bitdefender

INTERNET SECURITY 2008

Guía de usuario

BitDefender Internet Security 2008

Guía de usuario

publicado 2008.02.20

Advertencia legal


bitdefender

Tabla de contenidos

LICENCIA DE USO DE SOFTWARE PARA EMPRESAS

Esta Licencia está destinada al uso del software por parte de Empresas u otras personas jurídicas

Aviso

SI USTED NO ESTÁ DE ACUERDO CON LOS TÉRMINOS Y CONDICIONES DE ESTE CONTRATO DE LICENCIA, LE ROGAMOS QUE NO INSTALE ESTE SOFTWARE. UNA VEZ INSTALADO, O UTILIZADO DE CUALQUIER FORMA, SIGNIFICA QUE USTED CONOCE Y ACEPTA LOS TÉRMINOS Y CONDICIONES DEL CONTRATO, QUEDANDO VINCULADO POR LOS MISMOS.

Este Contrato de Licencia constituye un acuerdo legal entre Vd. (como persona jurídica) y BITDEFENDER S.R.L., en relación al uso del software BitDefender por parte de los usuarios del ámbito de su empresa. Este software, incluyendo también el soporte físico que lo contiene, así como toda la documentación impresa y/o electrónica relativa al mismo (en adelante referido como BitDefender), pertenece a BITDEFENDER S.R.L. (en adelante referida como BITDEFENDER) y se encuentra protegido por la legislación nacional e internacional aplicable en materia de derechos de propiedad intelectual.

La instalación, copia o cualquier otra forma de utilización de BitDefender significa que Vd. conoce y acepta los presentes términos y condiciones, quedando vinculado por los mismos. Si no está de acuerdo con dichos términos y condiciones, no instale ni utilice en forma alguna BitDefender.

Licencia BitDefender. BitDefender se encuentra protegido por la legislación nacional e internacional aplicable en materia de propiedad intelectual. El uso de BitDefender está sometido a la concesión de Licencia, la cual se adquiere junto con el soporte físico que contiene el software –que no se vende por separado–, sin que Vd. adquiera la propiedad de dicho soporte físico, sino que únicamente se le cede durante la vigencia de la Licencia.

Concesión de Licencia. . Mediante el presente Contrato, BITDEFENDER otorga al adquirente de la Licencia (en adelante referido como el Usuario), la facultad no exclusiva, limitada y no transferible de usar BitDefender en los terminos y condiciones del Contrato. Al efecto, el Usuario sólo queda autorizado para instalar y usar BitDefender en un único equipo o dispositivo (ordenador, PDA, o cualquier otro dispositivo idóneo) dentro de su propio ámbito y por parte de su propio personal. El

Usuario podrá realizar una copia adicional en otro dispositivo con el único fin de servir de copia de seguridad.

Precio de la Licencia. En contraprestación por la Licencia de uso de BitDefender concedida al Usuario, éste deberá satisfacer el precio establecido en cada momento por BITDEFENDER y/o el distribuidor autorizado. El precio de la Licencia estará sujeto a cambios, sin necesidad de aviso previo al Usuario.

Vigencia de la Licencia. La Licencia entrará en vigor a partir de la fecha de adquisición y finalizará al terminar el período para el cual ha sido adquirida, según consta en el correspondiente documento de compra, y sin perjuicio de lo que resulte de eventuales renovaciones.

Resolución por incumplimiento. BITDEFENDER podrá dar la Licencia por automaticamente terminada, sin necesidad de notificación previa al Usuario, en caso de incumplimiento por su parte de cualquiera de los términos y condiciones de la misma. En ese caso, el Usuario no tendrá derecho a la devolución del precio satisfecho.

Actualizaciones de BitDefender. Para disponer del servicio de actualizaciones de BitDefender el Usuario debe haberse registrado previamente. Este servicio incluye la actualización de BitDefender a la versión actual que reemplaza y/o complementa el producto inicial o una versión posterior del mismo. El Usuario sólo podrá usar la versión actualizada de BitDefender en los términos y condiciones estipulados en el presente Contrato, sin perjuicio de lo que resulte, en su caso, de la licencia propia de la actualización. En particular, el Usuario sólo podrá instalar y usar la versión actualizada de BitDefender si dispone de una Licencia de uso de una versión anterior, y asimismo, si BitDefender ha sido actualizado en un equipo o dispositivo queda expresamente prohibida su utilización en otros.

Derechos de propiedad intelectual. Todos los derechos, títulos e intereses relativos a BitDefender, incluyendo, en particular, y no limitado a los derechos de propiedad intelectual sobre el software, así como sobre cualesquiera imágenes, fotografías, logos, animaciones, vídeo, audio, música, textos y “applets” incorporados a BitDefender, y a cualesquiera materiales adjuntos, impresos o electrónicos, pertenecen a BITDEFENDER y están protegidos por las leyes y tratados internacionales que regulan los derechos de propiedad intelectual. Salvo el derecho de uso en los términos y condiciones establecidos en este Contrato de Licencia, Vd. no queda facultado para realizar cualquier otra utilización de BitDefender. En particular, queda expresamente prohibido conceder sublicencias, alquilar, vender, o ceder de cualquier otra forma la Licencia BitDefender.

Garantía limitada. BITDEFENDER garantiza que el soporte que contiene su copia de BitDefender está libre de defectos, durante un período de treinta días desde la

fecha de entrega al Usuario. En caso de incumplimiento de esta garantía, la reparación a la que tiene derecho el Usuario se limita única y exclusivamente a que BITDEFENDER, a eleccción del Usuario, o bien le reemplace el soporte defectuoso por uno libre de defectos, a la recepción de aquél, o bien le devuelva el precio pagado por la Licencia. Esta garantía no cubre el caso de pérdida, robo o daño accidental del soporte, ni cuando éste haya sido indebidamente utilizado o manipulado.

Excepto las garantías que expresamente se ofrecen en este Contrato, y en los términos de las mismas, BITDEFENDER no asume ninguna otra garantía relativa a BitDefender, así como a sus actualizaciones, mantenimiento, soporte técnico o cualesquiera servicios proporcionados en conexión con BitDefender. En particular, BITDEFENDER no garantiza al Usuario que BitDefender esté libre de errores, ni le asegura, en su caso, la corrección de los mismos. BITDEFENDER tampoco garantiza que BitDefender responda a los requerimientos y/o necesidades del Usuario al adquirirlo.

Daños y perjuicios. Cualquiera que use, pruebe, evalue o utilice en cualquier forma BitDefender asume todos los riesgos de tal utilización y será el único responsable de los daños y/o perjuicios causados. En ningún caso, BITDEFENDER será responsable de los daños y/o perjuicios de cualquier clase, ya sean directos o indirectos, derivados de la instalación, ejecución o utilización en cualquier forma de BitDefender, incluso en el caso que BITDEFENDER haya sido advertida de la existencia o de la posibilidad de que se produzcan tales daños. En todo caso, la responsabilidad de BITDEFENDER quedará limitada a la restitución al Usuario del importe satisfecho por la Licencia.

Entornos de utilización. Este software no ha sido diseñado ni está indicada su utilización en cualquier entorno que requiera una operativa altamente estable y libre de fallos. En particular, este software no está destinado para su utilización en la navegación aerea, centrales nucleares, comunicaciones, armamento, sistemas o equipos de vida asistida, control del tráfico aereo, o cualquier otra aplicación o instalación en las que un error de funcionamiento pudiera tener un resultado de muerte o provocar daños personales o materiales graves.

Eventual nulidad y modificación de las estipulaciones de la Licencia. En el caso que sea anulado o se declare nulo alguno de los términos y/o condiciones de esta Licencia, dicha invalidez no afectará al resto de las estipulaciones de la misma, que mantendrán su plena eficacia. BITDEFENDER se reserva el derecho a modificar en cualquier momento los términos y condiciones de la Licencia, siendo dichas modificaciones automáticamente aplicables a cualesquiera renovaciones de la Licencia que las incluyan.

Ley aplicable y jurisdicción. Esta Licencia se regirá por las leyes de Rumanía. Los Juzgados y Tribunales de Rumanía tendrán jurisdicción exclusiva para conocer y resolver cualesquiera disputas relacionadas con la presente Licencia, aceptando las

partes someterse a los mismos, con renuncia expresa a cualquier otra jurisdicción que pudiera corresponderles.

Prólogo

Esta guía está dirigida a todos los usuarios que han elegido **BitDefender Internet Security 2008** como solución de seguridad para sus ordenadores personales. La información presentada en este libro es apta no sólo para expertos en informática, sino para todo aquel capaz de trabajar bajo Windows.

Este manual le describirá el uso de **BitDefender Internet Security 2008**, la compañía y el equipo que lo ha desarrollado le guiarán a través del proceso de instalación y le enseñarán a configurarlo. Descubrirá cómo utilizar **BitDefender Internet Security 2008**, cómo actualizarlo, probarlo y personalizarlo. Aprenderá a sacarle el máximo provecho.

Le deseamos una provechosa y agradable lectura.

1. Convenciones utilizadas en este libro

1.1. Convenciones Tipográficas

En este manual se utilizan distintos estilos de texto con el fin de mejorar su lectura. Su aspecto y significado se indica en la tabla que aparece continuación.

Apariencia	Descripción
`sample syntax`	Los ejemplos de sintaxis se muestran con caracteres `monoespaciados`.
http://www.bitdefender.com	Los enlaces URL le dirigen a algunas ubicaciones externas, a servidores http o ftp.
support@bitdefender.com	Las direcciones de e-mail se incluyen en el texto como información de contacto.
“Prólogo” (p. xii)	Este es un enlace interno, que le dirigirá a algún apartado dentro de este documento.
`filename`	Los archivos y carpetas se muestran con una fuente `monoespaciada`.
option	Todas las opciones del producto se muestran usando letra en **negrita**.

Apariencia	Descripción
`sample code listing`	El listado de código se muestra con caracteres `monoespaciados`.

1.2. Advertencias

Las advertencias son notas dentro del texto, marcadas gráficamente, que atraen su atención con información adicional relacionada con el párrafo que está leyendo.

Nota
La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información interesante, como una característica específica o un enlace a algún tema relacionado.

Importante
Esta requiere su atención y no es recomendable saltársela. Normalmente proporciona información importante aunque no extremadamente crítica.

Aviso
Se trata de información crítica que debería tartar con extremada cautela. Nada malo ocurrirá si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente peligroso.

2. La Estructura del Manual

Esta guía está dividida en varias partes que abordan los temas más importantes: Además, se incluye un glosario para aclarar los términos técnicos utilizados en la guía.

Pasos de la Instalación. Instrucciones paso a paso para instalar BitDefender en una estación de trabajo. Se trata de un exhaustivo tutorial sobre la instalación de **BitDefender Internet Security 2008**. Se le guiará a través del proceso completo de instalación, empezando por los pre-requisitos para una correcta instalación. Finalmente, se le describirá el procedimiento de desinstalación en caso de que necesite desinstalar BitDefender.

Administración Básica. Descripción de la administración básica y del mantenimiento de BitDefender.

Administración Avanzada de Seguridad. Una presentación detallada de las opciones de seguridad de BitDefender. El capitulo detallará todas las opciones

avanzadas de configuración disponibles en la consola. Se le ha enseñado a configurar y utilizar todos los módulos de BitDefender para proteger a su equipo eficazmente contra toda clase de amenazas (malware, spam, hackers, contenido inapropiado y otros).

CD de Rescate de BitDefender. Descripción del CD de Rescate de BitDefender. Le ayuda a entender el funcionamiento y las características que le ofrece este CD de autoarranque.

Conseguir Ayuda. Dónde mirar y dónde pedir ayuda si se produce una situación inesperada.

Glosario. El Glosario trata de explicar algunos términos técnicos o poco comunes que encontrará en las páginas de este documento.

