Por supuesto, el software recuerda todos los teclados ya autorizados y no le volverá a consultar en relación a ellos.

# Ajustes

En el área **Ajustes** se pueden configurar cada uno de los módulos del programa según sus deseos. Normalmente, no es necesario realizar aquí modificaciones, ya que su software G DATA ya fue configurado óptimamente para su sistema durante la instalación. Para los ajustes tiene disponibles las siguientes funciones avanzadas:



**Guardar ajustes:** Aquí puede guardar los ajustes realizados en un archivo GDataSettings. Si desea usar su G DATA Software en varios ordenadores, puede realizar así los ajustes en un ordenador, guardarlos y cargar luego el archivo de configuración en otros ordenadores.



**Cargar ajustes:** Aquí se puede cargar el archivo GDataSettings creado en este o en otro ordenador.



**Restablecer ajustes:** Si se ha confundido en algo al realizar los ajustes de su software G DATA, con este botón se pueden restablecer todos los ajustes del programa a su estado de fábrica. Puede escoger además si desea restablecer todas o solo determinadas áreas de ajuste. Solo tiene que marcar con una marca de verificación las secciones que desee restablecer.

## General

### Seguridad/rendimiento

Si desea usar su protección antivirus en un ordenador lento, tiene la posibilidad de mejorar el rendimiento - es decir, la velocidad de trabajo del ordenador - a costa del nivel de seguridad. En la representación del diagrama se ve el efecto que tiene una optimización de los ajustes.

- **Ordenadores estándar (recomendado):** Aquí tendrá a su disposición la protección óptima del software G DATA. Los dos motores antivirus del programa funcionan a la par. Además, se comprueba si tienen malware todos los accesos de lectura y escritura de su ordenador.

**Motor:** Su software G DATA funciona con dos motores antivirus. La utilización de ambos motores garantiza unos resultados óptimos en la prevención de virus.

- **Ordenadores lentos:** En los ordenadores lentos, para no perjudicar la velocidad, su software G DATA puede funcionar con solo un motor. Esta protección es la única que le ofrecen numerosos programas antivirus corrientes que funcionan exclusivamente con un motor. Este modo de protección sigue siendo bueno. Además puede determinar que solo se compruebe en modo de vigilante cuando se realicen operaciones de escritura. De esta forma se examinan solo los datos nuevos que se guardan, lo que mejora aún más el rendimiento.
- **Definido por el usuario:** Aquí puede seleccionar individualmente si desea usar los dos motores o solo uno y determinar para el Vigilante si se debe activar al leer y escribir, solo al escribir (ejecutar) o en ningún caso (opción no recomendada).

## Contraseña

Puede proteger los ajustes de su software G DATA fijando una contraseña. De este modo, otro usuario de su ordenador, por ej., no podrá desconectar el Vigilante de virus o el escaneo en modo reposo.

Para asignar una contraseña, escríbala primero en "Contraseña" y luego repítala en "Repetir contraseña", para evitar errores ortográficos. Además, puede introducir un recordatorio de la contraseña en "Recordatorio".

**Nota:** El recordatorio se muestra cuando se ha indicado una contraseña equivocada. Por eso, este recordatorio solo le debe permitir a usted deducir la contraseña.

**Nota:** Esta protección por contraseña constituye otra característica protectora del software. La máxima seguridad se obtiene usando varias cuentas de usuario. Es decir, conviene usar como administrador una cuenta de usuario específica para gestionar, por ej., la protección antivirus y los otros usuarios (como por ej. los hijos, amigos o familiares) pueden usar cuentas de usuario propias con derechos limitados que no les permita realizar aquí cambios.

**Nota:** Si, por ejemplo, después de crear varias cuentas de usuario, ya no necesita contraseña para su software G DATA, puede anular la obligación de introducir una contraseña con el botón "Eliminar contraseña".

# AntiVirus

## Protección en tiempo real

La protección en tiempo real del Vigilante de virus revisa su ordenador de arriba a abajo para detectar virus, controla los procesos de escritura y lectura y, en cuanto un programa intenta ejecutar una función dañina o desea propagar archivos maliciosos, el Vigilante lo evita. ¡El Vigilante de virus es su protección más importante! Nunca debe estar desactivado.

Aquí tiene a su disposición las siguientes opciones:

- **Estado del vigilante:** Defina en esta opción si el Vigilante debe estar activado o desactivado.
- **Utilizar motores:** El software trabaja con dos motores (= del inglés engine), es decir con dos programas de comprobación de virus completamente independientes entre sí. Cada motor de por sí ya protegería el ordenador en un alto grado frente a los virus, pero justo la combinación de los dos motores proporciona los mejores resultados. En los ordenadores más antiguos y lentos, la utilización de un único motor puede acelerar la comprobación de virus. No obstante y por lo general, conviene mantener el ajuste **Ambos motores**.
- **Archivos infectados:** Si se detectan virus se le preguntará en el ajuste estándar cómo desea proceder con el virus y el archivo infectado. Si siempre va a realizar la misma acción, puede ajustar la opción elegida aquí. El ajuste que ofrece la máxima seguridad para sus datos es **desinfectar (si no es posible: en cuarentena)**.
- **Archivos comprimidos infectados:** Aquí puede determinar si los ficheros de archivos comprimidos (es decir, los archivos con la extensión RAR, ZIP o también PST) tendrán un tratamiento distinto de los archivos normales. No obstante, observe que al poner un archivo comprimido en cuarentena éste se puede dañar, de modo que incluso al recuperarlo de nuevo de la [Cuarentena](#) ya no se pueda utilizar más.
- **Supervisión de conducta:** Si la supervisión de conducta está activada, cada actividad en el sistema es controlada de manera independiente por el Vigilante de virus. De esta manera, se reconocen también virus para los cuales aún no existen firmas.
- **Anti-ransomware:** Protección frente a los cripto-virus.
- **Exploit Protection:** El llamado exploit aprovecha las vulnerabilidades de las aplicaciones habituales y, en el peor de los casos, puede llegar a tomar el control de su ordenador sirviéndose de estas vulnerabilidades. Los exploits pueden atacar incluso si se actualizan regularmente las aplicaciones (como p. ej. lector de PDF, navegador, etc.). Exploit Protection le protege contra estos accesos, y también de forma proactiva contra ataques hasta ahora desconocidos.

## Excepciones

Haciendo clic en el botón Excepciones puede excluir de la comprobación determinadas unidades de disco, directorios y archivos, lo que puede acelerar bastante el reconocimiento de virus.

Proceda como se describe a continuación:

- 1 Haga clic en el botón de **excepciones**.
- 2 En la ventana **Excepciones del vigilante**, haga clic en **Nuevo**.
- 3 Seleccione ahora si desea excluir una unidad, un directorio, un archivo y/o un tipo de archivo.
- 4 A continuación, seleccione allí el directorio o la unidad que desea proteger. Para proteger archivos, introduzca el nombre de archivo completo en el campo de entrada debajo de la máscara de archivo. Aquí también puede utilizar comodines.

**Nota:** El funcionamiento de los comodines es el siguiente:

- El signo de interrogación (?) representa caracteres sueltos.
- El signo de asterisco (\*) representa una secuencia completa de caracteres.

Para proteger, por ejemplo, todos los archivos con la extensión .sav, deberá introducir \*.sav. Para proteger una serie especial de archivos con nombres numerados sucesivamente (por ej. texto1.doc, texto2.doc, texto3.doc), introduzca por ejemplo texto?.doc.

Este procedimiento se puede repetir cuantas veces haga falta y volver a borrar o modificar las excepciones que se encuentren disponibles.

## Avanzado

Con el botón **avanzado** puede también determinar las comprobaciones adicionales que deba realizar el Vigilante de virus.

Por lo general, aquí no hace falta que realice ningún ajuste más.

- **Modo:** Aquí puede definir si los archivos en ejecución deben ser comprobados sólo durante la lectura o la escritura. Si la comprobación se realiza durante la escritura de un archivo, entonces al crear un nuevo archivo o versión de archivo se comprueba directamente si un proceso desconocido ha infectado eventualmente este archivo. En caso contrario, sólo se comprobará cuando éstos sean leídos por programas.
- **Supervisar especialmente las carpetas críticas:** Mediante esta función puede comprobar de forma más precisa las carpetas especialmente críticas, p. ej. carpetas compartidas en red, datos personales o servicios en la Nube (como p. ej. Microsoft Dropbox, OneDrive, Google Drive, etc.). Después de seleccionarlas en el cuadro de diálogo, estas se comprueban siempre – independientemente de los ajustes que se utilicen para todos los demás archivos, carpetas o directorios– en el modo **Comprobar al leer y escribir**. Si en general ha seleccionado el modo **Comprobar al leer y escribir** para todos los archivos, esta posibilidad de configuración para las carpetas críticas aparece atenuada.
- **Comprobar accesos a la red:** Cuando existe una conexión de red de su ordenador a un ordenador que no está protegido (p.ej. ordenadores portátiles ajenos), se recomienda comprobar también durante la transmisión si hay posibles programas dañinos. Si utiliza su ordenador como única ubicación sin acceso de red, no se debe activar esta opción. Si ha instalado un programa antivirus en todos los ordenadores de la red, se recomienda también desactivar esta opción ya que, de lo contrario, se comprobarían doblemente algunos archivos, lo que afectaría negativamente la velocidad.
- **Heurístico:** En el análisis heurístico los virus no se reconocen utilizando las actualizaciones de virus que le proporcionamos regularmente, sino sobre la base de ciertas características típicas del software dañino. Este método es otro plus de seguridad, que sin embargo en algunos casos puede producir una alarma de error.
- **Archivos comprimidos:** La comprobación de los datos comprimidos en los archivos comprimidos (se reconocen por su extensión, por ej., ZIP, RAR o también PST) requiere mucho tiempo y, por lo general, puede omitirse si el Vigilante de virus está siempre activo en el sistema. Para aumentar la velocidad de la comprobación de virus puede limitar la capacidad a un determinado valor en kilobytes (tamaño) de los ficheros de archivos comprimidos que se comprueban.
- **Comprobar archivos comprimidos de correo:** Como el programa ya ha comprobado si los correos entrantes y salientes están infectados con virus, en la mayoría de los casos es conveniente omitir las comprobaciones regulares de archivos comprimidos de correo electrónico, ya que este proceso puede durar varios minutos, dependiendo del tamaño del archivo comprimido del correo.
- **Comprobar áreas del sistema al iniciarlo:** Por lo general, no se deben excluir las áreas del sistema de su ordenador (p.ej. sectores de arranque) en el control de virus. Puede determinar si se comprueba al iniciar el sistema o al cambiar de medio (p.ej. CD-ROM nuevo). Como norma general, debe activar al menos una de estas dos funciones.
- **Comprobar áreas del sistema al cambiar de medio:** Por lo general, no se deben excluir las áreas del sistema de su ordenador (p.ej. sectores de arranque) en el control de virus. Puede determinar aquí si se comprueba al iniciar el sistema o al cambiar de medio (CD-ROM nuevo o similar). Como norma general, debe activar al menos una de estas dos funciones.
- **Comprobar dialer / spyware / adware / riskware:** Con el software también puede comprobar si su sistema contiene dialer y otros programas dañinos. Se trata, por ejemplo, de programas que establecen conexiones caras con Internet, sin conocimiento del usuario y que, desde el punto de vista del daño económico que pueden causar, se asemejan mucho a los virus. Entre otras cosas, estos programas guardan secretamente información sobre los sitios web que el usuario visita o incluso todas las entradas que realiza a través del teclado (y por tanto también sus contraseñas) y, en cuanto pueden, las transmiten a terceras personas a través de Internet.
- **Comprobar solo archivos nuevos o modificados:** Si activa esta función, al realizar la comprobación se saltarán los archivos que desde hace mucho tiempo no se han modificado y que anteriormente habían sido reconocidos como no dañinos. Esto brinda una ganancia en el rendimiento del trabajo diario, sin poner en riesgo su seguridad.



# Comprobación de virus manual

Aquí se pueden realizar los ajustes básicos del programa para la Comprobación de virus.

Pero no son necesarios para el uso normal.