3. Petición de Comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos probado y verificado toda la información como mejor hemos sabido. Por favor, escríbanos para contarnos cualquier tipo de defecto que encuentre en este manual o cómo cree que se podría mejorar, y así ayudarnos a ofrecerle la mejor documentación posible.

Háganoslo saber enviando un e-mail a documentation@bitdefender.com.

Importante

Por favor, escriba en Inglés todos aquellos correos relacionados con la documentación, para poder procesarlos correctamente.

Pasos de la Instalación

1. Instalación de BitDefender Internet Security 2008

El apartado **Instalación de BitDefender Internet Security 2008** de esta guía contiene los siguientes temas:

- Requisitos del Sistema
- Pasos de la Instalación
- Asistente de Configuración Inicial
- Actualización de la versión del Producto
- Reparar o Desinstalar BitDefender

1.1. Requisitos del Sistema

Para garantizar el correcto funcionamiento del producto, antes de la instalación compruebe que su equipo cumple los siguientes requisitos mínimos:

- Sistemas Operativos: Windows 2000 SP4 / XP SP2 32b y 64b / Vista 32b y 64b; Internet Explorer 6.0 (o superior)
- Clientes de correo soportados: Microsoft Outlook 2000 / 2003 / 2007; Microsoft Outlook Express; Microsoft Windows Mail; Thunderbird 1.5 y 2.0

Windows 2000

- Procesador de 800 MHz o superior
- Mínimo 256 MB de RAM (512 MB recomendado)
- Mínimo 60 MB de espacio libre en disco

Windows XP

- Procesador de 800 MHz o superior
- Mínimo 256 MB de RAM (1 GB recomendado)
- Mínimo 60 MB de espacio libre en disco

Windows Vista

- Procesador de 800 MHz o superior
- Mínimo 512 MB de RAM (1 GB recomendado)

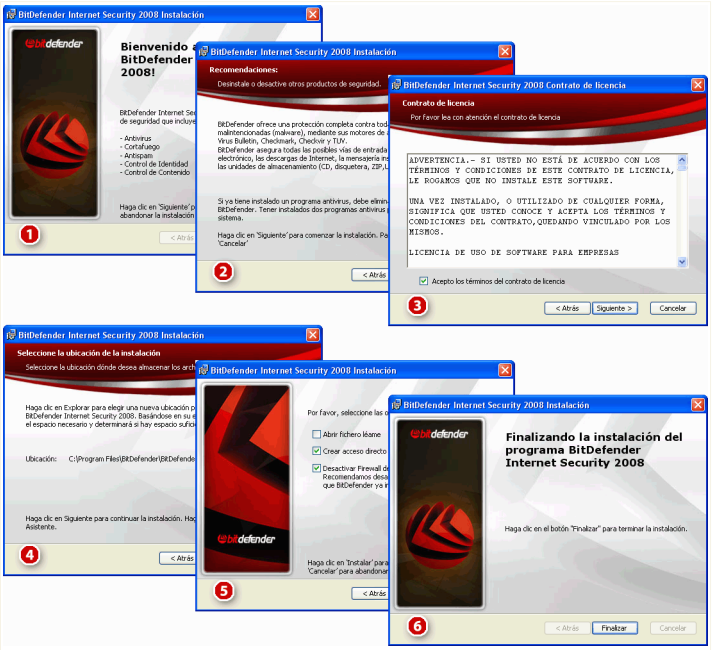
- Mínimo 60 MB de espacio libre en disco

BitDefender Internet Security 2008 está disponible para descargar y evaluar desde http://www.bitdefender.es.

1.2. Pasos de la Instalación

Localice el paquete de instalación y haga doble clic en él. Se iniciará un asistente que le guiará a través del proceso de instalación:

Antes de iniciar el asistente de instalación, BitDefender comprobará si existen nuevas versiones del paquete de instalación. Si existe una nueva versión, se le preguntará si desea descargarla. Haga clic en **Si** para descargar la nueva versión, o en **No** para continuar la instalación actual.



Pasos de la Instalación

Siga estos pasos para instalar BitDefender Internet Security 2008:

1. Haga clic en **Siguiente** para continuar con el proceso de instalación o haga clic en **Cancelar** si quiere abandonar.
2. Haga clic en **Siguiente**.

   BitDefender Internet Security 2008 le avisará si tiene otros productos antivirus instalados en su ordenador. Haga clic en **Desinstalar** para eliminar el producto correspondiente. Si desea continuar sin desinstalar los productos detectados, haga clic en **Siguiente**.

   Aviso
   Es sumamente recomendable desinstalar los productos antivirus detectados antes de instalar BitDefender. Ejecutar dos antivirus a la vez puede provocar inestabilidad en el sistema.

3. Por favor, lea el Contrato de Licencia para el usuario final con atención y si está de acuerdo con las condiciones previstas, seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**. Si no está de acuerdo con las cláusulas de este contrato, haga clic en **Cancelar**. Abandonará el proceso y saldrá de la instalación.
4. Por defecto, BitDefender Internet Security 2008 se instalará en `C:\Archivos de programa\BitDefender\BitDefender 2008`. Si desea cambiar la ruta de instalación, haga clic en **Explorar** y seleccione la carpeta dónde desea instalar BitDefender Internet Security 2008.

   Haga clic en **Siguiente**.
5. Seleccione las opciones relativas al proceso de instalación. Algunas opciones están seleccionadas por defecto:
   - **Abrir fichero léame** - para abrir el fichero léame al final de la instalación.
   - **Crear acceso directo en el Escritorio** - para poner un acceso directo de BitDefender Internet Security 2008 en el Escritorio al finalizar la instalación.
   - **Expulsar el CD al completar la instalación** - para expulsar el CD cuando finalice la instalación; esta opción aparece cuando instala el producto desde un CD.
   - **Desactivar el cortafuego de Windows** - para desactivar el Firewall de Windows.

     Importante
     Le recomendamos desactivar el Firewall de Windows puesto que BitDefender Internet Security 2008 ya incluye un cortafuego avanzado. Ejecutar dos cortafuegos en el mismo ordenador puede causar problemas.

   - **Desactivar Windows Defender** - para desactivar Windows Defender; esta opción sólo aparece en Windows Vista.

   Haga clic en **Instalar** para iniciar la instalación del producto.

Importante

Durante el proceso de instalación aparecerá un Asistente. Este Asistente le ayudará a registrar su **BitDefender Internet Security 2008**, crear una cuenta de BitDefender y configurar BitDefender para realizar las tareas necesarias para la seguridad de su equipo.

Debe completar el proceso guiado por el Asistente para poder avanzar al siguiente paso.

6. Haga clic en **Finalizar**. Se le solicitará reiniciar el sistema para que se complete el proceso de instalación. Recomendamos realizarlo lo antes posible.

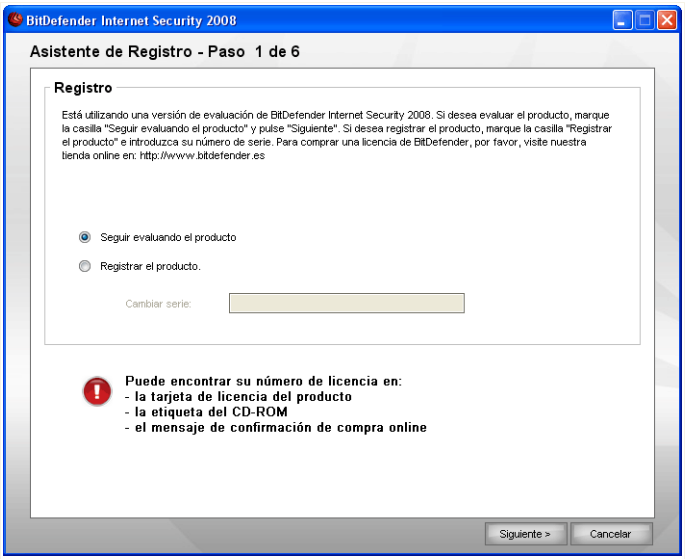
   Si ha aceptado la carpeta de instalación predeterminada, se creará una nueva carpeta llamada `BitDefender` dentro de `Archivos de Programa`, que a su vez contiene otra subcarpeta llamada `BitDefender 2008`.

1.3. Asistente de Configuración Inicial

Durante el proceso de instalación aparecerá un Asistente. Este Asistente le ayudará a registrar su **BitDefender Internet Security 2008**, crear una cuenta de BitDefender y configurar BitDefender para realizar las tareas necesarias para la seguridad de su equipo.

No es obligatorio completar este Asistente. Sin embargo, recomendamos hacerlo para así ganar tiempo y garantizar la seguridad de su sistema incluso antes de que BitDefender Internet Security 2008 esté instalado.

1.3.1. Paso 1/6 - Registrar BitDefender Internet Security 2008



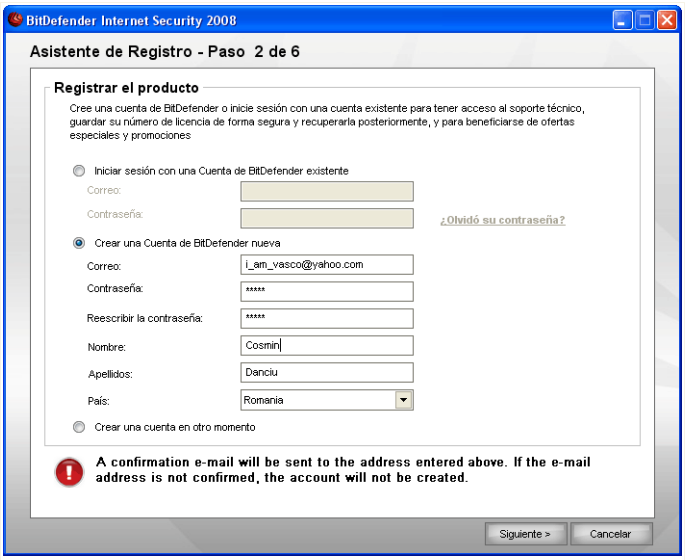
Registro

Seleccione **Registrar el Producto** para registrar **BitDefender Internet Security 2008**. Escriba el número de licencia en el campo **Cambiar serie**.

Para continuar la evaluación del producto seleccione **Seguir evaluando el producto**.

Haga clic en **Siguiente**.

1.3.2. Paso 2/6 - Crear una cuenta de BitDefender



Creación de la Cuenta

No tengo una cuenta de BitDefender

Para poderse beneficiar del soporte técnico de BitDefender y de otros servicios gratuitos necesita crear una cuenta.

Nota
Si desea crear una cuenta en otro momento, seleccione la opción correspondiente.

Para crear una cuenta de BitDefender, Seleccione **Crear una nueva cuenta BitDefender** e introduzca la información solicitada. Los datos que introduzca aquí serán confidenciales.

- **E-mail** - introduzca su dirección de correo.
- **Contraseña** - introduzca una contraseña para su cuenta de BitDefender.

Nota
La contraseña debe contener 4 caracteres como mínimo.

- **Repetir contraseña** - introduzca de nuevo la contraseña especificada anteriormente.
- **Nombre** - introduzca su nombre.
- **Apellidos** - introduzca sus Apellidos.
- **País** - introduzca el país en el que reside.

Nota
Utilice la dirección indicada y contraseña para iniciar sesión en su cuenta http://myaccount.bitdefender.com.

Para crear una cuenta con éxito, primero debe activar su dirección de e-mail. Consulte la cuenta de correo indicada anteriormente y siga las instrucciones indicadas en el mensaje enviado por el servicio de registro de BitDefender.

Haga clic en **Siguiente** para continuar.

Ya tengo una cuenta de BitDefender

BitDefender detectará automáticamente si previamente ha registrado una cuenta de BitDefender en su equipo. En este caso, sólo tendrá que hacer clic en **Siguiente**.

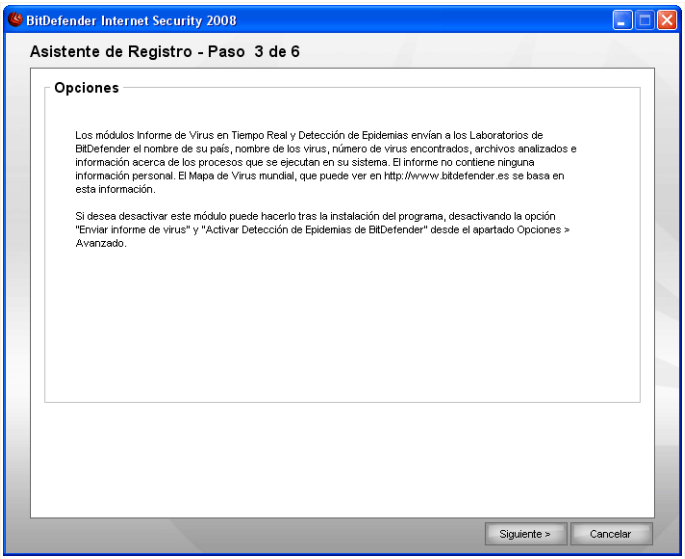
Si ya tiene una cuenta activa, pero BitDefender no la detecta, seleccione **Iniciar sesión con una Cuenta de BitDefender existente** e introduzca la dirección de correo y la contraseña de su cuenta.

Nota
Si la contraseña indicada es incorrecta, se le volverá a solicitar cuandopulse en **Siguiente**. Haga clic en **Aceptar** para introducir de nuevo la contraseña opulse en **Cancelar** para salir del Asistente.

Si ha olvidado su contraseña haga clic en **¿Olvidó su contraseña?** y siga las instrucciones.

Haga clic en **Siguiente** para continuar.

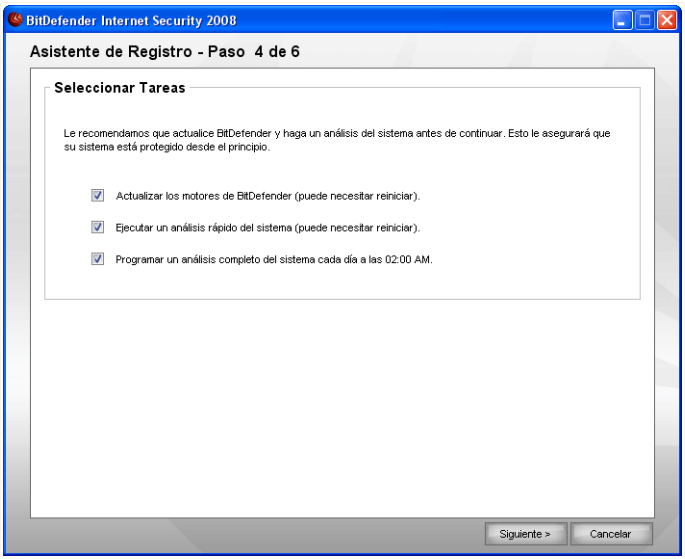
1.3.3. Paso 3/6 - Aprender sobre RTVR



Información RTVR

Haga clic en **Siguiente** para continuar o haga clic en **Atrás** para abandonar el Asistente.

1.3.4. Paso 4/6 - Seleccionar la Tarea a Ejecutar



Selección de la Tarea

Configure BitDefender Internet Security 2008 para que ejecute tareas importantes para la seguridad de su sistema.

Dispone de las siguientes opciones:

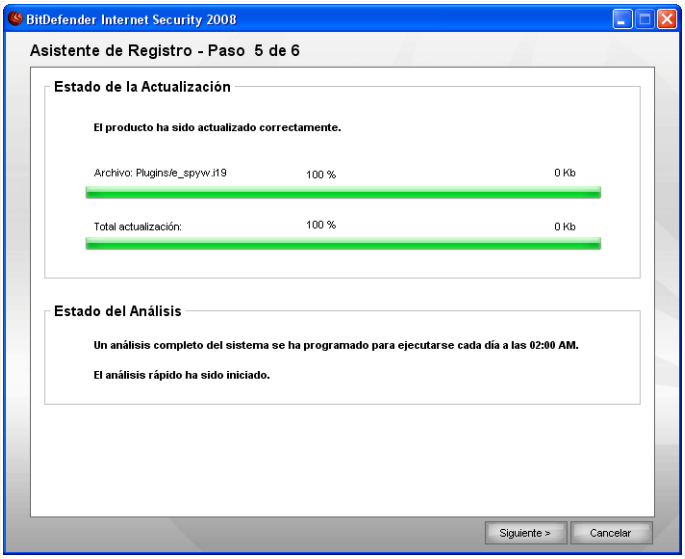
- **Actualizar los motores de BitDefender (puede solicitar el reinicio)** - durante el siguiente paso se realizará una actualización de los motores de análisis de BitDefender para proteger su equipo de las últimas amenazas.
- **Realizar un análisis rápido del sistema (puede solicitar el reinicio)** - durante el siguiente paso se realizará un análisis rápido del sistema para asegurarse que los ficheros de las carpetas `Windows` y `Archivos de Programa` no están infectados.
- **Prgramar un análisis completo del sistema cada día a las 02:00 AM** - ejecuta un análisis completo del sistema cada día a las 2 AM.

Importante
Recomendamos activar estas opciones antes de continuar con el siguiente paso, y así garantizar la seguridad de su sistema.

Si no selecciona ninguna opción, o selecciona sólo la última, omitirá el siguiente paso.

Haga clic en **Siguiente** para continuar o haga clic en **Atrás** para abandonar el Asistente.

1.3.5. Paso 5/6 - Esperar a que Finalicen las Tareas

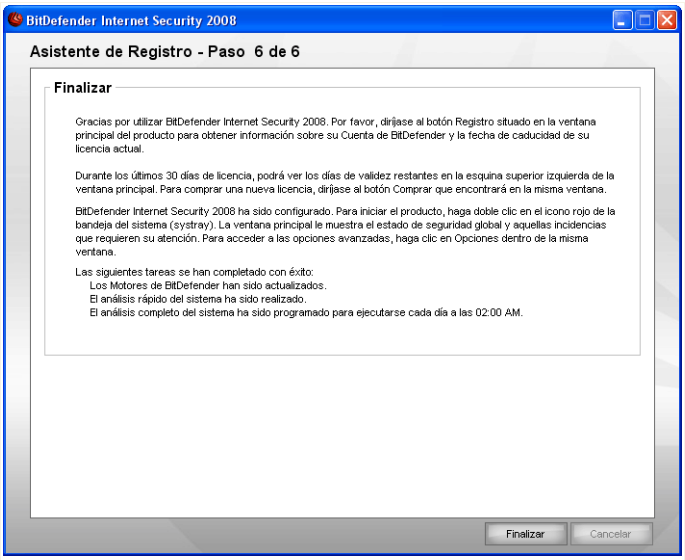


Estado de la Tarea

Espere que se complete(n) la(s) tarea(s). Puede comprobar el estado de las(s) tarea(s) seleccionada(s) en el paso anterior.

Haga clic en **Siguiente** para continuar o haga clic en **Atrás** para abandonar el Asistente.

1.3.6. Paso 6/6 - Resumen



Finalizado

Este es el último paso del asistente de configuración.

Haga clic en **Finalizar** para completar y continuar con el proceso de instalación.

1.4. Actualización de la versión del Producto

El proceso de actualización del producto puede realizarse a través de estas opciones:

- **Instalar la nueva versión sin desinstalar la versión anterior – para la v8 o superior, Internet Security excluido**

  Haga doble clic en el archivo de instalación y siga los pasos del asistente descrito en el apartado "*Pasos de la Instalación*" (p. 3).

  Importante
  Durante el proceso de instalación aparecerá un mensaje de error causado por el `servicio Filespy`. Haga clic en **Aceptar** para continuar con la instalación.

- **Desinstalar su versión anterior e instalar la nueva – válido para todas las versiones de BitDefender**

  Primero debe desinstalar su versión anterior, reinciar el equipo e instalar la nueva verión tal y como se describe en el apartado "*Pasos de la Instalación*" (p. 3).

Importante
Si actualiza el producto desde la versión BitDefender 8 o posterior, le recomendamos guardar la configuración de BitDefender y las listas de Amigos y Spammers. Cuando finalice el proceso de actualización del producto, podrá cargarlos de nuevo.

1.5. Reparar o Desinstalar BitDefender

Si desea reparar o desinstalar **BitDefender Internet Security 2008**, siga estos pasos en el menú Inicio de Windows: **Inicio** → **Programas** → **BitDefender 2008** → **Reparar o Desinstalar**.

Se le solicitará que confirme su elección pulsando **Siguiente**. Aparecerá una nueva ventana en la que podrá seleccionar:

- **Reparar** - para reinstalar todos los componentes del programa instalados anteriormente.

  Importante
  Antes de reparar el producto recomendamos guardar las listas de Amigos y Spammers. También puede guardar la configuración de BitDefender y la base de datos del filtro Bayesiano. Cuando finalice el proceso de reparación podrá cargarlos de nuevo.

  Si elige reparar BitDefender, aparecerá una nueva ventana. Haga clic en **Reparar** para iniciar el proceso de reparación.

  Reinicie el ordenador cuando se le indique, y a continuación haga clic en **Instalar** para reinstalar BitDefender Internet Security 2008.

  Al finalizar el proceso de instalación, aparecerá una nueva ventana. Haga clic en **Finalizar**.
- **Eliminar** - para eliminar todos los componentes instalados.

  Nota
  Le recomendamos elegir la opción **Desinstalar** para realizar una reinstalación limpia.

  Si decide desinstalar BitDefender, aparecerá una nueva ventana.

Importante

Al desinstalar BitDefender, no estará protegido contra las amenazas de malware, como virus, spyware, o hackers. Si desea activar el Firewall de Windows y Windows Defender (sólo en Windows Vista) al finalizar la desinstalación de BitDefender, seleccione la casilla correspondiente.

Haga clic en **Desinstalar** para iniciar la desinstalación de BitDefender Internet Security 2008 en su equipo.

Durante el proceso de desinstalación se le preguntará si desea enviarnos su feedback. Haga clic en **Aceptar** para realizar una encuesta online que consiste en 5 breves preguntas. Si no desea realizar la encuesta, haga clic en **Cancelar**.

Al finalizar el proceso, aparecerá una nueva ventana. Haga clic en **Finalizar**.

Nota

Al finalizar el proceso de desinstalación, recomendamos eliminar la carpeta `BitDefender` ubicada dentro de `Archivos de Programa`.

Error durante la desinstalación de BitDefender

Si se produce algún error durante la desinstalación de BitDefender, el proceso de desinstalación se cancelará y aparecerá una nueva ventana. Haga clic en **Ejecutar Desinstalación** para asegurarse que BitDefender se ha desinstalado completamente. La herramienta de desinstalación eliminará todos los archivos y claves del registro que no hayan sido eliminadas durante el proceso de desinstalación automático.

Administración Básica

2. Conseguir Ayuda

Una vez tenga BitDefender instalado, su equipo estará protegido. Puede abrir el Centro de Seguridad de BitDefender para comprobar el nivel de seguridad de su sistema, tomar medidas de prevención o configurar el producto.

Para acceder a la consola de administración debe hacer clic en el menú Inicio de Windows y luego seguir la ruta **Inicio** → **Programas** → **BitDefender 2008** → **BitDefender Internet Security 2008**, o de manera más rápida, haciendo doble clic en **el icono de BitDefender** situado en la bandeja del sistema.

Centro de Seguridad de BitDefender

El Centro de Seguridad de BitDefender contiene dos áreas:

- El área de **Estado**: contiene información sobre la seguridad de su equipo y le ayudará a reparar los fallos de seguridad detectados, o ver cuantas incidencias de seguridad podrían afectar a su equipo. Al hacer clic en el botón rojo **Reparar Incidencias**, las vulnerabilidades se solucionarán en el acto o bien se le guiará para que pueda solucionarlas con la máxima facilidad. Al mismo tiempo, encontrará

cuatro botones que corresponden a las categorías de seguridad disponibles. Los botones verdes indican que no existe ningún riesgo. Los botones amarillos o rojos indican riesgos de seguridad medios o altos, respectivamente. Para repararlos, haga clic en el botón amarillo/rojo, y a continuación haga clic en el botón **Reparar**, uno por uno, o en el botón **Reparar Todo**. El color gris indica que el componente no está configurado.