- **Utilizar motores:** El software trabaja con dos motores (= del inglés engine), es decir con dos programas de comprobación de virus sintonizados entre sí. En los ordenadores más antiguos y lentos, la utilización de un único motor puede acelerar la comprobación de virus. No obstante y por lo general, conviene mantener el ajuste **Ambos motores**.
- **Archivos infectados:** ¿Su software ha encontrado un virus? En el ajuste estándar, el software le pregunta lo que desea hacer con el virus y el archivo infectado. Si siempre va a realizar la misma acción, puede ajustar la opción elegida aquí. El ajuste que ofrece la máxima seguridad para sus datos es **desinfectar (si no es posible: en cuarentena)**.
- **Archivos comprimidos infectados:** Aquí puede determinar si los ficheros de archivos comprimidos (es decir, los archivos con la extensión RAR, ZIP o también PST) tendrán un tratamiento distinto de los archivos normales. No obstante, observe que al poner un archivo comprimido en cuarentena éste se puede dañar, de modo que incluso al sacarlo de nuevo de la [Cuarentena](#) ya no se pueda utilizar más.
- **En caso de sobrecarga del sistema, interrumpir la prueba del antivirus:** Normalmente, una comprobación de virus solo debe realizarse cuando el usuario no esté utilizando el ordenador. Pero si lo está usando en ese momento, la comprobación de virus hace una pausa para que el usuario tenga a su disposición toda la velocidad de cálculo del ordenador. Así, el examen de virus se produce mientras el usuario no está trabajando en el ordenador.

## Excepciones

Haciendo clic en el botón Excepciones puede excluir de la comprobación determinadas unidades de disco, directorios y archivos, lo que puede acelerar bastante el reconocimiento de virus.

Proceda como se describe a continuación:

1. Haga clic en el botón de excepciones.
2. En la ventana Excepciones para la comprobación manual del ordenador, haga clic en Nuevo.
3. Seleccione ahora si desea excluir una unidad, un directorio, un archivo y/o un tipo de archivo.
4. A continuación, seleccione allí el directorio o la unidad que desea proteger. Para proteger archivos, introduzca el nombre de archivo completo en el campo de entrada debajo de la máscara de archivo. Aquí también puede utilizar comodines.

**Nota:** El funcionamiento de los comodines es el siguiente:

- El signo de interrogación (?) representa caracteres sueltos.
- El signo de asterisco (\*) representa una secuencia completa de caracteres.

Para proteger, por ejemplo, todos los archivos con la extensión .sav, deberá introducir \*.sav. Para proteger una serie especial de archivos con nombres numerados sucesivamente (por ej. texto1.doc, texto2.doc, texto3.doc), introduzca por ejemplo texto?.doc.

Este procedimiento se puede repetir cuantas veces haga falta y volver a borrar o modificar las excepciones que se encuentren disponibles.

**Aplicar también las excepciones en el escaneo de modo de reposo:** Mientras que en la comprobación de virus manual se escanea el ordenador de manera precisa en búsqueda de virus y éste no debería utilizarse para otras tareas, el escaneo de modo de reposo es una comprobación inteligente de virus que continua realizando comprobaciones en búsqueda de una nueva infección con virus. El escaneo de modo de reposo trabaja como un salvapantallas siempre que no se utilice su ordenador durante un rato y se detiene automáticamente cuando se vuelve a utilizar el ordenador, para poder así garantizar un alto rendimiento. Aquí puede establecer si también se deben definir los archivos de excepciones o los directorios de excepciones para el escaneo de modo de reposo.

## Avanzado

Haciendo clic en el botón "Avanzado" se pueden realizar ajustes más detallados para la comprobación de virus.

No obstante, en la mayoría de los casos, la configuración estándar prevista es más que suficiente.

- **Tipos de archivo:** Aquí puede determinar qué tipos de archivo deberá comprobar el software ante posibles virus. La selección de la opción Sólo archivos de programa y documentos reporta algunas ventajas en cuestión de velocidad.
- **Heurístico:** En el análisis heurístico, los virus no sólo se detectan mediante las bases de datos de virus que recibe cada vez que actualiza el software antivirus, sino que también se determinan por ciertas características típicas de los virus. Este método es otro plus de seguridad, que sin embargo en algunos casos puede producir una alarma de error.
- **Archivos comprimidos:** La comprobación de los datos comprimidos en los archivos comprimidos (se reconocen por su extensión, por ej., ZIP, RAR o también PST) requiere mucho tiempo y, por lo general, puede omitirse si el Vigilante de virus está siempre activo en el sistema. Para aumentar la velocidad de la comprobación de virus puede limitar la capacidad a un determinado valor en kilobytes (tamaño) de los ficheros de archivos comprimidos que se comprueban.
- **Comprobar archivos comprimidos de correo:** Aquí se establece si también sus archivos de correo deben ser comprobados en búsqueda de infecciones.
- **Comprobar áreas del sistema:** Por lo general, no se deben excluir las áreas del sistema de su ordenador (p.ej. sectores de arranque) en el control de virus.
- **Comprobar dialer / spyware / adware / riskware:** Con esta función también puede comprobar si su sistema contiene dialer y otros programas dañinos. Se trata, por ejemplo, de programas que establecen conexiones caras con Internet, sin conocimiento del usuario y que, desde el punto de vista del daño económico que pueden causar, se asemejan mucho a los virus. Entre otras cosas, estos programas guardan secretamente información sobre los sitios web que el usuario visita o incluso todas las entradas que realiza a través del teclado (y por tanto también sus contraseñas) y, en cuanto pueden, las transmiten a terceras personas a través de Internet.
- **Comprobar rootkits:** Los rootkits intentan soslayar los métodos convencionales de detección de virus. Por eso siempre es recomendable una revisión adicional para detectar estos agentes dañinos.
- **Comprobar solo archivos nuevos o modificados:** Si activa esta función, al realizar la comprobación se saltarán los archivos que desde hace mucho tiempo no se han modificado y que anteriormente habían sido reconocidos como no dañinos. Esto brinda una ganancia en el rendimiento del trabajo diario, sin poner en riesgo su seguridad.
- **Elaborar registro:** Al marcar esta casilla puede establecer que el programa cree un registro sobre el proceso de comprobación de virus. Este registro puede verse después en el área **Registros**.
- **Ofrecer comprobación de virus para soportes de datos intercambiables:** Si marca esta casilla, al conectar un soporte de datos intercambiable (también memorias USB, discos duros externos, etc.) a su ordenador, se le preguntará si quiere comprobar este dispositivo en busca de virus.

## Actualizaciones

Si la actualización del software o de las firmas de virus vía Internet no funciona, en esta área puede proporcionar todos los datos necesarios para posibilitar una actualización automática. En las opciones, introduzca los datos de acceso (el nombre de usuario y la contraseña) que recibió por correo electrónico cuando registró su software online. Estos datos le identificarán en el Servidor de actualizaciones G DATA y las actualizaciones se realizarán de forma completamente automática.

Si usted ha adquirido una nueva licencia y desea activarla, seleccione [Activar licencia](#). La [Configuración de Internet](#) muestra opciones especiales que sólo se necesitan en casos excepcionales (servidor proxy u otra región). La comprobación de versión sólo debería estar desactivada temporalmente, si experimenta dificultades en la actualización de las firmas de virus.

**Administrar accesos:** Con esta opción tiene la posibilidad de determinar a través de qué conexiones a Internet desea obtener actualizaciones de firmas y de programa. Esto es especialmente útil si está conectado temporalmente a una red en la que la transferencia de datos es de pago, por ejemplo, en determinadas tarifas de telefonía móvil sin tarifa plana de datos real.

**Importación/Exportación de firmas de virus:** En ordenadores que se conectan a Internet solo en raras ocasiones o no se conectan nunca, o en los que existen limitaciones del volumen de datos de las descargas, puede actualizar las firmas de virus también desde un soporte de datos (p. ej. una memoria USB), es decir, realizar una **Actualización offline**. Para ello, debe exportar las firmas de virus a un soporte de datos en un ordenador que esté conectado a Internet y que disponga de los permisos necesarios, y luego importarlas en el ordenador sin conexión a Internet mediante la función "Importar desde". Así el sistema de este ordenador estará también protegido mediante las últimas firmas de virus. Al contrario de lo que sucede con las actualizaciones de firmas de virus

que se realizan regularmente por Internet, en este caso el propio usuario ha de encargarse de que las actualizaciones de firmas se hagan tan a menudo como sea posible.

## Actualizar firmas de virus automáticamente

Si no desea que el software G DATA se ocupe de manera automática de actualizar las firmas de virus a su estado más actual, entonces puede quitar la marca de esta opción. La desconexión, no obstante, representa un alto riesgo para la seguridad y sólo debería realizarse en casos excepcionales. Si el intervalo entre las actualizaciones le resulta demasiado corto, puede adaptarlo de manera individual y por ej. establecer que se realice sólo cuando exista conexión a Internet. En el caso de los ordenadores que no están conectados permanentemente a Internet, esta opción resulta muy útil.

**Elaborar registro:** Si activa aquí una marca de verificación, cada actualización de las firmas de virus quedará registrada. Este registro se puede consultar en la funciones adicionales del software G DATA (en el [Centro de seguridad](#) con la opción [Registros](#)). Además de estos registros encontrará informaciones acerca de virus encontrados y otras acciones que el programa haya ejecutado.

## Activar licencia

Si aún no hubiese registrado su software G DATA, puede hacerlo ahora e introducir su número de registro y los datos de cliente. Encontrará el número de registro según sea el tipo de producto, por ej. en el dorso del manual del usuario, en el correo electrónico de confirmación al descargar el software o en la caja del CD. Mediante la introducción del número de registro se activa su producto.

Haga clic en el botón **Registro** y se generarán sus datos de acceso en el Servidor de actualización. Si el registro se ha realizado correctamente aparecerá una pantalla informativa con el aviso **el registro se ha realizado correctamente**, de la que puede salir con el botón de cerrar.

**Atención:** Conserve sus datos de acceso que también ha recibido por correo electrónico para su archivo y las posibles nuevas instalaciones del software. Por esta razón, asegúrese de que es correcta la dirección de correo electrónico que ha indicado en el registro online. En caso contrario no dispondrá de los datos de acceso.

Por último, se cargan los datos de acceso de forma automática en la pantalla de entrada original y ahora puede actualizar las firmas de virus a través de Internet.

**¿No puede activar su licencia?** Si no puede registrarse en el servidor puede deberse quizás a un servidor proxy. Por favor, haga clic en el botón [Ajustes de Internet](#). Aquí puede realizar los ajustes para la conexión a Internet. Normalmente, en caso de problemas con la actualización de las firmas de virus, debería comprobar primero si puede acceder a Internet con el navegador de Internet (p. ej. Internet Explorer). Si no puede establecer una conexión a Internet, el problema seguramente estará en el área de la conexión a Internet y no en los datos del servidor proxy.

## Ajustes de Internet

Si utiliza un servidor proxy, coloque la marca de verificación en **Utilizar servidor proxy**. Solo debería cambiar esta configuración cuando la actualización de firmas de virus no funcione. En cuanto a la dirección proxy diríjase en su caso necesario a su administrador del sistema o proveedor de conexión a Internet. En caso necesario, puede introducir aquí además los datos de acceso para el servidor proxy.

**Servidor proxy:** Un servidor proxy conecta peticiones con redes y las distribuye en los ordenadores conectados. Si usted, por ejemplo, utiliza su ordenador en una red de una empresa, puede ser buena idea entrar en la red a través de un servidor proxy. Normalmente, en caso de problemas con la actualización de las firmas de virus, debería comprobar primeramente si puede acceder a la red con el navegador de Internet. Si no puede establecer una conexión a Internet, el problema seguramente estará en el área de la conexión a Internet y no en los datos del servidor proxy.

## Protección Web

Cuando la protección Web está activa, los contenidos de internet se analizan ya al navegar para detectar posible software dañino. Aquí puede realizar los siguientes ajustes.

- **Comprobar contenidos de Internet (HTTP):** Las opciones de la protección web permiten definir la comprobación de virus de todos los contenidos HTTP ya al navegar. Los contenidos infectados no serán ejecutados y las páginas correspondientes no se visualizarán. Con este fin marque la casilla de verificación en **Comprobar contenidos de Internet (HTTP)**.

Si no desea que se verifiquen los contenidos de Internet, cuando se ejecuten los archivos infectados se activará el Vigilante de virus. Por lo tanto, su sistema está protegido también sin la verificación de los contenidos de Internet, mientras el vigilante de virus está activado.

Puede definir determinadas páginas web también como excepciones si las considera inofensivas. Puede obtener más información en el capítulo [Definir excepciones](#). Con el botón [Avanzado](#) se pueden realizar otros ajustes para tratar los contenidos de Internet.