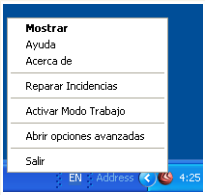
- El área **Tareas Rápidas**: contiene información sobre la seguridad de su equipo y le ayudará a reparar los fallos de seguridad detectados.

Además, el Centro de Seguridad BitDefender contiene varios accesos directos útiles.

Enlace	*Descripción*
Comprar	Abre una página desde la que puede comprar el producto.
Mi Cuenta	Abre la página de su cuenta de BitDefender.
Registro	Abre el asistente de registro.
Ayuda	Abre el archivo de ayuda.
Soporte	Abre la página web de soporte de BitDefender.
Configuración	Abre la consola de opciones avanzadas.
Historial	Abre una ventana con el historial y eventos de BitDefender.

2.1. Icono de BitDefender en la Bandeja del Sistema

Para poder administrar el producto rápidamente, puede utilizar el icono de BitDefender situado en la bandeja del sistema.



Icono de BitDefender

Haciendo doble clic en este icono se abrirá el Centro de Seguridad de BitDefender. Si hace clic con el botón derecho en el icono, aparecerá un menú contextual desde el que podrá administrar rápidamente el producto BitDefender.

- **Mostrar** - abre el Centro de Seguridad de BitDefender.
- **Ayuda** - abre el archivo de ayuda.
- **Acerca de** - abre la ventana de información de BitDefender.
- **Reparar Incidencias** - le ayuda a eliminar las vulnerabilidades de seguridad.
- **Activar / Desactivar Modo Trabajo** - activa o desactiva el Modo Trabajo.
- **Abrir opciones avanzadas** - da acceso a la consola de opciones avanzadas.
- **Actualizar** - realiza una actualización inmediata. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización.
- **Salir** - cierra la aplicación.

Cuando el Modo Trabajo está activado, puede ver la letra G encima del icono de BitDefender.

Si hay incidencias críticas que afectan a la seguridad de su sistema, aparecerá una marca de exclamación encima del icono de BitDefender. Puede situar el cursor encima del icono para ver el número de incidencias que afectan a la seguridad de su sistema.

2.2. La barra de actividad del análisis

La **barra de análisis de la actividad** es una vista gráfica de la actividad de análisis de su sistema.

Las barras verdes (**Archivos**) representan el número de archivos analizados por segundo con BitDefender, en una escala de 0 a 50.

Las barras rojas mostradas en la ventana **Internet** representan el número de KBytes transferidos (enviados y recibidos en Internet) por segundo, a una escala de 0 a 100.

Barra de Actividad

Nota
La Barra de Actividad del Análisis le avisará si la protección en tiempo real o el Cortafuego están desactivados, mostrando una cruz roja en la zona correspondiente (**Archivos** o **Internet**).

Puede utilizar la opción **Barra de actividad del Análisis** para analizar archivos. Arrastre y suelte los archivos que desea analizar sobre la ventana de actividad BitDefender.

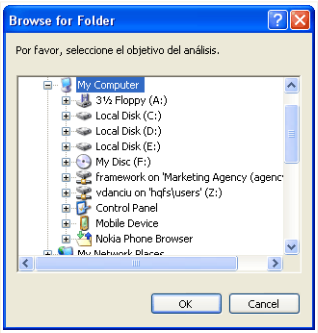
Nota
Para más información, por favor, consulte el "*Análisis al Arrastrar y Soltar*" (p. 69) de esta guía de usuario.

Para ocultar la barra de actividad haga clic derecho encima y seleccione **Ocultar**. Para ocultar completamente la barra, haga clic en **Avanzado** dentro de la consola de configuración, y desmarque la casilla **Activar barra de Actividad del Análisis**.

2.3. Análisis Manual de BitDefender

Si desea analizar rápidamente una carpeta determinada, puede utilizar el Análisis Manual de BitDefender.

Para acceder al Análisis Manual de BitDefender, siga estos pasos en el menú Inicio de Windows **Inicio** → **Programas** → **BitDefender 2008** → **Análisis Manual de BitDefender** Aparecerá la siguiente pantalla:



Análisis Manual de BitDefender

Sólo tiene que navegar entre sus carpetas, seleccionar la carpeta que desea analizry hacer clic en **Aceptar**. El BitDefender Scanner aparecerá y la guiará a través del proceso de análisis.

2.4. Modo Trabajo

El nuevo Modo Trabajo modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el funcionamiento del sistema. Cuando activa el Modo Trabajo, se aplica la siguiente configuración:

- Todas las alertas y ventanas emergentes de BitDefender quedan desactivadas.
- El nivel de protección en tiempo real de BitDefender queda fijado a **Permisivo**.
- El Cortafuego de BitDefender está configurado en **Modo Trabajo**.

Cuando el Modo Trabajo está activado, puede ver la letra G encima del icono de BitDefender.

2.4.1. Utilizando el Modo Trabajo

Si desea activar el Modo Trabajo, siga uno de estos métodos:

- Clic derecho en el icono de BitDefender de la Bandeja del Sistema y seleccione **Activar Modo Trabajo**.
- Pulse `Alt+G` (el atajo de teclado predeterminado).

Importante
No olvide desactivar el Modo Trabajo una vez haya terminado. Para desactivarlo puede seguir los mismos pasos que ha utilizado para activarlo.

2.4.2. Cambiando el Atajo de Teclado del Modo Trabajo

Si desea cambiar el atajo de teclado, siga estos pasos:

1. Haga clic en **Opciones** en el Centro de Seguridad de BitDefender para abrir la consola de opciones de configuración.

   Nota
   También puede hacer clic derecho sobre el icono de BitDefender situado en la Bandeja del Sistema y seleccione **Abrir opciones avanzadas**.

2. Haga clic en **Avanzado**.
3. Debajo de la opción **Activar Atajo de Teclado para el Modo Trabajo**, configure las teclas deseadas:
   - Elija las teclas que desea utilizar seleccionado alguna de estas teclas: Control (`Ctrl`), Shift (`Shift`) o Alternate (`Alt`).
   - En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

   Por ejemplo, si desea utilizar la combinación de teclas `Ctrl+Alt+D`, marque sólo `Ctrl` y `Alt`, y a continuación escriba la tecla `D`.

   Nota
   Si desmarca la casilla situada junto a **Activar Atajo de Teclado para el Modo Trabajo**, desactivará la combinación de teclas.

3. Estado de Seguridad

El estado de seguridad muestra una lista sistemáticamente organizada y fácilmente manejable de vulnerabilidades de seguridad detectadas en su ordenador. BitDefender Internet Security 2008 le avisará siempre que detecte un problema que pueda afectar a la seguridad de su equipo.

Hay 4 botones de estado de seguridad:

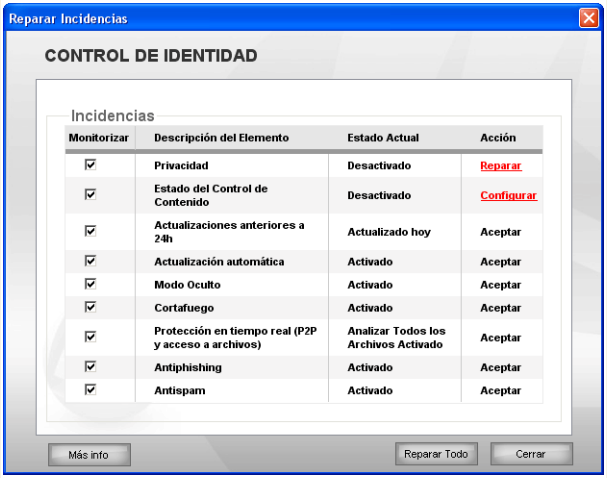
- **SEGURIDAD DEL PC**
- **SEGURIDAD DE LA RED**
- **CONTROL DE IDENTIDAD**
- **CONTROL PARENTAL**

En la parte izquierda podrá ver el número de incidencias que afectan a la seguridad de su sistema, junto con el botón rojo **Reparar Incidencias**.

Los cuatro botones de estado pueden aparecer en color verde, amarillo, rojo o gris, en función de su nivel actual de protección.

- **Verde** indica un riesgo de seguridad bajo.
- **Amarillo** indica un riesgo de seguridad medio.
- **Rojo** indica un riesgo de seguridad alto.
- **Gris** indica que el componente no está configurado.

Solucionar las incidencias de seguridad no supone ningún esfuerzo, puede hacerse con un simple clic en el botón **Reparar Incidencias**. Aparecerá una nueva ventana.



Problemas de Seguridad

Podrá ver una lista de problemas de seguridad y una breve descripción sobre su estado.

Para solucionar una incidencia haga clic en el botón **Reparar**. La incidencia se solucionará, o bien inmediatamente, o bien siguiendo los pasos del asistente. Si decide solucionarlas todas a la vez, haga clic en el botón **Reparar Todo** y siga los pasos del asistente.

Si necesita más ayuda, haga clic en el bóton **Más info**, situado en la parte inferior de la ventana. Aparecerá una página de ayuda contextual con información detallada sobre estas incidencias y como repararlas.

Importante
Para cada una de las incidencias, existe una casilla de selección que está activada por defecto. Si no desea reparar alguna incidencia, desmarque la casilla correspondiente. Por favor, utilice esta opción con cuidado, ya que podría provocar un aumento de los riesgos de seguridad a los que se expone su equipo.

Para solucionar los problemas en otro momento, haga clic en el botón **Cerrar**.

3.1. Botón de Estado del Control de Contenido

Si el botón de estado del Control de Contenido está en verde, el módulo está activado. Si está en gris, el módulo está desactivado.

Para activar el Control de Contenido, siga estos pasos:

1. Haga clic en el botón de estado del Control de Contenido.
2. Puede utilizar cualquiera de estos métodos:
   - Para activar el Control de Contenido para todos los usuarios, haga clic en **Reparar Todo**.
   - Para activar el Control de Contenido sólo para un usuario en concreto, haga clic en el botón **Reparar** correspondiente a este usuario.

3.2. Botón del Estado de Seguridad del PC

Si el botón de estado de seguridad está en verde, no tiene nada de qué preocuparse. De lo contrario, si el botón está en amarillo, rojo o gris, significa que su ordenador está expuesto a un riesgo medio o alto.

El color del botón de estado puede cambiar cuando modifica la configuración que afecta a la seguridad de su sistema o bien cuando olvida realizar alguna tarea importante. Por ejemplo, si su último análisis es un poco antiguo, el botón de estado de seguridad estará en amarillo. Si es muy antiguo, el color será rojo.

La siguiente tabla le mostrará los elementos que se tienen en cuenta para calcular el riesgo de seguridad.

Problema	*Color*
El último análisis del sistema es antiguo.	Amarillo
El último análisis del sistema es muy antiguo.	Rojo
Protección en tiempo real desactivada.	Rojo
El nivel de protección antivirus está en nivel permisivo.	Amarillo
Actualización automática desactivada.	Rojo
La última actualización tiene un día de antigüedad.	Rojo
Antispam desactivado	Gris

Para reparar todas las incidencias, siga estos pasos:

1. Haga clic en el botón de estado de seguridad.
2. Haga clic en el botón **Reparar** para resolver las incidencias una por una o haga clic en la opción **Reparar Todo** para resolver todas las incidencias a la vez.
3. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

3.3. Botón de Estado de Seguridad de la Red

Si el botón de estado de seguridad de la red está en verde, no hay nada de qué preocuparse. De lo contrario, si el botón está en amarillo, rojo o gris, significa que su ordenador está expuesto a un riesgo medio o alto.

La siguiente tabla le mostrará los elementos que se tienen en cuenta para calcular el riesgo de seguridad.

Problema	*Color*
Cortafuego desactivado	Rojo
Modo Oculto desactivado	Rojo
La conexión wireless no está asegurada.	Rojo

Para reparar todas las incidencias, siga estos pasos:

1. Haga clic en el botón de estado de seguridad de la red.
2. Haga clic en el botón **Reparar** para resolver las incidencias una por una o haga clic en la opción **Reparar Todo** para resolver todas las incidencias a la vez.
3. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

3.4. Botón de Estado del Control de Identidad

Si el botón de estado del control de identidad está en verde, no tiene nada de qué preocuparse. De lo contrario, si el botón está en amarillo, rojo o gris, significa que su ordenador está expuesto a un riesgo medio o alto.

La siguiente tabla le mostrará los elementos que se tienen en cuenta para calcular el riesgo de seguridad.

Problema	Color
La protección de privacidad está activada.	Verde
La protección de privacidad está desactivada.	Rojo
La protección de privacidad está configurada.	Gris

Para reparar todas las incidencias, siga estos pasos:

1. Haga clic en el botón de estado de privacidad.
2. Haga clic en el botón **Reparar** para resolver las incidencias una por una o haga clic en la opción **Reparar Todo** para resolver todas las incidencias a la vez.
3. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

4. Tareas Rápidas

Debajo de los cuatro botones de estado está situada el área de **Tareas Rápidas**.

4.1. Seguridad

BitDefender incluye un módulo de Seguridad que le ayuda a mantener a BitDefender actualizado y a su equipo libre de virus.

Para entrar en el módulo de Seguridad, haga clic en la pestaña **Seguridad**.

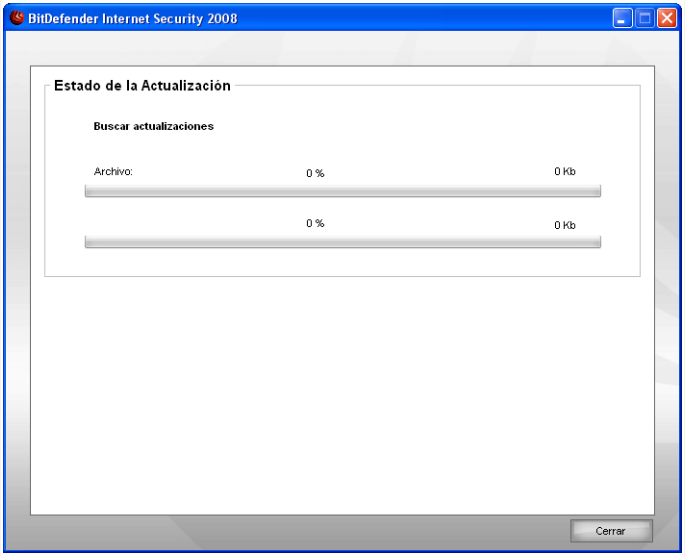
Dispone de los siguientes botones:

- **Actualizar** - realiza una actualización inmediata.
- **Analizar Mis Documentos** - inicia un análisis rápido de sus documentos.
- **Análisis en Profundidad** - inicia un análisis completo de su equipo (archivos comprimidos incluidos).
- **Análisis Completo** - inicia un análisis completo de su equipo (archivos comprimidos excluidos).

4.1.1. Actualizando BitDefender

Cada día se encuentra nuevo malware. Por esta razón es muy importante mantener BitDefender actualizado con las últimas firmas de malware.

Por defecto, BitDefender comprueba si hay nuevas actualizaciones cuando enciende su ordenador y **cada hora** desde entonces. Sin embargo, puede actualizar BitDefender en cualquier momento haciendo clic en **Actualizar**. Se iniciará el proceso de actualización e inmediatamente aparecerá la siguiente ventana:



Actualizando BitDefender

En esta ventana podrá ver el estado del proceso de actualización.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afectará al rendimiento del producto a la vez que se evita cualquier riesgo.

Si desea cerrar esta ventana, haga clic en **Cerrar**. En cualquier caso, al cerrar la ventana no se detiene el proceso de actualización.

Nota
Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar BitDefender manualmente.

Reinicie el equipo si así se le solicita. Cuando se produzca una actualización importante, se le solicitará reiniciar el equipo. Si no desea que se le vuelva a solicitar el reinicio tras una actualización, marque la casilla **Esperar a que el usuario reinicie, en lugar de preguntar**. De este modo, la próxima vez que una actualización necesite reiniciar, el producto seguirá trabajando con los archivos antiguos hasta que reinicie el equipo de forma voluntaria.

Haga clic en **Reiniciar** para reiniciar el equipo inmediatamente.

Si desea reiniciar el equipo más tarde, haga clic en **Aceptar**. Recomendamos reiniciar el equipo tan pronto como sea posible.

4.1.2. Analizando con BitDefender

Para analizar su equipo en busca de malware, inicie una tarea de análisis haciendo clic en el botón correspondiente. La siguiente tabla presenta las tareas de análisis disponibles, junto con su descripción:

Tarea	Descripción
Analizar Mis Documentos	Utilice esta tarea para analizar las carpetas del usuario en uso: `Mis Documentos`, `Escritorio` e `Inicio`. Así asegurará el contenido de sus documentos, conseguirá un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración por defecto, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración por defecto, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.

Nota

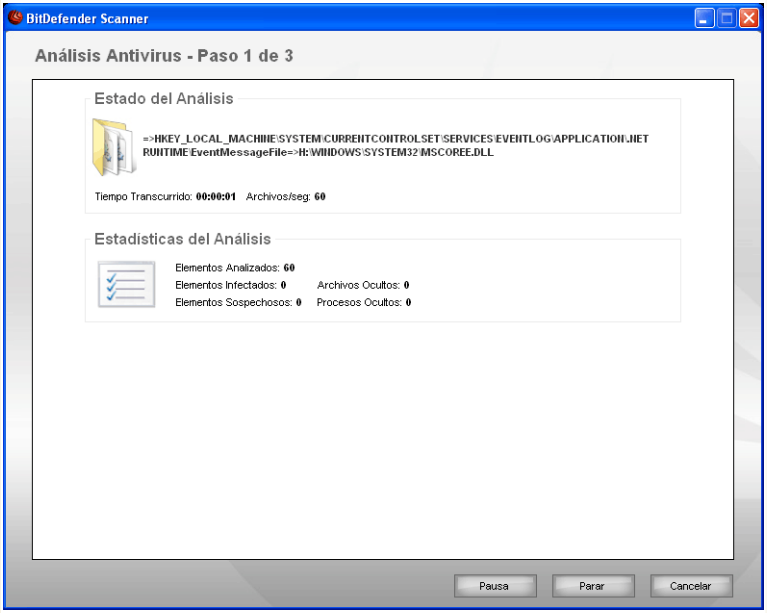
Desde las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso llevará un tiempo. Por ello, recomendamos ejecutar estas tareas con baja prioridad, o preferiblemente, cuando no utilice el equipo.

Cuando inicia un proceso de análisis bajo demanda, ya sea rápido o completo, aparecerá BitDefender Scanner.

Siga el proceso guiado de tres pasos para completar el proceso de análisis.

Paso 1/3 – Analizando

BitDefender analizará los objetos seleccionados.



Analizando

Puede ver el estado y las estadísticas del análisis (velocidad de análisis, número de archivos analizados / infectados / sospechosos / objetos ocultos y otros).

Nota
El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis.

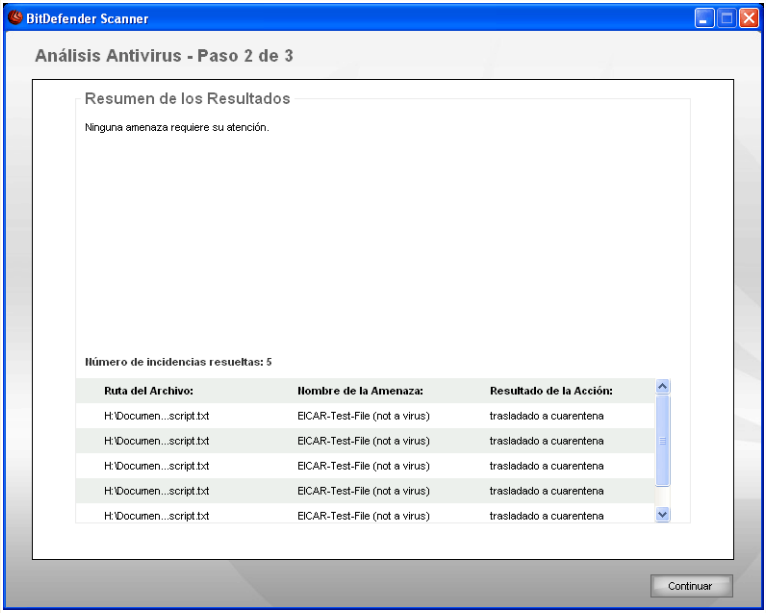
Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

Puede detener el análisis en cualquier momento, haciendo clic en botón **Parar**. Irá directamente al último paso del asistente.

Espere a que BitDefender finalice el análisis.

Paso 2/3 – Seleccionar Acciones

Cuando el análisis haya finalizado, aparecerá una nueva ventana dónde podrá ver los resultados del análisis.



Acciones

Puede ver el número de incidencias que afectan a su sistema.

Los objetos infectados se muestran agrupados en base al malware que los haya infectado. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todos los elementos cada grupo, o bien elegir una opción para cada uno de los elementos.

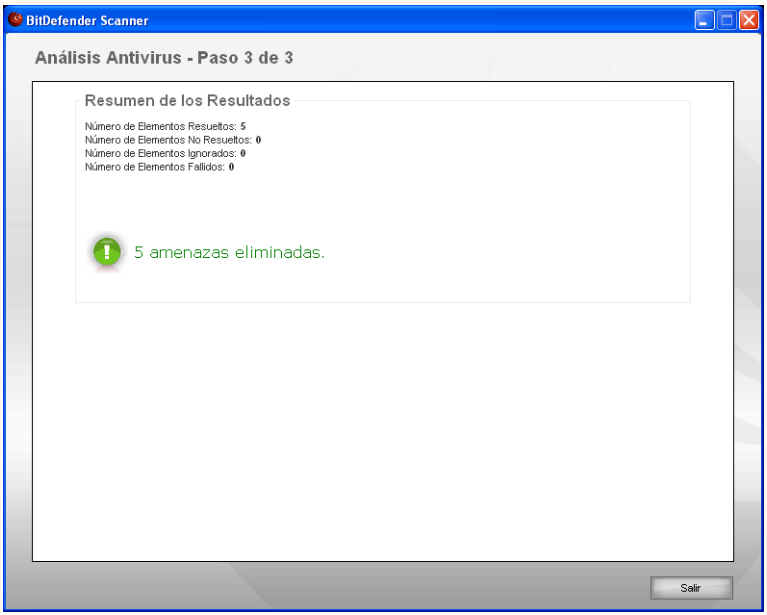
Pueden aparecer las siguientes opciones en el menú:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción sobre los archivos detectados.
Desinfectar	Desinfecta los archivos infectados.
Eliminar	Elimina los archivos detectados.
Hacer visible	Hace visible el objeto oculto.

Haga clic en **Continuar** para aplicar las acciones indicadas.

Paso 3/3 – Ver Resultados

Una vez BitDefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana.



Resumen

Puede ver el resumen de los resultados. El informe se guarda automáticamente en el apartado Informes de la ventana **Propiedades** de la tarea seleccionada.

Importante
En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección.

Haga clic en **Salir** para cerrar la ventana de resultados.

BitDefender No Ha Podido Reparar Algunas Incidencias

En la mayoría de casos, BitDefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, algunas incidencias no pueden repararse.