- **Protección antiphishing:** Con el método del Phishing los ciberdelincuentes intentan llevar a los clientes de un banco o de una tienda online a una página Web falsificada para, una vez allí, sustraerles sus datos. La activación de esta protección antiphishing es muy recomendable.
- **Enviar direcciones de páginas de Internet infectadas:** Con esta función y de modo totalmente anónimo (por supuesto), puede notificarnos automáticamente las páginas de Internet que el software considere peligrosas. Procediendo así mejora la seguridad para todos los usuarios.
- **BankGuard - protección de navegador:** Los troyanos bancarios se están convirtiendo en una amenaza cada vez más importante. En cuestión de horas, los cibercriminales desarrollan nuevas variantes de malware (por ejemplo, ZeuS, SpyEye) para robarle su dinero. Los bancos se ocupan de la seguridad del tráfico de datos en Internet, pero estos datos se descodifican en el navegador y justo aquí es donde atacan los troyanos bancarios. La tecnología puntera de G DATA BankGuard asegura las transacciones bancarias desde el principio y las protege inmediatamente allí donde se produce el ataque. G DATA BankGuard comprueba la autenticidad de las bibliotecas de red usadas, asegurando así que ningún troyano bancario llegue a manipular el navegador de Internet. Se recomienda dejar activada la protección de G DATA BankGuard.

Información: Aparte del método man-in-the-middle, en el que el atacante influye sobre la comunicación entre el usuario y el ordenador de destino, también existe el método de ataque man-in-the-browser (MITB). En este método, el atacante infecta el propio navegador y accede a los datos antes de que estos se codifiquen. El módulo BankGuard también le protege frente a este tipo de ataques, mediante la comparación de la denominada huella digital de un archivo o de una parte de una página web con una base de datos en Internet. De este modo, se detecta inmediatamente una estafa, y el software G DATA sustituye la conexión de datos fraudulenta automáticamente por la original.

- **Protección frente a keyloggers:** La protección frente a keyloggers vigila también, independientemente de las firmas de virus, si en su sistema se están espiando las pulsaciones de teclado. De esta forma se evita que los atacantes puedan también registrar sistemáticamente la introducción de contraseñas. Esta opción debe permanecer siempre activada.

## Definir excepciones

Para definir una página web como excepción en la lista blanca, proceda del modo siguiente:

- 1 Haga clic en el botón **definir excepciones**. Aparecerá entonces la ventana lista blanca. Se muestran las páginas web que haya clasificado como seguras y las haya apuntado aquí.
- 2 Para añadir una página web más, haga clic en el botón **nuevo**. Se abre el diálogo de entrada de datos. En el campo **URL**, indique la dirección de la página web, por ej. (www.unbedenklichesite.de) y en **Observación** puede, si lo desea, apuntar brevemente por qué ha incluido esta página. Confirme los datos introducidos haciendo clic en **Aceptar**.
- 3 Ahora confirme con un clic en **Aceptar** todas las modificaciones realizadas en la lista blanca.

Para borrar una página Web que figure en la Lista blanca, selecciónela en la lista con el ratón y luego simplemente pulse con el ratón el botón **borrar**.

## Avanzado

Aquí puede establecer qué puerto del servidor debe ser supervisado por la protección Web. Por regla general, para una supervisión del navegador normal basta con el puerto 80.

- **Impedir exceso de tiempo en el navegador:** Como el software procesa los contenidos de Internet antes de ser presentados en su navegador de Internet y para esto necesita un cierto tiempo, dependiendo del tráfico de datos puede suceder que el navegador muestre un mensaje de error, porque no recibe inmediatamente los datos que está examinando el antivirus para encontrar rutinas maliciosas. Activando la casilla **Impedir exceso de tiempo en el navegador** se suprime un mensaje de error de este tipo y en cuanto se ha comprobado que los datos del navegador no contienen virus, se entregan con total normalidad al navegador web.
- **Limitación de tamaño para descargas:** Con ello puede evitar la comprobación HTTP de los contenidos web demasiado grandes. Los contenidos serán comprobados después por el vigilante de virus en cuanto se active cualquier rutina maliciosa. La ventaja de esta limitación de tamaño reside en que no se producen retrasos al navegar por Internet debidos al control de virus.

## Comprobación de correo electrónico

La comprobación de correo electrónico le permite explorar los emails entrantes y salientes y sus archivos adjuntos y eliminar directamente las posibles infecciones en el origen. Cuando el software encuentra un virus, puede borrar directamente los archivos adjuntos o reparar los archivos infectados.

**Atención:** En Microsoft Outlook, los emails se escanean mediante un plugin. Esta utilidad proporciona la misma protección que la función de protección basadas en POP3/IMAP dentro de las opciones de antivirus. Después de instalar este plugin encontrará la función **Comprobar carpeta** en la opción **Herramientas** del menú de Outlook. Con esta función puede revisar cada una de sus carpetas de correos para detectar si tienen virus.

## Correos entrantes

Tiene disponibles las siguientes opciones para protegerse de los virus en los correos entrantes:

- **En caso de infección:** Aquí puede determinar qué debe suceder al descubrir un mensaje de correo infectado. Según el uso que le da a su ordenador, aquí se recomiendan varios ajustes. En general, se recomienda configurar la opción **Desinfectar (si no es posible: eliminar datos adjuntos/texto)**.
- **Comprobar correos electrónicos recibidos:** Activando esta opción se comprobará si hay virus en todos los correos electrónicos que le llegan mientras está trabajando con el ordenador.
- **Adjuntar informe a los correos infectados recibidos:** Si ha activado la opción de informe, cada vez que se detecte un virus aparecerá la advertencia **VIRUS** en la línea de asunto del correo infectado y al inicio del texto del correo **el aviso ¡Atención! Este correo contiene el siguiente virus** seguido del nombre del virus e información sobre si se ha podido borrar el virus o reparar el archivo infectado.

## Correos salientes

Para evitar que usted mismo, inadvertidamente, pueda propagar virus, el software le ofrece la posibilidad de verificar que sus correos estén exentos de virus antes de enviarlos. Si se da la eventualidad de que vaya a enviar un virus (involuntariamente), aparece el mensaje **El correo [Asunto] contiene el virus siguiente: [nombre del virus]**. El correo no se puede enviar y el correo electrónico correspondiente no se envía. Para que en los correos salientes se compruebe si tienen virus antes de enviarlos, active la marca de verificación en **Escanear correos antes de enviarlos**.

## Opciones de escáner

Aquí puede conectar o desconectar las opciones generales de la comprobación de virus:

- **Utilizar motores:** El software utilizan dos motores antivirus y dos unidades de análisis sintonizadas. La utilización de ambos motores garantiza unos resultados óptimos en la prevención de virus.
- **OutbreakShield:** Con esta opción se activa el programa OutbreakShield. Con OutbreakShield activado, el software crea sumas de comprobación de los correos y las compara con las listas negras anti-spam de Internet, actualizadas de modo permanente, con lo que tiene los medios para actuar ante un mailing masivo antes de que estén disponibles las correspondientes firmas de virus. OutbreakShield se informa a través de Internet acerca de ciertas concentraciones de correos sospechosos y cierra prácticamente en tiempo real la brecha que existe entre el comienzo de un envío de correos en masa y su combate mediante las firmas especialmente adaptadas del virus. OutbreakShield está integrado en el Bloqueador de virus de correo electrónico.

## Conexiones cifradas (SSL)

Muchos proveedores de correo electrónico (p. ej. GMX, WEB.DE, T-Online y Freenet) han cambiado al cifrado SSL. De este modo, los correos electrónicos y las cuentas de correo se han vuelto claramente más seguros. Aún así, sigue siendo necesario proteger sus correos electrónicos mediante un programa antivirus. Para ello, G DATA le ofrece el módulo para **conexiones cifradas (SSL)**. Tiene asimismo la posibilidad de comprobar si los correos electrónicos con cifrado SSL contienen virus o software dañino.

Para poder comprobar los correos electrónicos con cifrado SSL mediante el software de G DATA, hay que importar el certificado del software de G DATA desde el programa de correo electrónico. Así se garantiza que el software de G DATA va a poder comprobar los correos electrónicos entrantes.

Es compatible con todos los programas de correo que puedan importar certificados o que puedan acceder al almacén de certificados de Windows, como p. ej.:

- Outlook 2003 o posterior

- Thunderbird
- The Bat
- Pegasusmail

Proceda como sigue si el certificado de G DATA no se ha instalado automáticamente:

1. Durante la instalación del certificado sus programas de correo electrónico no deberían estar activos. Por tanto, cierre primero todos los programas de correo electrónico antes de crear e instalar el certificado.
2. En el software de G DATA active la casilla de verificación para la comprobación con conexiones SSL.
3. Haga clic en el botón para exportar el certificado. A continuación, el software de G DATA crea un certificado. Este archivo se llama GDataRootCertificate.crt.
4. Abra ahora el archivo GDataRootCertificate.crt. Aparece una ventana de diálogo en la cual puede instalar el certificado en su ordenador.
5. En la ventana de diálogo haga clic en el botón **Instalar certificado** y siga las instrucciones del asistente de instalación.

Listo. Ahora, Outlook y todos los demás programas de correo electrónico que acceden al almacén de certificados de Windows incluyen el certificado necesario para comprobar también si los correos electrónicos transmitidos con cifrado SSL contienen virus o software dañino.

**Nota:** Si utiliza **Thunderbird (portable)** y el certificado no se importó automáticamente, debe importarlo posteriormente y administrar la configuración de confianza del certificado de G DATA que se ha creado. Para ello, en Thunderbird (portable), en **Opciones > Avanzado > Certificados** seleccione el botón **Ver certificados**. Al hacer clic aquí aparecen varias pestañas. Seleccione la pestaña **Autoridades** y luego el botón **Importar**. Ahora puede seleccionar el certificado **G DATA Mail Scanner Root**.

Si marca en este momento las siguientes casillas de opciones y hace clic en Aceptar, G DATA protegerá su Thunderbird portable:

- **Este certificado puede identificar sitios web.**
- **Este certificado puede identificar a los usuarios de correo.**
- **Este certificado puede identificar desarrolladores de software.**

En otros programas de correo electrónico existen funciones parecidas para importar certificados. En caso de duda, consulte en la ayuda correspondiente el funcionamiento del programa de correo electrónico utilizado.

## Avanzado

Si no utiliza los puertos estándar al trabajar con sus programas de correo electrónico, también puede indicar en el **número de puerto del servidor** el puerto que utilice para los correos entrantes o salientes. Haciendo clic en el botón **Estándar** puede recuperar automáticamente los números de puerto estándar. También puede indicar varios puertos. Tiene entonces que separarlos por comas.

**Atención:** Microsoft Outlook está protegido a través de un plugin especial, con el que puede analizar directamente desde Outlook carpetas y correos. Para comprobar si un correo o una carpeta están infectados, solo tiene que hacer clic en el icono de G DATA, que comprobará si tiene virus la carpeta de correo seleccionada en ese momento.

Como el software escanea los correos entrantes antes que el verdadero programa de email, en caso de tener un gran volumen de correo o una conexión lenta puede ocurrir que el programa de correo muestre un mensaje de error al no recibir inmediatamente los datos de correo, porque el software está verificando si tienen virus. Al activar la casilla **Impedir exceso de tiempo en el servidor de correo electrónico** se evita que el programa de correo muestre ese mensaje de error y, tan pronto como se hayan comprobado todos los datos del correo electrónico, el software los transferirá normalmente al programa de correo.

## Comprobaciones de virus automáticas

En este punto se puede conectar y desconectar el escáner en modo de reposo. Además, en lugar de ello o de manera adicional puede examinar periódicamente su ordenador o áreas de su ordenador en búsqueda de infecciones. Por ejemplo, puede realizar estas comprobaciones en momentos en los cuales no se utilice el ordenador.

**Comprobaciones de virus planificadas:** En muchos casos, es suficiente con realizar una comprobación mediante el escaneo de modo de reposo. Con el botón **Nuevo** puede realizar comprobaciones de virus automáticas que sean diferentes e independientes entre sí. Así, por poner un ejemplo, podría comprobar diariamente la carpeta Descargas mientras que, por otro lado, su colección de MP3 sólo la examinaría una vez por mes.

En los siguientes capítulos se explica como se puede crear comprobaciones de virus individuales.

## General

Establezca aquí el nombre que debe tener la nueva tarea de comprobación automática de virus creada. Para distinguirlos, se aconseja que utilice nombres explicativos como p.ej. *discos duros locales (comprobación semanal)* o *archivos comprimidos (comprobación mensual)*.

Si marca la casilla **Apagar el PC tras finalizar la tarea**, el ordenador se apagará automáticamente después de realizar la comprobación automática de virus. Esta forma de actuación es conveniente si, por ejemplo, desea realizar la comprobación de virus después de acabar la jornada en la oficina.

**Tarea:** Cada orden realizada automáticamente para comprobar el ordenador o determinadas áreas se denomina tarea.

## Volumen de análisis

Aquí puede seleccionar dónde quiere realizar la exploración de virus: en los discos duros locales, los sectores de la memoria e inicio automático o únicamente en directorios y archivos específicos. Si selecciona la última opción, indique con el botón **Selección** los directorios deseados.

**Seleccionar directorios/archivos:** Si hace clic en los símbolos de más del árbol de directorios, podrá seleccionar y abrir directorios y en la vista de archivos se puede visualizar sus contenidos. A continuacin, el software procederá a escanear los directorios y archivos que haya marcado. Si no se comprueban todos los archivos de un directorio, este directorio aparecerá marcado con una marca de verificación gris.

## Planificación horaria

Con esta pestaña puede determinar cuándo y con qué frecuencia se va a realizar el trabajo correspondiente. En **ejecutar** se introduce un valor de referencia que luego se especifica con la opción **fecha**. Si selecciona **al iniciar el sistema**, no hace falta especificar la planificación horaria porque el software ejecutará la comprobación siempre que se reinicie el ordenador.

- **Ejecutar automáticamente el trabajo en el próximo inicio del sistema si el ordenador está apagado en el momento programado de comienzo:** Mediante la activación de esta opción se ejecutarán las comprobaciones de virus automáticas que no se habían efectuado, tan pronto como se reinicie nuevamente el ordenador.
- **No ejecutar en modo batería:** Para no disminuir de manera innecesaria el periodo de vigencia de la batería usted puede, por ejemplo, para portátiles determinar, que las comprobaciones automáticas de virus se realicen sólo cuando el ordenador portátil esté conectado a la red eléctrica.

## Ajustes de escaneo

En esta zona puede seleccionar los parámetros que desee utilizar en la comprobación automática de virus.

- **Utilizar motores:** El software utilizan dos motores, es decir, dos programas perfectamente sintonizados de análisis de virus. En los ordenadores más antiguos y lentos, la utilización de un único motor puede acelerar la comprobación de virus. No obstante y por lo general, conviene mantener el ajuste **Ambos motores**.
- **Archivos infectados:** ¿Su software ha encontrado un virus? En el ajuste estándar, el software le pregunta lo que desea hacer con el virus y el archivo infectado. Si siempre va a realizar la misma acción, puede ajustar la opción elegida aquí. El ajuste que ofrece la máxima seguridad para sus datos es **desinfectar (si no es posible: en cuarentena)**.
- **Archivos comprimidos infectados:** Aquí puede determinar si los ficheros de archivos comprimidos (es decir, los archivos con la extensión RAR, ZIP o también PST) tendrán un tratamiento distinto de los archivos normales. No obstante, observe que al mover un archivo comprimido a cuarentena éste se puede dañar, de modo que incluso al deshacer la acción ya no se pueda utilizar más.

Con el botón **Avanzado** se pueden determinar las comprobaciones adicionales que deba realizar o no el Vigilante de virus.

No obstante, en la mayoría de los casos, la configuración estándar prevista es más que suficiente.

- **Tipos de archivo:** Aquí puede determinar qué tipos de archivo deberá comprobar el software ante posibles virus.
- **Heurístico:** En el análisis heurístico, los virus no sólo se detectan mediante las bases de datos de virus que recibe cada vez que actualiza el software, sino que también se determinan por ciertas características típicas de los virus. Este método es otro plus de seguridad, que sin embargo en algunos casos puede producir una alarma de error.
- **Archivos comprimidos:** La comprobación de los datos comprimidos en los archivos comprimidos (se reconocen por su extensión, por ej., ZIP, RAR o también PST) requiere mucho tiempo y, por lo general, puede omitirse si el Vigilante de virus está siempre activo en

el sistema. Al descomprimir el archivo, el vigilante detecta el virus escondido hasta entonces e impide automáticamente su propagación.

- **Comprobar archivos comprimidos de correo:** Aquí se establece si también sus archivos de correo deben ser comprobados en búsqueda de infecciones.
- **Comprobar áreas del sistema:** Por lo general, no se deben excluir las áreas del sistema de su ordenador (p.ej. sectores de arranque) en el control de virus.
- **Comprobar dialer / spyware / adware / riskware:** Con esta función puede examinar su sistema para detectar dialer y otros programas dañinos (programas espía, adware y programas de riesgo). Se trata, por ejemplo, de programas que establecen conexiones caras con Internet, sin conocimiento del usuario y que, desde el punto de vista del daño económico que pueden causar, se asemejan mucho a los virus. Entre otras cosas, dichos programas guardan secretamente información sobre los sitios web que el usuario visita o incluso todas las entradas que realiza a través del teclado (y por tanto también sus contraseñas) y, en cuanto pueden, las transmiten a terceras personas a través de Internet.
- **Comprobar rootkits:** Los rootkits intentan soslayar los métodos convencionales de detección de virus. Por eso siempre es recomendable una revisión adicional para detectar estos agentes dañinos.
- **Elaborar registro:** Al marcar esta casilla puede establecer que el programa cree un registro acerca del proceso de comprobación de virus. Este registro puede consultarse después en el área **Registros**.

## Cuenta de usuario

Aquí puede indicar la cuenta de usuario del ordenador en la que debe realizarse la comprobación de virus. La cuenta es necesaria para acceder a las unidades de red.

## AntiSpam

### Filtro antispam

El filtro antispam le ofrece amplias posibilidades de configuración para cerrar el paso de forma eficaz a los correos electrónicos con contenidos o procedencia indeseados (por ejemplo, de remitentes de correos en masa). El programa verifica numerosas características de los correos electrónicos que son típicas del spam. Teniendo en cuenta las características encontradas en el mensaje se calcula un valor que refleja la probabilidad de que sea spam. Con el botón **Utilizar filtro antispam** se puede activar y desactivar el filtro antispam.

Para conectar o desconectar las diferentes clases de filtros del filtro antispam solo tiene que colocar o quitar la marca delante de la entrada elegida. Para realizar modificaciones en los distintos filtros, pulse simplemente en la entrada correspondiente. Se abre entonces una ventana de diálogo para modificar los parámetros. Tiene las siguientes posibilidades de ajuste:

- **Spam-OutbreakShield:** Con el OutbreakShield pueden identificarse y combatirse los programas dañinos en los correos masivos antes de que estén disponibles las firmas de virus actualizadas. OutbreakShield se informa a través de Internet acerca de ciertas concentraciones de correos sospechosos y cierra prácticamente en tiempo real la brecha que existe entre el comienzo de un envío masivo de correos y su eliminación mediante las firmas de virus especialmente adaptadas. Si utiliza un ordenador detrás de un servidor proxy, haga clic en **Ajustes de Internet** para realizar los ajustes. Sólo debería cambiar esta configuración cuando no funcione el OutbreakShield.
- **Emplear lista blanca:** Mediante la lista blanca puede excluir de forma explícita de la sospecha de spam determinadas direcciones de remitentes o dominios. Simplemente indique en el campo **Direcciones/dominios** la dirección de correo (p. ej., *newsletter@paginainformativa.es*) o el dominio (p. ej., *paginainformativa.es*) que desea excluir de la sospecha de spam, y el software G DATA considerará que los correos electrónicos de este remitente o dominio del remitente no son spam.

Con el botón **Importación** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista blanca. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **Exportación** también puede exportar la lista blanca como archivo de texto.

- **Emplear lista negra:** Mediante una lista negra se puede presuponer explícitamente que determinadas direcciones de remitentes o dominios posiblemente son spam. Simplemente, introduzca en el campo **Direcciones/Dominios** la dirección de correo (p. ej., *newsletter@megaspam.de.vu*) o dominio (p. ej., *megaspam.de.vu*) que desea considerar bajo sospecha de spam, y el software G DATA tratará, por norma general, los correos electrónicos de este remitente o dominio como correos con probabilidad muy alta de spam. Con el botón **Importación** puede también incluir listas ya confeccionadas de direcciones de correo o de dominios en la lista negra. Las direcciones y dominios deben aparecer en la lista en renglones separados. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Con el botón **exportación** también puede exportar la lista negra como archivo de texto.



- **Emplear listas negras en tiempo real (ajuste estándar):** En Internet se encuentran listas que contienen direcciones IP de servidores de los que se tiene constancia de que se usan para enviar spam. El software G DATA averigua mediante consultas a las Realtime Blacklists (Listas negras en tiempo real) si el servidor remitente está incluido en alguna lista negra. En caso afirmativo, aumenta la probabilidad de spam. Como norma general debería utilizar aquí el ajuste estándar, aunque en las listas negras 1, 2 y 3 pueden indicarse direcciones propias de listas negras de Internet.
- **Emplear palabras clave (texto de correo):** Mediante la lista de palabras clave también puede poner correos bajo sospecha de spam en función de las palabras utilizadas en el texto del correo. Si aparece como mínimo uno de los términos en el texto del correo electrónico, aumenta la probabilidad de spam. Esta lista se puede modificar según las propias necesidades con los botones **Agregar**, **Modificar** y **Borrar**. Mediante el botón **Importación** también puede añadir a su lista otras listas ya confeccionadas de palabras clave. Cada entrada debe aparecer en la lista en un renglón propio. Como formato se empleará un simple archivo txt como los que, por ejemplo, pueden crearse con el bloc de notas de Windows. Mediante el botón **Exportación** también puede exportar la lista de palabras clave como archivo de texto. Marcando la opción **Buscar solo palabras completas** puede determinar que el software G DATA busque solo palabras completas en el texto del asunto de un correo.
- **Emplear palabras clave (asunto):** Mediante la lista de palabras clave también puede poner bajo sospecha de spam los correos en función de las palabras utilizadas en la línea del asunto. Si aparece como mínimo uno de los términos en la línea de asunto, aumenta la probabilidad de spam.
- **Emplear filtro de contenido:** En el caso del filtro de contenido se trata de un filtro autoadaptable que, basándose en las palabras utilizadas en el texto del mensaje, calcula una probabilidad de spam. Para ello, este filtro no se basa únicamente en listas fijas de palabras, sino que aprende con cada correo electrónico que se recibe. Mediante el botón **Consultar contenido de tabla** pueden consultarse las listas de palabras que utiliza el filtro de contenido para la clasificación de un correo como spam. Mediante el botón **Restablecer tablas** se borran todos los contenidos aprendidos de las tablas y el filtro de contenido autoadaptable comienza desde el principio el proceso de aprendizaje.

## Reacción

Aquí puede determinar qué procedimiento debe seguir el filtro antispam con los correos electrónicos que posiblemente incluyen spam. Aquí se pueden distinguir tres niveles, que dependen de lo elevada que el software G DATA estime la probabilidad de que el correo en cuestión sea spam.

- **Sospecha de spam:** Aquí se determina cómo tratar los correos en los que el software G DATA encuentra algunos elementos de spam. En estos casos, no tiene por qué tratarse siempre de spam, sino que en ocasiones puede también tratarse de boletines de noticias o envíos publicitarios que el destinatario sí desea recibir. En estos casos se recomienda avisar al destinatario de la sospecha de spam.
- **Probabilidad de spam alta:** Aquí se reúnen los correos electrónicos que incluyen muchas características de spam y sólo en casos muy raros son deseados por el destinatario.
- **Probabilidad de spam muy alta:** Aquí se encuentran los correos electrónicos que cumplen todos los criterios del correo spam. En este caso, prácticamente nunca se trata de mensajes deseados y rechazar este tipo de correos está recomendado la mayoría de las veces.

Estas tres reacciones de distinto grado puede configurarlas de forma personalizada. Haga clic simplemente en el botón **Modificar** y defina la reacción que deba tener el software G DATA. De este modo, con la opción **Rechazar correo** tiene la posibilidad de que el correo electrónico no llegue siquiera a su buzón de correo. Mediante **Insertar aviso de spam en asunto y texto** puede marcar de forma llamativa los emails identificados como spam para así poder filtrarlos mejor. Si utiliza **Microsoft Outlook** (atención: No confundir con Outlook Express ni con Windows Mail), tiene igualmente la posibilidad de mover los correos electrónicos sospechosos de spam a una carpeta de su elección en su buzón de correo (**Mover correo a carpeta**). Puede crear esta carpeta directamente con el software G DATA definiendo en **Nombre de carpeta** la carpeta correspondiente.

**Nota:** También en el caso de que no utilice Outlook, puede mover los e-mails identificados como spam a una carpeta. Introduzca para ello una advertencia en la línea de asunto (p.ej. "[Spam]") y cree una regla con su programa de correo que mueva los correos electrónicos con ese texto en la línea de asunto a otra carpeta.

## Ajustes profesionales

En esta área se puede modificar en detalle la forma en que el software G DATA detecta el correo basura y adaptarla así a las necesidades específicas de su tráfico de correo. Sin embargo, se recomienda en estos casos utilizar por norma general los ajustes estándar. Realice modificaciones en los ajustes profesionales únicamente si conoce la materia y sabe perfectamente lo que está haciendo.

## Otros filtros

Los siguientes filtros vienen ajustados de serie y también pueden desactivarse, si hace falta, quitando la marca de la casilla.