En estos casos, recomendamos contactar con el equipo de Soporte Técnico en www.bitdefender.es. Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

Elementos Protegidos con Contraseña Detectados por BitDefender

La categoría de elementos protegidos incluye dos tipos de elementos: archivos comprimidos e instaladores. Éstos no representan una amenaza real para la seguridad de su sistema, a no ser que contengan archivos infectados y sólo si estos archivos se ejecutan.

Para asegurarse que estos elementos están limpios:

- Si el elemento protegido con contraseña es un archivo comprimido que ha protegido usted mismo, extraiga los archivos que contiene y analícelos aparte. La manera más fácil de analizar estos elementos es hacer clic con el botón derecho y seleccione la opción **BitDefender Antivirus 2008** en el menú.
- Si el elemento protegido con contraseña es un instalador, asegúrese que la protección en tiempo real está activado antes de ejecutar el instalador. Si el instalador está infectado, BitDefender lo detectará y aislará la infección.

Si no desea que estos objetos sean detectados de nuevo por BitDefender, deberá añadirlos como excepciones del proceso de análisis. Para añadir excepciones, haga clic en **Opciones** para abrir la consola de opciones, y diríjase a **Antivirus > Excepciones**.

Nota
Para más información, por favor diríjase al apartado Objetos Excluidos del Análisis.

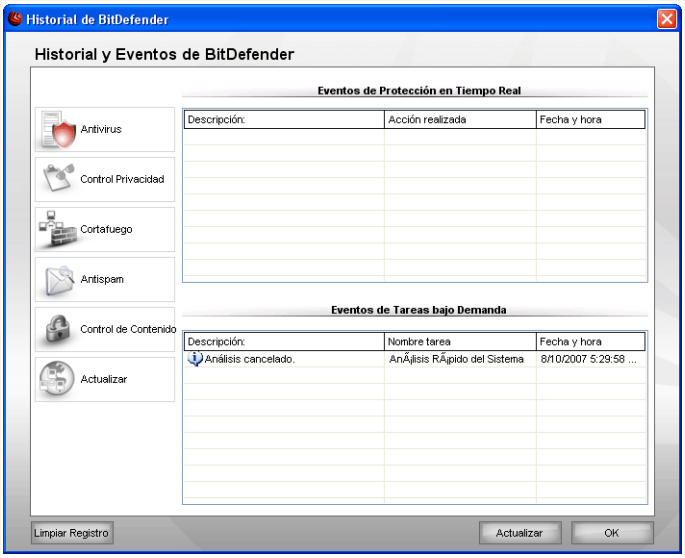
Objetos Sospechosos Detectados por BitDefender

Los archivos sospechosos son archivos detectados por el análisis heurístico como potencialmente infectados con malware, aunque su firma de virus todavía no se ha realizado.

Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de BitDefender. Haga clic en **Aceptar** para enviar estos archivos al Laboratorio de BitDefender para su posterior análisis.

5. Historial

El enlace del **Historial** situado en la parte inferior del Centro de Seguridad de BitDefender le conducirá a la ventana de Historial y Eventos de BitDefender. Esta ventana le ofrece una vista general de los eventos relacionados con la seguridad de su equipo. Por ejemplo, puede comprobar fácilmente si la actualización se ha realizado con éxito, si se ha encontrado malware en su equipo, si las tareas de copia se han realizado sin errores, etc.



Eventos

Para ayudarle a filtrar el historial y eventos BitDefender se le facilitan las siguientes categorías en la parte izquierda:

- **Antivirus**
- **Cortafuego**
- **Antispam**
- **Control de Privacidad**
- **Control de Contenido**
- **Actualización**

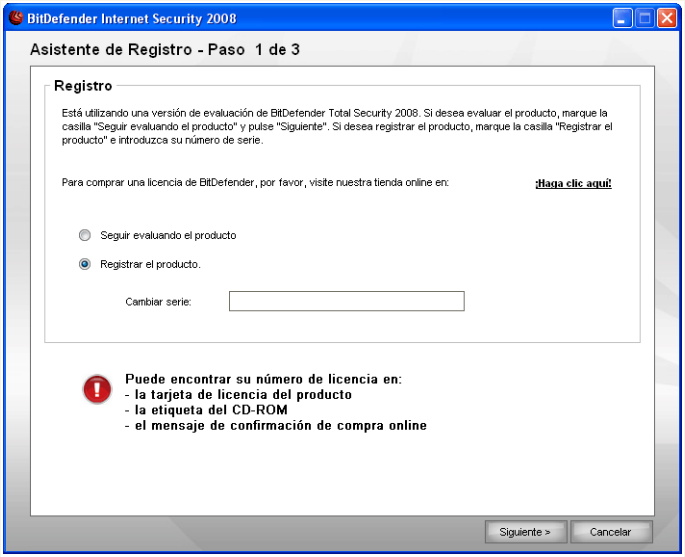
Dispone de una lista de eventos para cada categoría. Cada evento incluye la siguiente información: un descripción breve, la acción realizada por BitDefender, su resultado, y la fecha y hora en que se ha producido. Si desea más información sobre un evento en particular, haga clic encima del mismo.

Haga clic en **Limpiar Registro** si desea eliminar los registros antiguos, o en **Actualizar** para asegurarse que se visualizan los últimos registros.

6. Registro

BitDefender Internet Security 2008 viene con un periodo de evaluación de 30 días. Si desea registrar BitDefender Internet Security 2008, cambiar el número de licencia o crear una cuenta de BitDefender, haga clic en enlace **Registrar**, ubicado en la parte superior de la ventana de Centro de Seguridad. Aparecerá el asistente de registro aparecerá.

6.1. Paso 1/3 - Registrar BitDefender Internet Security 2008



Resumen

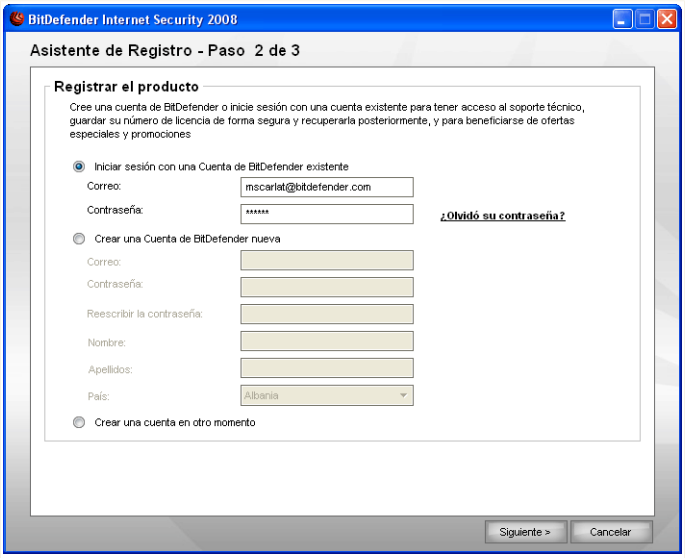
Si no tiene una licencia de BitDefender, haga clic en el enlace proporcionado para dirigirse a la tienda online de BitDefender y comprar un número de licencia.

Para registrar BitDefender Internet Security 2008, seleccione **Registrar el Producto** e introduzca el número de licencia en el campo **Cambiar serie**.

Si el periodo de evaluación no ha expirado y desea seguir evaluando el producto, seleccione la opción **Seguir evaluando el producto**.

Haga clic en **Siguiente** para continuar.

6.2. Paso 2/3 - Crear una cuenta de BitDefender



Resumen

No tengo una cuenta de BitDefender

Para poderse beneficiar del soporte técnico de BitDefender y de otros servicios gratuitos necesita crear una cuenta.

Nota
Si desea crear una cuenta en otro momento, seleccione la opción correspondiente.

Para crear una cuenta de BitDefender, Seleccione **Crear una nueva cuenta BitDefender** e introduzca la información solicitada. Los datos que introduzca aquí serán confidenciales.

- **E-mail** - introduzca su dirección de correo.
- **Contraseña** - introduzca una contraseña para su cuenta de BitDefender.

Nota
La contraseña debe contener 4 caracteres como mínimo.

- **Repetir contraseña** - introduzca de nuevo la contraseña especificada anteriormente.
- **Nombre** - introduzca su nombre.
- **Apellidos** - introduzca sus Apellidos.
- **País** - introduzca el país en el que reside.

Nota
Utilice la dirección indicada y contraseña para iniciar sesión en su cuenta http://myaccount.bitdefender.com.

Para crear una cuenta con éxito, primero debe activar su dirección de e-mail. Consulte la cuenta de correo indicada anteriormente y siga las instrucciones indicadas en el mensaje enviado por el servicio de registro de BitDefender.

Haga clic en **Siguiente** para continuar.

Ya tengo una cuenta de BitDefender

BitDefender detectará automáticamente si previamente ha registrado una cuenta de BitDefender en su equipo. En este caso, sólo tendrá que hacer clic en **Siguiente**.

Si ya tiene una cuenta activa, pero BitDefender no la detecta, seleccione **Iniciar sesión con una Cuenta de BitDefender existente** e introduzca la dirección de correo y la contraseña de su cuenta.

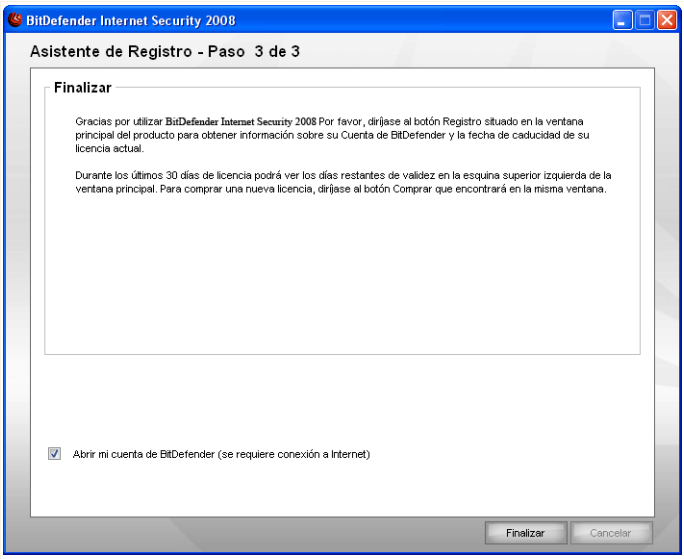
Nota

Si la contraseña indicada es incorrecta, se le volverá a solicitar cuandopulse en **Siguiente**. Haga clic en **Aceptar** para introducir de nuevo la contraseña opulse en **Cancelar** para salir del Asistente.

Si ha olvidado su contraseña haga clic en **¿Olvidó su contraseña?** y siga las instrucciones.

Haga clic en **Siguiente** para continuar.

6.3. Paso 3/3 - Registrar BitDefender Internet Security 2008



Resumen

Seleccione **Abrir mi cuenta de BitDefender** para entrar en su cuenta de BitDefender. Necesita estar conectado a Internet.

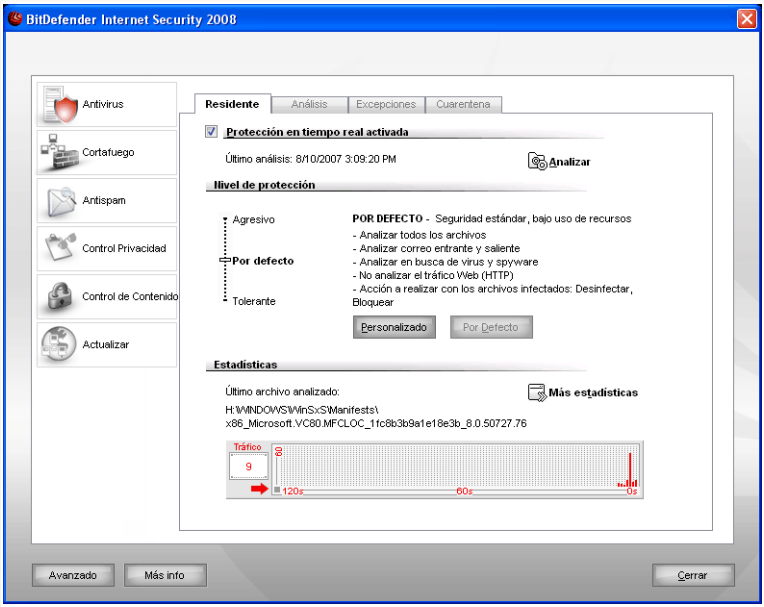
Haga clic en **Aceptar** para cerrar la ventana.