- **Desactivar scripts en HTML**
- **Filtrar adjuntos peligrosos**

Además, también puede crear nuevas reglas de filtrado con el botón **Nuevo** o editar filtros existentes con el botón **Editar**. Los filtros creados se visualizan en la lista y pueden activarse o desactivarse según las propias necesidades con las casillas de verificación situadas a la izquierda de cada registro. Cuando la casilla de verificación está marcada, el filtro correspondiente está activo. Cuando la casilla de verificación no esté marcada, el filtro no estará activo. Para borrar definitivamente un filtro, márkelo haciendo clic en él con el ratón y pulse luego el botón **Borrar**.

Estas posibilidades de filtrado disponibles constituyen filtros adicionales que complementan el filtro de spam propiamente dicho del software G DATA y facilitan los ajustes individuales. El filtro antispam le ofrece amplias posibilidades de configuración para cerrar el paso de forma eficaz a los correos electrónicos con contenidos o procedencia indeseados (por ejemplo, de remitentes de correos en masa). El programa verifica numerosas características de los correos electrónicos que son típicas del spam. Teniendo en cuenta las características encontradas en el mensaje se calcula un valor que refleja la probabilidad de que sea spam. Para esta acción hay disponibles varias pestañas en las que figuran ordenadas por temas todas las posibilidades de configuración relevantes.

Cuando se crea un nuevo filtro, se abre una ventana de selección en la que puede determinar el tipo de filtro básico. En una ventana de asistente específica del tipo de filtro se pueden especificar todos los demás datos sobre el filtro que se va a crear. De este modo se crean con la mayor comodidad filtros contra cualquier amenaza imaginable.

- **Desactivar scripts en HTML:** Este filtro desactiva los scripts HTML de su correo. Los scripts, que en una página web seguro que tienen su razón de ser, si van acompañando un correo HTML, son más bien molestos. En algunos casos, los scripts en HTML se usan activamente para infectar el ordenador, ya que tienen la posibilidad no solo de difundirse al abrir un fichero adjunto, sino que pueden activarse ya en la vista previa de un mensaje de correo.
- **Filtrar datos adjuntos peligrosos:** A la hora de filtrar archivos hay muchas posibilidades de filtrar los datos adjuntos al correo (= attachments) y los anexos. La mayoría de virus de correo electrónico se propagan a través de estos adjuntos, que, por lo general, incluyen archivos ejecutables más o menos ocultos. Puede tratarse del clásico archivo EXE, que incluye un programa dañino, pero también de scripts VB, que en algunas circunstancias pueden esconder archivos gráficos, de video o música aparentemente seguros. Como norma general, todo usuario debería tener mucho cuidado al ejecutar archivos adjuntos a un correo y, en caso de duda, lo mejor es consultar al remitente de un correo antes de ejecutar un archivo que no se haya solicitado explícitamente.

En las **extensiones de archivos** se puede definir una lista de las distintas terminaciones de los archivos sobre las que aplicar el filtro correspondiente. Aquí puede incluir, por ejemplo, todos los archivos ejecutables en un filtro (p.ej. archivos EXE y COM), pero filtrar también otros formatos (p.ej. MPEG, AVI, MP3, JPEG, JPG, GIF etc.), cuando debido a su tamaño, representen una carga para el servidor de correo. Por supuesto, puede filtrar también cualquier otro tipo de archivos comprimidos (como p. ej. ZIP, RAR o CAB). Separe todas las extensiones de archivo de un grupo de filtro con un punto y coma.

La función **Filtrar adjuntos en los correos incrustados** se ocupa de que también se filtren los tipos de datos seleccionados en **extensiones de archivo** en los correos que sean, a su vez, un anexo dentro de otro e-mail. Esta opción debe activarse como norma general.

Mediante la función **Sólo cambiar el nombre de los datos adjuntos** no se borran automáticamente los anexos que se deben filtrar sino que simplemente se les cambia el nombre. Esto es especialmente útil, por ejemplo, con archivos ejecutables (como p.ej. EXE y COM), pero también con archivos de Microsoft Office, que podrían incluir scripts y macros ejecutables. Al cambiar el nombre de un archivo adjunto éste no podrá abrirse simplemente con un clic de ratón, sino que primero debe ser guardado por el destinatario y llegado el caso renombrado de nuevo, antes de poder volver a utilizarse. Si la marca de verificación de **Sólo cambiar el nombre de los datos adjuntos** no está activa, se borrarán directamente los archivos adjuntos.

En **sufijo** introduzca los caracteres con los que desee ampliar la extensión de archivo. De este modo se evita que se ejecute un archivo con un simple clic (por ejemplo, exe\_danger). Con la opción **Insertar mensaje en el texto del mensaje de correo electrónico** puede informar al destinatario del correo filtrado de que un archivo adjunto se ha borrado o renombrado debido a una regla de filtro.

- **Filtro de contenido:** El filtro de contenido le permite bloquear cómodamente los correos que incluyan determinados temas o textos.

Para ello simplemente introduzca en **Criterio de búsqueda** las palabras clave y las expresiones frente a las que deba reaccionar el software G DATA. Aquí puede combinar texto a su elección con los operadores lógicos "Y" y "O".

En el **área de búsqueda** puede introducir en qué secciones de un correo deben buscarse estas expresiones. Con **Encabezamiento** se identifica el campo del correo que incluye la dirección de correo del remitente y el destinatario, la línea de asunto e información

sobre los programas, protocolos y datos de envío empleados. A diferencia del anterior, en el **asunto** sólo se comprueba el contenido de la línea de asunto excluyendo las demás informaciones del encabezamiento. En la opción **texto del mensaje** puede elegir además limitar el campo de búsqueda estrictamente a correos de texto puros o desea incluir el texto en los correos HTML (texto HTML).

A través de la opción **Correos incrustados** puede determinar si extiende la búsqueda del filtro de contenido a los correos que aparecen adjuntos dentro de otros correos recibidos.

En la opción **Reacción** puede determinar qué procedimiento seguir con los correos que han sido reconocidos como spam por el software G DATA. Con la opción **Rechazar correo**, su programa de correo no acepta recibir el correo correspondiente.

Si activa la marca en **Insertar aviso en el asunto y en el texto del correo (prefijo en la línea de asunto)** puede introducir un texto de advertencia como *spam* o *atención* precediendo el propio texto de la línea del asunto. Alternativamente, puede también introducir un texto antepuesto al propio texto del correo en caso de sospecha de spam (mensaje en texto).

Si utiliza *Microsoft Outlook* (**atención:** No confundir con Outlook Express ni con Outlook Mail), tiene igualmente la posibilidad de mover los correos electrónicos sospechosos de spam a una carpeta de su elección en su buzón de correo (**Mover correo a carpeta**). Puede crear esta carpeta directamente con el software G DATA definiendo en **Nombre de carpeta** la carpeta correspondiente.

- **Filtro de remitentes:** Mediante el Filtro de remitentes pueden bloquear cómodamente mensajes de correo electrónico que provienen de determinados remitentes. Simplemente tiene que introducir en **Remitente/Dominio** las direcciones de correo electrónico o los nombres de los dominios frente a los que el software G DATA tenga que reaccionar. En caso de que haya varias entradas, puede separarlas mediante punto y coma.

En la opción **Reacción** puede determinar qué procedimiento seguir con los correos que han sido reconocidos como spam por el software G DATA.

Con la opción **Rechazar correo**, su programa de correo no acepta recibir el correo correspondiente.

Si activa la marca en **Insertar aviso en el asunto y en el texto del correo (prefijo en la línea de asunto)** puede introducir un texto de advertencia como *spam* o *atención* precediendo el propio texto de la línea del asunto. Alternativamente, puede también introducir un texto antepuesto al propio texto del correo en caso de sospecha de spam (mensaje en texto).

Si utiliza *Microsoft Outlook* (**atención:** No confundir con Outlook Express ni con Windows Mail), tiene igualmente la posibilidad de mover los correos electrónicos sospechosos de spam a una carpeta de su elección en su buzón de correo (**Mover correo a carpeta**). Puede crear esta carpeta directamente con el software G DATA definiendo en **Nombre de carpeta** la carpeta correspondiente.

- **Filtro de idiomas:** Con el filtro de idiomas puede definir automáticamente como spam correos en determinados idiomas. Si, p.ej., no suele tener contacto por correo electrónico con ninguna persona de habla inglesa, puede filtrar muchísimos correos basura definiendo el inglés como idioma spam. Seleccione aquí los idiomas en los que no suele recibir correos para aumentar considerablemente la valoración de spam realizada por el software G DATA para los correos escritos en estos idiomas.

En la opción **Reacción** puede determinar qué procedimiento seguir con los correos que han sido reconocidos como spam por el software G DATA.

Con la opción **Rechazar correo**, su programa de correo no acepta recibir el correo correspondiente.

Si activa la marca en **Insertar aviso en el asunto y en el texto del correo (prefijo en la línea de asunto)** puede introducir un texto de advertencia como *spam* o *atención* precediendo el propio texto de la línea del asunto. Alternativamente, puede también introducir un texto antepuesto al propio texto del correo en caso de sospecha de spam (mensaje en texto).

Si utiliza *Microsoft Outlook* (**atención:** No confundir con Outlook Express ni con Windows Mail), tiene igualmente la posibilidad de mover los correos electrónicos sospechosos de spam a una carpeta de su elección en su buzón de correo (**Mover correo a carpeta**). Puede crear esta carpeta directamente con el software G DATA definiendo en **Nombre de carpeta** la carpeta correspondiente.

## Otros

En esta sección tiene la oportunidad de configurar otros parámetros más.

- **Comprobar los mensajes no leídos de la bandeja de entrada al iniciar el programa:** *Sólo para Microsoft Outlook* Esta opción sirve para controlar los correos con sospecha de spam. En cuanto abra Outlook, el software G DATA controlará de esta manera todos los correos no leídos que haya en la bandeja de entrada y en las subcarpetas que contenga.
- **Otros programas de correo (utilización de POP3):** Por cuestiones técnicas, los correos electrónicos recibidos mediante POP3 no pueden borrarse directamente. Cuando un filtro tenga que rechazar correos, el correo electrónico en cuestión incluirá un texto sustitutivo estándar. El texto sustitutorio para los correos rechazados es el siguiente: **El mensaje ha sido rechazado**. Pero puede configurar un texto propio para estas funciones de notificación. Para el texto libre correspondiente al **asunto** y al **texto del correo** se pueden utilizar los siguientes comodines (definidos por el signo de porcentaje seguido de una letra minúscula):

%s Remite

%u Asunto

En el programa de correo, puede definir una regla que borre automáticamente los correos electrónicos con el texto sustitutivo aquí definido.

## Cortafuegos

### Automaticidad

Si no desea profundizar más en el tema del Cortafuegos, puede dejar la configuración en el modo automático. Además del modo de piloto automático, que para muchos usuarios seguramente es la mejor elección, tiene una completa gama de opciones que permite adaptar el Cortafuegos de G DATA de manera óptima a sus necesidades y requisitos.

En los ajustes del Cortafuegos existen dos áreas básicas que se pueden configurar de manera individual:

#### Piloto automático

Aquí puede definir si el Cortafuegos actúa de forma autónoma y autoadaptable, sin preguntar al usuario al decidir bloquear o permitir las solicitudes de Internet o bien si consulta al usuario en los casos de duda.

- **Modo piloto automático:** Aquí el Cortafuegos trabaja de modo totalmente autónomo y mantiene automáticamente el ordenador doméstico resguardado de los peligros. Este ajuste ofrece prácticamente una protección total y se recomienda en la mayor parte de los casos.
- **Creación manual de reglas:** Si desea configurar su Cortafuegos de modo personalizado, puede adaptar la protección del Cortafuegos totalmente a sus necesidades mediante la creación manual de reglas.
- **Ofrecer el modo de piloto automático cuando se inicia una aplicación en pantalla completa:** En los juegos de ordenador (y otras aplicaciones a pantalla completa) puede resultar molesto que el Cortafuegos interrumpa con excesivas consultas el ritmo del juego o, simplemente, la reproducción. Para disfrutar del juego sin interrupciones y de un modo seguro, se recomienda el ajuste de piloto automático ya que omite las consultas del Cortafuegos. Si no utiliza el piloto automático como configuración estándar, mediante esta función puede asegurarse de que éste siempre se active si utiliza un programa que utilice modo de pantalla completa.

#### Ajustes de seguridad definidos por el usuario

Mientras utiliza su ordenador en su trabajo diario, el Cortafuegos va aprendiendo continuamente qué programas utiliza para el acceso a Internet, cuáles no y qué programas suponen un riesgo para la seguridad. La utilización de niveles de seguridad predefinidos tiene la ventaja de que permite adaptar el Cortafuegos a las necesidades individuales del usuario, pero sin necesidad de invertir tiempo de gestión ni de poseer conocimientos especializados en seguridad de redes. Basta simplemente con colocar el control deslizante en el nivel de seguridad requerido. Están disponibles los siguientes niveles de seguridad:

- **Seguridad máxima:** Las reglas de Cortafuegos se crean siguiendo unas directrices muy estrictas. Para ello deberá estar familiarizado con términos especializados sobre redes (TCP, UDP, puertos, etc.). El Cortafuegos detecta la más mínima incoherencia y le consultará muy a menudo durante la etapa de aprendizaje.
- **Seguridad alta:** Las reglas de Cortafuegos se crean siguiendo unas directrices muy estrictas. Para ello deberá estar familiarizado con términos especializados sobre redes (TCP, UDP, puertos, etc.). El Cortafuegos se consultará a menudo bajo determinadas circunstancias durante la etapa de aprendizaje.
- **Seguridad normal:** Las reglas de Cortafuegos se crean únicamente en el ámbito de la aplicación. Los asistentes no implican al usuario en los detalles específicos de la red. Durante la fase de aprendizaje se consultará lo menos posible.
- **Seguridad baja:** Las reglas de Cortafuegos se crean únicamente en el ámbito de la aplicación. Los asistentes no implican al usuario en los detalles específicos de la red y durante la etapa de aprendizaje se le consulta muy raramente. En este nivel de seguridad también hay una protección máxima frente a las peticiones de conexión que lleguen de fuera.
- **Cortafuegos desactivado:** En caso de necesidad también se puede apagar el Cortafuegos. Su ordenador sigue conectado a Internet y otras redes, pero el Cortafuegos ya no le sirve de escudo ante los ataques o intentos de espionaje.

Si desea configurar el Cortafuegos de un modo más específico, marque la opción **Ajustes de seguridad definidos por el usuario**. Pero tenga en cuenta que, para realizar esta configuración, es necesario poseer por lo menos conocimientos básicos sobre seguridad de redes.

## Consultar

Aquí puede determinar cómo, cuándo y si el Cortafuegos debe consultar al usuario cada vez que los programas quieran establecer una conexión con Internet o la red.

### Crear regla

Cuando el Cortafuegos detecta un establecimiento de conexión con la red, aparece una ventana de información para que indique cómo proceder con la aplicación correspondiente. Aquí puede definir qué es lo que desea determinar exactamente al permitir o prohibir el acceso a una red:

- **Por aplicación:** Aquí se concede o deniega la autorización de acceso a la red para la aplicación mostrada en este momento de forma global para todos los puertos y con cualquier protocolo de transferencia (p.ej., TCP o UDP).
- **Por protocolo/puerto/aplicación:** La aplicación que solicite acceso a la red recibirá la autorización para una conexión online únicamente con el protocolo de transferencia solicitado y exclusivamente con el puerto solicitado. Si esta misma aplicación solicita un nuevo acceso a la red por otro puerto o con otro protocolo, aparecerá la consulta y podrá crearse una regla distinta para este caso.
- **Por aplicación, si hay al menos x consultas:** Hay aplicaciones (p.ej., Microsoft Outlook) que en una consulta de red se dirigen directamente a varios puertos o bien emplean simultáneamente distintos protocolos. Como este sistema conllevaría varias consultas en la modalidad Por protocolo/puerto/aplicación, en este caso se puede definir que las aplicaciones reciban una autorización o prohibición general con respecto al empleo de la red en cuanto el usuario les permita o les deniegue la conexión.

### Aplicaciones de servidor desconocidas

Las aplicaciones que todavía no se gestionen mediante una regla definida en el Cortafuegos pueden someterse a distintos tratamientos. En el momento de la consulta hay un cierto margen de decisión sobre la acción a realizar. Cuando la aplicación de servidor pasa al estado de recepción significa que, como si dijéramos, está en modo standby esperando una petición de conexión. En caso contrario, la consulta se produce únicamente cuando se crea la petición de conexión real.

### Comprobación de redes inalámbricas sin protección

Naturalmente, un Cortafuegos sólo puede funcionar como es debido si reconoce y supervisa todas las redes a las que acceda el ordenador bajo protección. Por esta razón, debería dejar activada necesariamente esta comprobación de redes inalámbricas sin protección.

### Preguntas de aplicación repetidas

Las consultas de conexión repetitivas de una aplicación pueden agruparse. De este modo, en los intentos de conexión para los que todavía no se haya especificado una regla, no aparecerá continuamente una consulta, sino sólo, p.ej., cada 20 segundos u otro intervalo definible por el usuario.

## Comprobación de referencias

En la comprobación de referencias, a las aplicaciones, a las que el Cortafuegos ya haya permitido acceder a la red, se les asigna una suma de comprobación basada en el tamaño del archivo y en otros criterios. Si esta suma de comprobación del programa cambia de repente, puede deberse a que este programa haya sido modificado por un programa dañino. En este caso, el Cortafuegos alerta al usuario.

**Comprobación de referencias para módulos cargados:** Aquí no solo se vigilan las aplicaciones, sino también los módulos (por ej. DLL) que usan las aplicaciones. Como estos cambian con frecuencia o se cargan otros módulos nuevos, una comprobación consecuente de las referencias modificadas y desconocidas en los módulos puede conllevar un trabajo considerable de administración. Porque, según este sistema, cada módulo modificado daría lugar a una consulta de seguridad del Cortafuegos. Por ello, la comprobación de módulos sólo debe utilizarse de esta manera cuando haya que aplicar unos estándares de seguridad muy elevados.

## Otros

Aquí tiene a su disposición más posibilidades de ajuste.

### Especificación para el asistente de reglas

Aquí puede definir en general si desea crear reglas nuevas mediante el Asistente para reglas o en Modo de edición avanzado. Para los usuarios que no estén muy duchos en materia de seguridad de redes se recomienda el asistente para reglas.

### Comprobaciones al inicio del programa

Aquí puede establecer si el Cortafuegos busca con cada inicio de programa las aplicaciones desconocidas de servidor. Estas funciones de búsqueda deben estar siempre activadas, salvo en el caso de que trabaje en una red cerrada.

### Guardar el registro de conexión



Aquí puede determinar el tiempo que el Cortafuegos debe guardar los datos de conexión. Puede conservar los datos desde una hora a 60 horas y se pueden visualizar en el área de registros.

## Optimizador de sistema

### General

Aquí puede realizar los ajustes siguientes:

- **Borrar datos de restauración:** Aquí puede determinar cuándo se deben borrar los datos de restauración (que crea el software G DATA en caso de modificaciones).
- **Borrar datos antiguos:** Aquí puede determinar cuándo se deberán borrar los datos obsoletos (por ej carpetas TEMP de hace tiempo).
- **Borrar vínculos de escritorio:** Aquí puede determinar cuándo se deben borrar los vínculos de escritorio no utilizados (si no han sido utilizados desde hace una determinada cantidad de días).
- **En Microsoft Update buscar también actualizaciones de Office:** Aquí puede configurar si el módulo Optimizador de sistema debe buscar o no en Internet, además de las actualizaciones de Windows actuales, también las actualizaciones de Office. Una actualización de ambos elementos ahorra tiempo y lo mantiene actualizado en cuestiones técnicas de seguridad. Por supuesto, la búsqueda de actualizaciones de Office funcionará sólo si Microsoft Office está instalado en el ordenador respectivo.
- **No crear archivos de registro con información detallada sobre los elementos borrados:** El módulo de Optimizador del sistema está concebido de modo que crea un registro con información completa sobre las modificaciones realizadas. Si considera que un archivo de registro que contiene la información sobre los elementos eliminados por el módulo de Optimizador del sistema representa un riesgo para la seguridad, puede cancelar la creación de este tipo de registros de elementos borrados.
- **Borrar definitivamente los archivos temporales:** Con esta función puede excluir los archivos web (por ej. las cookies o los datos temporales de Internet) de las opciones de restauración del módulo de optimización del sistema, lo que significa que no podrá volver a restaurar estos archivos. Activando esta función, reducirá considerablemente la cantidad de archivos que el módulo de Optimizador del sistema tiene que administrar en el área Restaurar. lo que aporta ventajas de rendimiento.
- **No permitir el reinicio automático del PC por el servicio:** Con esta opción impide un posible reinicio del ordenador, que, de lo contrario, ejecutaría el módulo de Optimizador del sistema en caso necesario durante una tarea de puesta a punto a intervalos programados. El módulo Optimizador del sistema sólo ejecuta el reinicio del ordenador sin preguntar cuando no haya ningún usuario identificado, por eso, en la mayoría de los casos se recomienda no activar esta opción.
- **Permitir la creación de puntos de restauración individuales:** Sin esta función, el software G DATA no puede realizar ninguna restauración más.
- **No tener en cuenta el tipo de unidad al efectuar la desfragmentación:** Como la mayoría de fabricantes desaconsejan la desfragmentación de sus SSD, la desfragmentación de este tipo de disco duro se ha exceptuado de manera predeterminada en el G DATA Optimizador del sistema. Cuando no sea posible asignar automáticamente un tipo a las unidades del software G DATA, pero usted esté seguro de que no hay ninguna unidad SSD en su ordenador, puede dejar marcada aquí esta opción. Posteriormente, cada vez que ejecute el tuner éste iniciará la desfragmentación de todos los discos duros que se encuentren en el sistema.

## Configuración

En este área puede seleccionar todos los módulos que debe utilizar el Optimizador del sistema para realizar un proceso de puesta a punto. Los módulos seleccionados se iniciarán bien a través de una acción automática programada (véase el capítulo [Planificación horaria](#)) o manual. Para activar un módulo, haga sólo un doble clic encima con el ratón. Las siguientes áreas de Tuning se pueden optimizar aquí de manera individual:

- **Seguridad:** Muchas funciones que descargan posterior y automáticamente datos de Internet, le benefician únicamente al proveedor y no a usted. Con frecuencia, estas funciones son la puerta de entrada de software malicioso. Con estos módulos Ud. protege su sistema y lo mantiene en el nivel más actualizado:
- **Rendimiento:** Los archivos temporales, como por ej. copias de seguridad que ya no se necesitan, archivos de registro o datos de instalación que, una vez realizada la instalación, sólo ocupan espacio en el disco duro, lo ralentizan y consumen valiosa memoria. Además, los procesos y vínculos de archivos superfluos ralentizan el sistema notablemente. Con los módulos que citamos a continuación puede librar a su ordenador de este lastre innecesario, acelerando así la velocidad de operación.
- **Protección de datos:** Aquí se agrupan los módulos que se ocupan de la protección de los datos. Aquí se borran los rastros que se dejan involuntariamente al navegar o al utilizar el ordenador y que desvelan mucha información sobre los hábitos del usuario incluso datos importantes y contraseñas.

## Protección de carpetas

En esta ficha se pueden excluir determinadas carpetas (por ej. también la partición de Windows) del borrado automático de archivos antiguos.



Para ello, haga clic simplemente en el símbolo **Agregar** y seleccione la carpeta correspondiente o la unidad de disco que desee.



Para volver a liberar un directorio de excepciones, selecciónelo de la lista mostrada y haga clic en el botón **Borrar**.

## Protección de archivos

Con la protección de archivos puede proteger determinados archivos para que no se borren con el módulo de optimización del sistema, como por ejemplo los estados de los juegos de ordenador o archivos similares con extensiones inusuales que podrían interpretarse como archivos de copia de seguridad o temporales.



Para proteger archivos concretos, haga clic en el botón **añadir** e introduzca el nombre del archivo en cuestión. Aquí también puede utilizar comodines.

El funcionamiento de los comodines es el siguiente:

- El signo de interrogación (?) representa caracteres sueltos.
- El signo de asterisco (\*) representa una secuencia completa de caracteres.

Para proteger, por ejemplo, todos los archivos con la extensión .sav, deberá introducir \*.sav. Para proteger, por ejemplo, archivos de formatos distintos en los que el principio nombre del archivo sea igual, deberá introducir text\*.\*.

A continuación, seleccione la carpeta en la que deban protegerse los archivos haciendo clic en el botón Avanzado. Una vez aquí seleccione la ubicación en la que se encuentran los archivos a proteger. El módulo de optimización del sistema protegerá así sólo los archivos definidos en esta carpeta (por ejemplo: los estados del juego sólo de la carpeta Juegos).



Para volver a liberar una protección de archivos, selecciónela en la lista mostrada y haga clic en el botón **Borrar**.

## Planificación horaria

Mediante la ficha **Planificación horaria** puede determinar cuándo y con qué frecuencia debe tener lugar la operación automática de tuning.

En la opción **A diario** puede especificar bajo días de la semana que su ordenador, p. ej., ejecute la puesta a punto sólo en los días hábiles o sólo cada dos días o durante el fin de semana, cuando no se utiliza para trabajar. Para modificar las fechas y las horas en la opción **Fecha**, simplemente marque el elemento que quiera modificar (p. ej., día, hora, mes, año) con el ratón y utilice luego las flechas del teclado o los pequeños símbolos de flecha a la derecha del campo de entrada para moverse cronológicamente por el correspondiente elemento.