Administración Avanzada de Seguridad

7. Conseguir Ayuda

BitDefender Internet Security 2008 incluye una consola de configuración centralizada, que permite modificar las opciones avanzadas y la administración de BitDefender.

Para acceder a la configuración de la consola, haga clic en el enlace **Configuración**, situado en la parte inferior del Centro de Seguridad.



Consola de Configuración

La consola de configuración está organizada en diferentes módulos: **Antivirus**, **Cortafuego**, **Antispam**, **Control de Privacidad**, **Control de Contenido** y **Actualizar**. Esto le permite administrar fácilmente la configuración de BitDefender en función el tipo de incidencia de seguridad que desee abordar.

En el lado izquierdo de la consola de configuración puede ver el selector de módulos:

- Antivirus - en este apartado puede configurar el módulo **Antivirus**.
- Cortafuego - en este apartado puede configurar el módulo **Cortafuego**.

- Antispam - en este apartado puede configurar el módulo **Antispam**.
- Control Privacidad - en este apartado puede configurar el módulo **Control de Privacidad**.
- Control de Contenido - en este apartado puede configurar el módulo **Control de Contenido**.
- Actualización - en este apartado puede configurar el módulo **Actualización**.

En la parte inferior de la consola, encontrará el botón **Más info** que abre una página de ayuda contextual. Haga clic en este botón para encontrar más información en el momento en que necesite ayuda.

Si necesita más ayuda, haga clic en el bóton **Más info**, situado en la parte inferior de la ventana. La ayuda contextual contiene información detallada sobre el apartado en el que se encuentra.

7.1. Modificando la Configuración General

Para modificar la configuración general de BitDefender Internet Security 2008 haga clic en **Avanzado**. Aparecerá una nueva ventana.

Configuración General

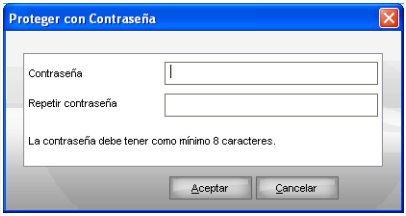
En este apartado puede configurar el comportamiento general de BitDefender. Por defecto, BitDefender se carga al inicio de Windows y sigue funcionando minimizado en la barra del sistema.

7.1.1. Configuración General

- **Activar protección por contraseña** - pemite introducir una contraseña para proteger la configuración de BitDefender.

  Nota
  Si no es el único usuario con permisos de administrador que utiliza este ordenador, es recomendable que proteja su configuración de BitDefender con una contraseña.

  Si selecciona esta opción, aparecerá la siguiente ventana:



Confirmar contraseña

  Introduzca la contraseña en el campo **Contraseña**, introdúzcala de nuevo en el campo **Repetir contraseña** y haga clic en **Aceptar**.

  Una vez definida la contraseña, se le solicitará introducirla para poder cambiar la configuración de BitDefender. Los otros administradores del sistema (en caso que existan) también deberán introducir la contraseña para poder cambiar la configuración de BitDefender.

  Si quiere que se le solicite la contraseña sólo cuando configura el Control de Contenido, debe marcar la opción **Introducir contraseña para el módulo Control de Contenido**. Por otro lado, si ha definido una contraseña sólo para el Control de Contenido y desmarca esta opción, se solicitará la respectiva contraseña al cambiar cualquier opción de BitDefender.

  Importante
  Si ha olvidado la contraseña tendrá que reparar el programa para poder cambiar la configuración de BitDefender.

- **Introducir contraseña para el módulo Control de Contenido** - si esta opción está activada y no se ha definido ninguna contraseña, se le solicitará introducirla al activar el Control de Contenido.

- **Mostrar Noticias de BitDefender (noticias relacionadas con la seguridad)** - muestra de vez en cuando noticias acerca de las epidemias de virus, enviadas desde los servidores de BitDefender.
- **Mostrar pop-ups (notas en pantalla)** - muestra pop-ups acerca del estado del producto.
- **Cargar BitDefender al iniciar Windows** - carga BitDefender automáticamente al iniciar el sistema. Recomendamos mantener esta opción seleccionada.
- **Activar barra de Actividad del Análisis** - activa/desactiva la Barra de Actividad del Análisis al iniciar Windows. Desmarque esta casilla si no desea que la Barra de Actividad se muestre más.

Nota
Esta opción sólo puede configurarse para la cuenta de usuario de Windows en uso.

- **Activar atajo de teclado para el Modo Trabajo** - permite activar / desactivar el Modo Trabajo utilizando una combinación de teclas. El atajo de teclado predeterminado es `Alt+G`.

  Para modificar el atajo de teclado, realice lo siguiente:

  1. Marque las teclas que desea utilizar entre las siguientes opciones: Control (`Ctrl`), Shift (`Shift`) o Alternate (`Alt`).
  2. En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

7.1.2. Configuración del Informe de Virus

- **Enviar informe de virus** - permite enviar a los Laboratorios BitDefender información acerca de los virus detectados en su equipo. Con esta información, nos ayuda a mantener un registro de las epidemias de virus.

  Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otra información, ni serán utilizados con fines comerciales. Los datos proporcionados incluirán únicamente el nombre del país y del virus, y serán utilizados exclusivamente para crear informes y estadísticas.
- **Activar la Detección de Epidemias** - envia informes acerca de las posibles epidemias de virus a los Laboratorios de BitDefender.

  Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otra información, y no serán empleados con fines comerciales. La información

enviada sólo contiene el posible virus y sólo será utilizada para detectar nuevos virus.

7.1.3. Importar/Exportar Configuración

Utilice los botones **Guardar Toda la Configuración** / **Cargar Toda la Configuración** para guardar / cargar la configuración de BitDefender a otro destino. De este modo, podrá utilizar la misma configuración después de reinstalar o reparar el producto BitDefender.

Importante
Sólo los usuarios con permisos de administración pueden guardar y cargar la configuración.

Para cargar la configuración por defecto, haga clic en **Restaurar Configuración Inicial**.

8. Antivirus

BitDefender protege a su equipo de todo tipo de malware (virus, troyanos, spyware, rootkits y otros).

Además del análisis clásico basado en las firmas de virus, BitDefender también realiza un análisis heurístico de los archivos a los que accede. El objetivo de este tipo de análisis es identificar nuevos virus basándose en ciertos patrones y algoritmos, antes de encontrar una firma de virus, aunque puede generar falsas alarmas. Al detectar un fichero de este tipo, se clasificará como sospechoso. En estos casos, le recomendamos enviar el fichero para que sea analizado en los laboratorios de BitDefender.

La protección que ofrece BitDefender está dividida en dos apartados:

- **Análisis al acceder** - impide que las amenazas de malware entren en su sistema. A este tipo de protección también se le llama protección en tiempo real, y analiza los archivos a medida que accede a los mismos. Por ejemplo, BitDefender analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.
- **Análisis bajo demanda** - permite detectar y eliminar malware que ya reside en su sistema. Se trata del clásico análisis antivirus iniciado por el usuario - usted selecciona la unidad, carpeta o archivo que BitDefender debe analizar, y BitDefender lo analizará cuando se lo indique. Las tareas de análisis le permiten crear rutinas de análisis personalizadas, que pueden planificarse para que se ejecuten regularmente.

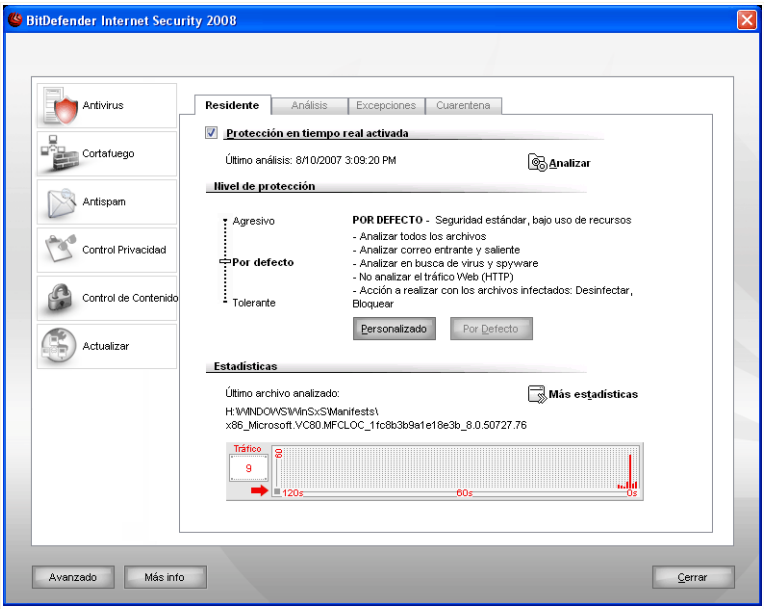
El apartado **Antivirus** de esta guía comprende los siguientes temas:

- Análisis en Tiempo Real
- Análisis Bajo Demanda
- Objetos Excluidos del Análisis
- Cuarantena

8.1. Análisis en Tiempo Real

El análisis al acceder, también conocido como protección en tiempo real, mantiene su ordenador a salvo de todo tipo de amenazas de malware, analizando todos los achivos a los que accede, los mensajes y las comunicaciones a través de aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger).

Para configurar y monitorizar la protección en tiempo real, haga clic en **Antivirus > Residente** en la consola de configuración. Aparecerá la siguiente pantalla:



Protección en Tiempo Real.

Importante
Para impedir que los virus infecten su ordenador manenga la **Protección en Tiempo Real** activada.

En la parte inferior de este apartado podrá ver las estadísticas sobre los archivos y mensajes analizados por la **Protección en Tiempo Real**. Haga clic en **Más estadisticas** si quiere ver una ventana con más explicaciones sobre las estadísticas.

Para iniciar un análisis rápido del sistema, haga clic en **Analizar**.

8.1.1. Configurando el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel adecuado de protección.

Hay 3 niveles de seguridad:

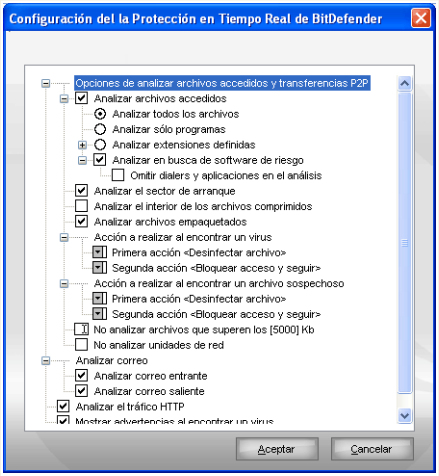
Nivel de Protección	Descripción
Tolerante	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. Los programas y mensajes entrantes se analizan sólo en busca de virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se detectan archivos infectados son las siguientes: desinfectar archivo/bloquear acceso.
Por Defecto	Ofrece seguridad estándar. El nivel de consumo de recursos es bajo. Todos los archivos y mensajes entrantes y salientes son analizados en busca de virus y spyware. Además del clásico análisis basado en firmas, también se utiliza el análisis heurístico. Las acciones que se realizan cuando se detectan archivos infectados son las siguientes: desinfectar archivo/bloquear acceso.
Agresivo	Ofrece seguridad de alta calidad. El nivel de consumo de recursos es moderado. Todos los archivos, mensajes entrantes y salientes y el tráfico de web se analizan en busca de virus y spyware. Además del clásico análisis basado en firmas, también se utiliza el análisis heurístico. Las acciones que se realizan cuando se detectan archivos infectados son las siguientes: desinfectar archivo/bloquear acceso.