Si no desea permitir que se realice una optimización automática del sistema, desmarque simplemente la marca de la opción **Activado** para la optimización automática.

## Control de dispositivos

Con el control de dispositivos podrá definir para su ordenador los soportes de memoria que se permiten para leer o grabar datos. Así puede impedir, por ejemplo, que se copien datos privados en una memoria USB o en un CD. Además, podrá definir exactamente en cuales soportes de datos intercambiables, como memorias o discos duros USB, se pueden descargar datos. Así por ej. puede usar su propio disco duro USB para salvaguardar datos, pero dejar sin acceso a otros discos duros.

Para utilizar el control de dispositivos, coloque la marca de verificación en **Activar control de dispositivos** y seleccione luego para que dispositivos desea establecer limitaciones:

- **Soporte de datos intercambiable (por ej. memorias USB)**
- **Unidades de CD/DVD**
- **Unidades de disco**

Ahora tiene la posibilidad de definir reglas para los distintos soportes de memoria.

### Reglas generales

Aquí puede establecer si el dispositivo correspondiente no se puede usar en absoluto (**Bloquear acceso**), si solo se permite descargar datos de él (**Acceso de lectura**) o si no se aplica ninguna limitación para ese dispositivo (**Acceso completo**). Estas reglas serán luego aplicables a todos los usuarios del ordenador.

### Reglas específicas del usuario

Si desea que solo determinados usuarios obtengan derechos limitados para soportes de memoria, en este área puede primero seleccionar el nombre del usuario registrado en su ordenador y luego restringir el acceso al soporte de memoria correspondiente, como se describe en **Reglas generales**. De este modo, usted como administrador, por ej., puede tener un acceso completo al ordenador, mientras que los otros usuarios tienen solo derechos limitados.

Seleccione el usuario. Al pulsar Aceptar se abre otro diálogo en que puede definir el tipo de acceso que desea que tenga ese usuario y si el permiso para ese usuario tiene un periodo limitado de duración (como por ej. dos semanas) (**Validez**).

**Nota:** La regla específica del usuario anula la regla general. Es decir, si prohíbe en general el acceso a las memorias USB, puede de todos modos autorizar el uso a un usuario concreto mediante reglas específicas para ese usuario. Si un usuario ha obtenido a través del control de dispositivos determinadas limitaciones de acceso limitadas en el tiempo, al expirar el periodo de validez de la limitación, se vuelven a aplicar las reglas generales al usuario.

### Reglas específicas del dispositivo

Cuando utilice soportes de datos intercambiables, como por ej. memorias USB o discos duros externos, puede establecer también que solo puedan acceder a su ordenador determinados soportes de datos intercambiables. Solo tiene que unir el soporte de datos intercambiable con su ordenador y luego pulsar el botón **Agregar**. En el cuadro de diálogo que aparece se puede elegir el soporte de datos intercambiable deseado. Al pulsar Aceptar se abre otro diálogo en que puede definir el tipo de acceso que desea que tenga ese soporte de datos, si el empleo de ese soporte de datos tiene un periodo limitado de duración (como por ej. dos semanas) (**Validez**) y si todos los usuarios pueden usar o no ese soporte de datos con su acceso de usuario.



# Copia de seguridad

En este área se pueden realizar los ajustes generales sobre la funcionalidad del módulo de Copia de seguridad.

- **Directorio para archivos temporales:** Defina donde se guardan los datos temporales del módulo de copia de seguridad. Estos datos se originan al crear y también al restaurar una copia de seguridad y se borran de nuevo automáticamente después del proceso correspondiente. No obstante, conviene tener suficiente espacio disponible en el disco duro, porque si no se restringe la velocidad de la copia de seguridad y la restauración. Este ajuste solo debe modificarse cuando no haya suficiente espacio disponible en el directorio seleccionado para archivos temporales.
- **Comprobación de unidad de disco de origen y destino en el mismo disco duro:** Normalmente el módulo de Copia de seguridad avisa cada vez que el usuario pretende realizar una copia de seguridad en el mismo soporte de datos en el que se encuentran los archivos de origen. Esta advertencia se debe a que en caso de pérdida o fallo de ese soporte de datos, también desaparecería consecuentemente la copia de seguridad. Pero si, por la razón que sea, desea realizar periódicamente copias de seguridad en el soporte de datos original, puede desactivar aquí esta advertencia.

# Registros

En los distintos módulos hay disponibles funciones de registro con las que podrá conocer siempre las acciones que el software G DATA lleva a cabo para protegerle.

## Registros de protección antivirus

En el área de registros aparece una lista de registros creados por el software. Haciendo clic en las columnas con el nombre **Hora de inicio**, **Tipo**, **Título** o **Estado**, puede ordenar los registros disponibles según estos criterios. Con los botones **Guardar** como e **Imprimir** se pueden guardar también los datos de registro en un archivo de texto o imprimirse directamente. Para borrar un registro, seleccione la entrada de la tabla con el ratón y pulse la tecla Del o pulse el botón **Borrar**.

## Registros de Cortafuegos

En la zona de registros aparece un pormenorizado archivo de registro para cada acción del Cortafuegos. Aquí se pueden abrir actividades concretas haciendo clic sobre ellas y, si se desea, imprimir las o guardarlas como archivo de texto. Lea también el capítulo [Ajustes: Otros](#).

## Registros de Copia de seguridad

En la zona de registros aparece un pormenorizado archivo de registro para cada acción y cada tarea de copia de seguridad. Aquí se pueden abrir actividades concretas haciendo clic sobre ellas y, si se desea, imprimir las o guardarlas como archivo de texto. Lea también el capítulo [Guardar y restaurar](#).

## Registros de protección antispam

En la zona de registros aparece un archivo de registro pormenorizado para cada acción. Aquí se pueden abrir actividades concretas haciendo clic sobre ellas y, si se desea, imprimir las o guardarlas como archivo de texto.

## Registros de protección infantil

En el área de registro el administrador puede ver un resumen de todos los intentos de los demás usuarios de acceder a contenidos bloqueados. Arriba puede seleccionar de la lista el usuario cuyo registro quiera ver. Para más información consulte el capítulo [Ajustes: Registro](#).

**Nota:** Estos registros puede también borrarlos pulsando el botón **Eliminar registros**.

## Registros del control de dispositivos

En la zona de registros aparece un archivo de registro pormenorizado para cada acción del administrador de dispositivos. Para más información, consulte también el siguiente capítulo: [Ajustes: Control de dispositivos](#).

# FAQ: BootScan

Si su ordenador es totalmente nuevo o ha estado hasta ahora protegido por un software antivirus, puede efectuar la instalación siguiendo los pasos descritos a continuación.

Pero si tiene motivos razonables para sospechar que su ordenador pudiera estar infectado, le recomendamos que antes de instalar el software lleve a cabo un análisis BootScan.

**BootScan:** Al encender el ordenador, normalmente se inicia automáticamente el sistema operativo de Windows. Esta operación recibe el nombre de inicializar. Pero también es posible arrancar otros sistemas operativos y programas automáticamente.

Con el fin de comprobar la presencia de virus en su ordenador antes de que arranque Windows, G DATA dispone de una versión especial autoarrancable además de la versión para Windows.

## Requisitos

El BootScan le ayuda a combatir los virus que se hayan arraigado subrepticamente en su ordenador antes de la instalación del programa antivirus.

Para este cometido existe una versión especial del software que se puede ejecutar antes de iniciar Windows.

**Arrancar desde un CD/DVD-ROM:** Si su ordenador no se inicializa automáticamente desde el CD/DVD-ROM, efectúe los siguientes pasos:

- 1** Apague el ordenador.
- 2** Encienda de nuevo el ordenador. Normalmente, puede entrar en la configuración de la BIOS pulsando durante el arranque (=inicio) del ordenador la tecla Supr (dependiendo del sistema también las teclas F2 o F10).
- 3** La forma exacta de modificar los ajustes de la configuración de su BIOS varía de un ordenador a otro.

Consulte por favor la documentación de su ordenador.

Así, la secuencia de arranque debería ser **CD/DVD-ROM, C**, es decir, la unidad CD/DVD-ROM se convierte en el **1º dispositivo de arranque** y la partición del disco duro con el sistema operativo Windows se convierte en el **2º dispositivo de arranque**.

- 4** Guarde los cambios y vuelva a arrancar el ordenador. Ahora su ordenador está listo para un examen BootScan.

**¿Como se cancela un proceso de BootScan?** Si después del reinicio no apareciese el entorno Windows habitual, sino una interfaz especial del software G DATA BootScan, no hay que preocuparse.

Si no tiene previsto realizar ningún BootScan, solo tiene que seleccionar con las teclas de flecha la entrada **Microsoft Windows** y luego pulsar la tecla **Intro**. Ahora Windows se abrirá como siempre, sin BootScan previo.

**Arrancar desde una memoria USB:** Si utiliza una memoria USB como soporte de arranque, puede también seleccionarla como 1er dispositivo de arranque.

# FAQ: Funciones del programa

## Icono de seguridad

El software G DATA protege permanentemente su ordenador frente a los virus y los programas dañinos. En el margen inferior, en la barra de tareas junto al reloj se muestra un icono señalizando que la protección está activa.



Este icono de G DATA le indica que todo está en orden y que la protección está activa en su ordenador.



Si se ha desconectado el Vigilante o ha surgido algún otro problema, el icono de G DATA muestra una indicación de advertencia. En ese caso deberá abrir lo antes posible el software G DATA y revisar los ajustes.



Si el software G DATA realiza una descarga de datos de Internet, se le indicará mediante un icono especial.

Cuando se selecciona el símbolo con el botón derecho del ratón, aparece un menú de contexto con el que puede controlar las funciones básicas del software.

Aquí tiene a su disposición las siguientes funciones:

- **Iniciar G DATA Software:** De este modo se accede al Centro de seguridad y se pueden realizar, por ejemplo, los ajustes del Vigilante de virus. Lo que se puede hacer en el Centro de seguridad lo puede leer en el capítulo: [Centro de seguridad](#)
- **Desactivar el Vigilante:** En caso necesario, aquí puede desactivar y volver a activar el Vigilante de virus. Esto puede por ejemplo ser conveniente cuando copie en su disco duro grandes cantidades de datos de un lugar a otro o vaya a ejecutar procesos de cálculo que requieran mucho espacio de almacenamiento (p.ej., copiar DVDs o similar). Sólo debería desactivar el Vigilante de virus el tiempo imprescindible, y asegurarse de que, si es posible, el sistema no esté conectado durante este periodo con Internet y que no pueda acceder a nuevos archivos no comprobados (p.ej., mediante CDs, DVDs, tarjetas de memoria o lápices USB).
- **Desactivar Cortafuegos:** Si usa una versión del software G DATA con Cortafuegos integrado, puede también desactivar si desea el Cortafuegos mediante el menú contextual. Su ordenador sigue conectado a Internet y otras redes, pero el Cortafuegos ya no le sirve de escudo ante los ataques o intentos de espionaje.
- **Desactivar piloto automático:** El piloto automático forma parte del Cortafuegos y decide de forma autónoma los contactos y consultas que su ordenador puede aceptar o no a través de la red o Internet. Para los usos habituales, el piloto automático es ideal y debería tenerlo siempre activo. Del mismo modo que el Cortafuegos, el piloto automático también está disponible en versiones seleccionadas del software G DATA.
- **Actualizar firmas de virus:** Un software antivirus debe siempre estar totalmente actualizado. El software se puede, por supuesto, programar para que realice las actualizaciones automáticamente. Pero si en algún momento necesitase urgentemente una actualización, puede iniciarla con el botón Actualizar firmas de virus. Para qué se necesita una actualización de virus se explica en el capítulo: [Comprobación de virus](#)
- **Estadística:** Aquí puede ver una estadística de las comprobaciones del Vigilante de virus, pero también información acerca de los escaneos de modo de reposo, mensajes del filtro web y otros parámetros.

## Realizar comprobación de virus

Con la comprobación de virus examina su ordenador para detectar una posible infección con programas maliciosos. Cuando se inicia la comprobación de virus, comprueba cada archivo en su ordenador para detectar si puede infectar otros archivos o si él mismo ya está infectado.

Si en el curso de una comprobación de virus se encuentran virus u otro tipo de malware, hay distintas formas de eliminar el virus o hacerlo inocuo.

- 1 Inicie la comprobación de virus. La forma de hacerlo se explica en el capítulo: [Protección antivirus](#)
- 2 A continuación el programa examina su ordenador para detectar una posible infección de virus. Se abre además una ventana informando del estado de la comprobación.

Una barra de progreso en la parte superior de la ventana le indica cuánto ha avanzado ya la verificación del sistema. Ya durante la comprobación de virus hay distintas posibilidades de influir en el desarrollo de esta operación:

- **En caso de sobrecarga del sistema, interrumpir la prueba del antivirus:** Con este campo de selección puede establecer que el programa no siga con la comprobación de virus hasta que Ud. haya acabado sus otras actividades en el ordenador.
- **Apagar PC tras el comprobación de virus:** Cuando se quiere ejecutar la comprobación de virus durante la noche o al término de la jornada de trabajo, esta función resulta muy práctica. Tan pronto como ha finalizado la comprobación de virus por parte del software G DATA, se apaga su ordenador.
- **Archivos comprimidos protegidos mediante contraseña:** Si un archivo comprimido está protegido mediante contraseña, el software G DATA no podrá comprobar si hay virus en el archivo comprimido. Si marca esta opción, el software antivirus le informará de los archivos comprimidos protegidos mediante contraseña que no haya podido comprobar. Mientras no se descompriman estos archivos comprimidos, los posibles virus que contengan no representarán una amenaza para su sistema.
- **Acceso denegado:** En general, en Windows hay archivos que son utilizados por aplicaciones en régimen exclusivo y que por eso el antivirus no las puede escanear cuando las aplicaciones están abiertas. Por lo tanto, no debería tener abierto ningún otro programa durante una comprobación de virus. Si marca esta casilla, se mostrarán los datos que no hayan sido comprobados.

**3a** Si su sistema no tiene virus, cuando concluya la comprobación puede cerrar la ventana del asistente pulsando el botón **cerrar**. Ahora su sistema ha sido examinado y no tiene virus.

**3b** En el caso de que se hayan encontrado virus y otros programas dañinos, podrá decidir la forma de actuar ante estos hallazgos. Por lo general es suficiente con hacer clic en el botón **ejecutar acciones**.

El software G DATA aplica ahora un ajuste estándar (si no ha realizado una configuración diferente en [Ajustes: Comprobación de virus manual](#) para los ficheros y archivos comprimidos infectados) y desinfecta el archivo o fichero afectado, es decir, lo repara para que pueda volver a usarse sin limitaciones y ya no suponga ningún peligro para su ordenador.

Si no es posible desinfectarlos, los archivos se ponen en cuarentena, es decir, se encriptan en una carpeta especialmente blindada en la que ya no pueden causar daño alguno.

Si necesita estos archivos infectados, puede, si el caso así lo requiere, sacarlos del área de cuarentena y utilizarlos.

Ahora su sistema ha sido examinado y no tiene virus.

**3c** Cuando ya conozca los objetos/ archivos infectados y sepa cuales de ellos quizá ya no va a necesitar más, tiene también la posibilidad de reaccionar de forma individualizada a cada virus encontrado.

En la lista de los virus encontrados puede definir en la columna acción la forma de proceder con cada archivo infectado en particular.

- **Sólo registrar:** La infección se registra en la vista de [Registros](#). No obstante, no se reparan ni se borran los archivos correspondientes. **Atención:** Cuando un virus solo se registra sigue estando activo y representa un peligro para el sistema.
- **Desinfectar (si no es posible: sólo registrar):** Aquí se intenta borrar el virus del archivo infectado. Si no es posible hacerlo sin dañar el archivo, el virus simplemente se registra; el usuario puede ocuparse posteriormente de este virus. **Atención:** Cuando un virus solo se registra sigue estando activo y representa un peligro para el sistema.
- **Desinfectar (si no es posible: en cuarentena):** Este es el ajuste estándar. Aquí se intenta borrar el virus del archivo infectado. Si no es posible hacerlo sin dañar el archivo, el archivo completo se mueve a un lugar de [Cuarentena](#). Para más información consulte el capítulo: [Archivos en cuarentena](#)
- **Desinfectar (si no es posible: eliminar archivo):** En este caso se intenta eliminar el virus del archivo afectado y, si no es posible, se borra el archivo. Esta función solo debería utilizarla si en su ordenador no tiene ningún dato importante. Borrar los archivos infectados de modo consecuente puede causar, en el peor de los casos, que Windows ya no le funcione y tenga que instalarlo de nuevo.
- **Poner el archivo en cuarentena:** Los archivos infectados se trasladan directamente a la Cuarentena. En este lugar los archivos se guardan codificados. Es decir, el virus no puede aquí hacer ningún daño y los archivos infectados se conservan para poder repararlos en un futuro. Para más información consulte el capítulo: [Archivos en cuarentena](#)
- **Eliminar archivo:** Esta función solo debería utilizarla si en su ordenador no tiene ningún dato importante. Borrar los archivos infectados de modo consecuente puede causar, en el peor de los casos, que Windows ya no le funcione y tenga que instalarlo de nuevo.

Si ahora pulsa el botón **Ejecutar acciones**, el software G DATA procederá con cada virus del modo que haya definido.

Ahora su sistema ha sido examinado para detectar virus. Pero si ha utilizado el ajuste con la opción **Registrar**, puede ser que su ordenador no esté exento de virus.

## Alerta de virus

Cuando el software G DATA encuentra en su ordenador un virus u otro programa malicioso, aparece una ventana informativa en el borde de la pantalla.

En ese caso tiene las siguientes posibilidades de tratar el archivo infectado.

- **Sólo registrar:** La infección simplemente se registra en una lista en el área Registros, pero no se repara ni se borra el archivo correspondiente. Posteriormente, desde el registro se pueden comprobar uno a uno los virus encontrados y eliminarlos selectivamente. Atención: Cuando un virus solo se registra sigue estando activo y representa un peligro para el sistema.
- **Desinfectar (si no es posible: poner en cuarentena):** Aquí se intenta borrar el virus del archivo infectado. Si no es posible hacerlo sin dañar el archivo, el archivo completo se mueve a un lugar de Cuarentena. Para más información consulte el capítulo: [¿Cómo funciona la cuarentena?](#)
- **Poner el archivo en cuarentena:** Los archivos infectados se trasladan directamente a la Cuarentena. En este lugar los archivos se guardan codificados. Es decir, el virus no puede aquí hacer ningún daño y los archivos infectados se conservan para poder repararlos en un futuro. Para más información consulte el capítulo: [Archivos en cuarentena](#)
- **Eliminar archivo infectado:** Esta función solo debería utilizarla si en su ordenador no tiene ningún dato importante. Borrar los archivos infectados de modo consecuente puede causar, en el peor de los casos, que Windows ya no le funcione y tenga que instalarlo de nuevo.

**Cuarentena y bandejas de correo:** Hay archivos que no es conveniente moverlos a la cuarentena, por ejemplo los ficheros de archivos comprimidos de las bandejas de correos. Si traslada una bandeja de correo a la zona de cuarentena, su programa de correo ya no podrá acceder a la bandeja y puede que por eso ya no funcione luego. Especialmente en los **archivos con la extensión PST** conviene que tenga cuidado, porque, por lo general, contienen datos de su bandeja de correo de Outlook.

## Alerta de Cortafuegos

Por norma general, en el modo de creación manual de reglas, el Cortafuegos consulta si el acceso debe ser permitido o rechazado cuando algún programa o proceso desconocido intenta establecer una conexión con la red. Para ello se abre una ventana de información en la que se aportan detalles sobre la aplicación correspondiente. Aquí tiene también la posibilidad de permitir o rechazar el acceso de la aplicación a la red una vez o de forma duradera. En cuanto permita o rechace el acceso a un programa de forma duradera, esta decisión se incorporará como regla al conjunto de reglas de la red correspondiente, y a partir de entonces no volverá a consultarse.

Están disponibles los siguientes botones:

- **Autorizar siempre:** Con este botón se crea una regla para la aplicación arriba indicada (p.ej. Opera.exe, Explorer.exe o iTunes.exe), que permite a la aplicación tener en la red mencionada un acceso permanente a la red o a Internet. Esta regla puede encontrarla bajo la denominación "Regla creada previa petición" en el área Conjuntos de reglas.
- **Autorizar temporalmente:** Con este botón se permite a la aplicación correspondiente un único acceso a la red. En el próximo intento de acceso a la red de ese programa, el Cortafuegos volverá a consultarle.
- **Denegar siempre:** Con este botón se crea una regla para la aplicación arriba indicada (p.ej. dialer.exe, spam.exe o troyano.exe), que en la red mencionada deniega de forma permanente a la aplicación un acceso a la red o a Internet. Esta regla puede encontrarla bajo la denominación "Regla creada previa petición" en el área Conjuntos de reglas.
- **Denegar temporalmente:** Con este botón se impide a la aplicación correspondiente el acceso a la red en una sola ocasión. En el próximo intento de acceso a la red de ese programa, el Cortafuegos volverá a consultarle.

Además encontrará información sobre cómo van a interactuar el protocolo, el puerto y la dirección IP con la aplicación correspondiente.

## Mensaje "no es un virus"

Los archivos clasificados como "no es un virus" pueden llegar a ser aplicaciones peligrosas. Estos programas no tienen directamente funciones dañinas, pero, bajo determinadas circunstancias, pueden ser utilizados en su contra por algún atacante. En esta categoría se encuentran, por ejemplo, determinados programas de servicio para la administración remota, programas para el cambio automático de la disposición del teclado, clientes IRC, servidores FTP o distintos programas de servicio para editar u ocultar procesos.

## Desinstalación

Si alguna vez quiere eliminar el software de G DATA de su ordenador, realice la desinstalación a través del Panel de control de su sistema operativo. La desinstalación se realiza de modo totalmente automático.

Si durante la desinstalación tiene aún archivos en la zona de cuarentena del software G DATA, recibirá un mensaje consultándole si desea borrar o no estos archivos. Si no los borra, los archivos se conservarán codificados en una carpeta especial de G DATA en su ordenador, de forma que no podrán causar ningún daño. No podrá volver a utilizar estos archivos hasta que no vuelva a instalar el software G DATA en su equipo.

Durante la desinstalación se le preguntará si desea borrar los ajustes y los registros. Si no borra los archivos, los registros y ajustes estarán disponibles una vez que se haya vuelto a instalar el software.

Finalice la desinstalación haciendo clic en el botón **Salir**. La desinstalación del software se llevó a cabo completamente.

# FAQ: Consultas sobre la licencia

## Licencias múltiples

Con una licencia múltiple puede utilizar el software G DATA en el número de ordenadores previsto en la licencia. Después de la instalación del primer ordenador y de la actualización online recibirá vía Internet los datos de acceso. Cuando instale el software en el siguiente ordenador, introduzca simplemente el nombre de usuario y la contraseña que haya recibido al registrarse en el Servidor de actualizaciones G DATA. Repita este procedimiento en todos los demás ordenadores.

Utilice para la actualización online en todos sus PCs los datos de acceso (el nombre de usuario y la contraseña) que se le hayan asignado al registrarse por primera vez. Para ello realice los siguientes pasos:

- 1** Inicie el software G DATA.
- 2** En el **Centro de seguridad**, haga clic en el botón **Actualizar firmas de virus**.
- 3** En la ventana que se abre a continuación, introduzca los datos de acceso que recibió por correo electrónico. Si ahora pulsa **aceptar**, su ordenador obtendrá su licencia.

## Extensión de la licencia

Unos días antes de que transcurra su periodo de licencia, aparece una ventana de información en la barra de tareas. Si pulsa sobre ella con el ratón, se abre una ventana de diálogo en la que puede prolongar directamente su licencia en unos pocos pasos y con toda facilidad. Simplemente haga clic en el botón **Comprar ahora**, complete sus datos e inmediatamente tendrá asegurada la protección antivirus. A los pocos días recibirá cómodamente la factura en PDF por correo electrónico.

**Nota:** Este cuadro de diálogo aparece solamente después del primer año. Luego su licencia G DATA se prolongará cada año de manera automática. No obstante, puede rescindir este servicio de prolongación en todo momento y sin justificación.

## Cambio de ordenador

Con sus datos de acceso existentes puede utilizar su producto G DATA en otro ordenador o en uno nuevo. Simplemente, instale el software y introduzca sus datos de acceso. El servidor de actualizaciones configura la conexión con el nuevo ordenador. Si en su ordenador antiguo se encuentra aún el software G DATA se debe transferir la licencia desde el ordenador anterior al nuevo.

**Nota:** El número de transferencias de licencias es limitado, al alcanzar el valor límite la licencia se bloquea completamente de manera que no se pueden descargar más actualizaciones.

## Copyright

Copyright © 2017 G DATA Software AG

Motor: El motor de escaneo de virus y los motores de escaneo de spyware están basados en BitDefender technologies © 1997-2017 BitDefender SRL.

OutbreakShield: © 2017 Commtouch Software Ltd.

[G DATA - 17/02/2017, 10:00]