Para aplicar la configuración predeterminada de la protección en tiempo real haga clic en **Por Defecto**.

8.1.2. Personalizando el Nivel de Protección

Los usuarios avanzados querrán aprovechar las opciones de análisis que BitDefender ofrece. El análisis puede configurarse para analizar sólo un tipo de extensiones definidas, para buscar amenazas específicas, o para omitir archivos comprimidos. Esta característica permite disminuir notablemente los tiempos de análisis y mejorar el rendimiento de su equipo durante un análisis.

Puede personalizar la **Protección en Tiempo Real** haciendo clic en **Personalizado**. Se le mostrará la siguiente ventana:



Configurar el Residente BitDefender

Las opciones de análisis están organizadas en forma de menú extensible, de manera similar a los de Windows. Haga clic en la casilla "+" para desplegar una opción o en "-" para cerrarla.

Nota

Observará que en ciertas opciones de análisis, aunque aparezca la casilla "+" no puede extenderse. Esto debido a que estas opciones no han sido seleccionadas. Sin embargo, si selecciona estas opciones, podrá abrirlas.

- **Analizar archivos accedidos y transferencias P2P** - analiza los ficheros a los que accede y las comunicaciones de mensajería instantánea (ICQ, NetMeeting,

Yahoo! Messenger, MSN Messenger). Más adelante podrá seleccionar el tipo de ficheros a analizar.

Opción		Descripción
Analizar archivos accedidos	**Analizar todos los archivos**	Se analizarán todos los archivos, independientemente de su tipo.
	Analizar sólo programas	Únicamente se analizarán los archivos con las siguientes extensiones: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` y `.nws`.
	Analizar extensiones definidas	Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ";".
	Analizar en busca de software de riesgo	Analizar en busca de software de riesgo. Los archivos detectados con este método se tratarán como archivos infectados. El software que incluya componentes de adware puede funcionar incorrectamente si esta opción está activada. Seleccione **Omitir dialers y aplicaciones en el análisis** si quiere excluir este tipo de archivos del análisis.
Analizar los sectores de arranque		Para analizar el sector de arranque del sistema.
Analizar el interior de los archivos comprimidos		Para analizar el contenido de los archivos comprimidos. Con esta opción activada su ordenador puede ralentizarse un poco.
Analizar archivos empaquetados		Para analizar todos los archivos empaquetados.

Opción		Descripción
Primera acción		En el menú desplegable, seleccione la primera acción que desea realizar al encontrar archivos infectados o sospechosos.
	Bloquear acceso y seguir	Si se detecta un fichero infectado, se denegará el acceso al mismo.
	Desinfectar archivo	Desinfecta los archivos infectados.
	Eliminar archivo	Elimina los ficheros infectados inmediatamente y sin previa advertencia.
	Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena.
Segunda acción		En el menú desplegable, seleccione la segunda acción que desea realizar al encontrar archivos infectados o sospechosos, en caso que falle la primera acción.
	Bloquear acceso y seguir	Si se detecta un fichero infectado, se denegará el acceso al mismo.
	Eliminar archivo	Elimina los ficheros infectados inmediatamente y sin previa advertencia.
	Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena.
No analizar archivos que superen los [x] Kb		Introduzca el tamaño máximo de los archivos a analizar. Si el tamaño es 0 Kb, se analizarán todos los archivos, independientemente de su tamaño.
No analizar unidades de red		Si esta opción está activada, BitDefender no analizará los recursos compartidos de la red, consiguiendo un acceso a la red más rápido. Recomendamos activar esta opción sólo si la red a la que pertenece está protegida por una solución antivirus.

- **Analizar correo** - analiza el correo electrónico.

  Dispone de las siguientes opciones:

Opción	Descripción
Analizar correo entrante	Analiza todos los correos entrantes.
Analizar correo saliente	Analiza todos los correos salientes.

- **Analizar el tráfico HTTP** - analiza el tráfico HTTP.
- **Mostrar advertencias al encontrar un virus** - mostrará una ventana de advertencia al detectarse un virus en un fichero o correo electrónico.

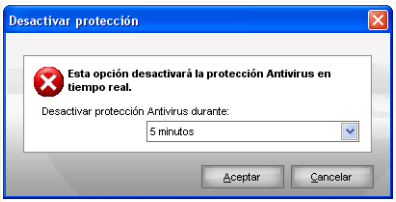
  Al detectarse un archivo infectado aparecerá una la alerta que contiene el nombre del virus, la ubicación, la acción realizada por BitDefender y un enlace a la página web de BitDefender, donde podrá encontrar más información acerca del virus. En los mensajes infectados se mostrará también información sobre el remitente y el destinatario del correo.

  Si el programa detecta ficheros sospechosos, puede iniciar el asistente desde la ventana de alertas para enviar el fichero al Laboratorio BitDefender. Una vez analizado, puede recibir información a través de la dirección de e-mail introducida en el asistente.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

8.1.3. Desactivando la Protección en Tiempo Real

Si decide desactivar la protección en tiempo real, aparecerá una ventana de advertencia.



Desactivar Protección en Tiempo Real

Para confirmar su elección, deberá indicar durante cuanto tiempo desea desactivar la protección. Puede desactivar la protección durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

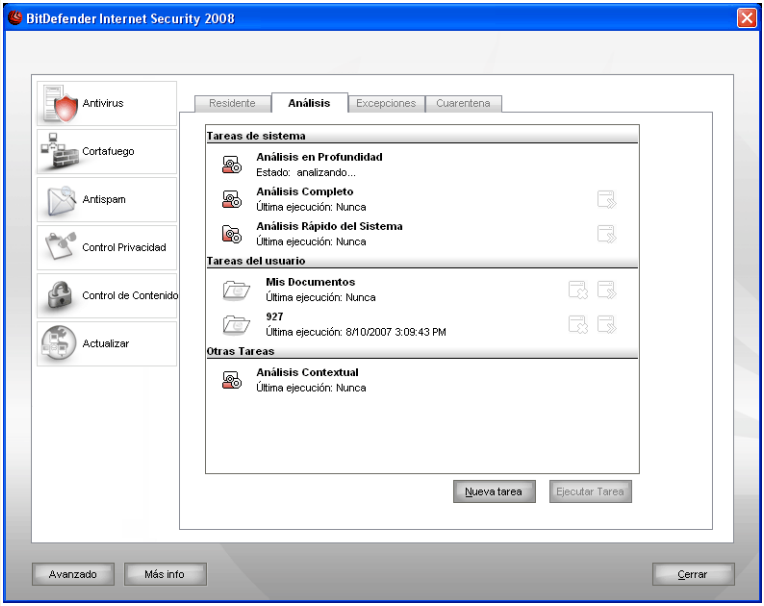
Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Mientras la protección esté desactivada, no tendrá protección contra amenazas de malware.

8.2. Análisis Bajo Demanda

El objetivo principal de BitDefender es mantener su ordenador libre de virus. Los primeros dos pasos para lograr tal meta consisten en impedir el acceso de nuevos virus a su sistema y en analizar sus mensajes de correo y cualquier fichero descargado o copiado en su PC.

Sin embargo, queda un riesgo: que algún virus haya entrado al sistema antes de instalar BitDefender. Por esta razón recomendamos analizar su ordenador inmediatamente después de instalar BitDefender. Además, también es una buena práctica realizar análisis periódicamente.

Para configurar e iniciar un análisis bajo demanda, haga clic en **Antivirus > Analisis** en la consola de configuración. Aparecerá la siguiente pantalla:



Tareas de Análisis

El análisis bajo demanda se basa en tareas de análisis. Estas tareas indican las opciones y los objetivos a analizar. Puede analizar el ordenador cuando desee ejecutando alguna de las tareas predeterminadas o creando sus tareas propias. También puede planificar las tareas para que se realicen en momentos en que el sistema esté inactivo y no interfieran con su trabajo.

8.2.1. Tareas de Análisis

BitDefender incluye diferentes tareas predeterminadas que cubren las necesidades de seguridad más comunes. Pero también puede crear sus propias tareas de análisis personalizadas.

Cada tarea tiene su propia ventana de **Propiedades** que le permiten configurar la tarea y ver los resultados del análisis. Para más información, consulte el apartado "*Configurando una Tarea de Análisis*" (p. 57).

Existen 3 tipos de tareas de análisis:

- **Tareas de Sistema** - contiene una lista de tareas de sistema predeterminadas. Las siguientes tareas están disponibles:

Tarea Predeterminada	Descripción
Análisis en Profundidad	Analiza el sistema por completo. En la configuración por defecto, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración por defecto, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Rápido del Sistema	Analiza las capetas `Windows`, `Archivos de Programa` y `All Users`. En la configuración por defecto, analiza en busca de cualquier tipo de malware, excepto rootkits, pero no analiza la memoria, el registro ni las cookies.

Nota
Desde las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso llevará un tiempo. Por ello, recomendamos ejecutar estas tareas con baja prioridad, o preferiblemente, cuando no utilice el equipo.

- **Tareas del Usuario** - contiene las tareas definidas por el usuario.

  Existe una tarea llamada `Mis Documentos`. Utilice esta tarea para analizar las carpetas del usuario que está utilizando: `Mis Documentos`, `Escritorio` e `Inicio`. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.
- **Otras tareas** - contiene una lista de otras tareas de análisis. Estas tareas de análisis se refieren a tipos de análisis alternativos que no se pueden ejecutar desde esta ventana. Sólo puede modificar sus opciones o ver los informes de análisis.

Hay tres botones disponibles en la parte derecha de cada tarea:

- **Programador** - indica que la tarea está programada para iniciarse en otro momento. Haga clic en este botón para abrir la ventana de **Propiedades**, pestaña Programador, donde podrá ver la planificación de la tarea y modificarla.

- **Eliminar** - elimina la tarea seleccionada.

Nota
No disponible para tareas de sistema. No se puede eliminar una tarea de sistema.

- **Analizar** - ejecuta la tarea seleccionada, iniciando un análisis inmediato.

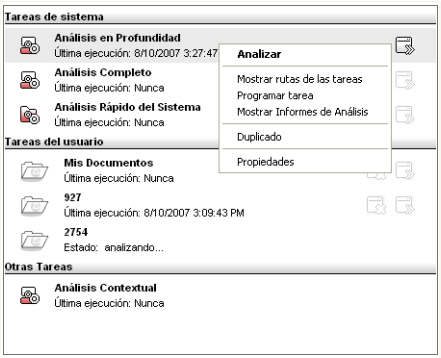
A la izquierda de cada tarea verá el botón de **Propiedades**, que le permite configurar la tarea y ver los resultados del análisis.

8.2.2. Utilizando el Menú Rápido

Dispone de un menú rápido para cada tarea. Haga clic con el botón derecho sobre la tarea seleccionada para abrirlo.

El menú rápido dispone de los siguientes comandos:

- **Analizar** - ejecuta la tarea seleccionada, iniciando inmediatamente el análisis.
- **Cambiar el Objeto del Análisis** - abre la ventana **Cambiar el objeto de análisis**, pestaña Ruta, dónde podrá cambiar el objetivo del análisis de la tarea seleccionada.



Menú Rápido

Nota
En las tareas del sistema, esta opción será reemplazada por **Mostrar rutas de las tareas**, donde podrá ver las rutas que se analizarán.

- **Programador** - abre la ventana de **Propiedades**, pestaña Programador, dónde podrá cambiar la planificación de la tarea seleccionada.
- **Mostrar Informes de Análisis** - abre la ventana de **Propiedades**, pestaña Informes, dónde podrá ver los informes generados tras la realización del análisis.
- **Duplicar** - duplica la tarea seleccionada.

Nota
Esta opción es muy útil para crear nuevas tareas, ya que puede modificar las opciones de la tarea duplicada.

- **Eliminar** - elimina la tarea seleccionada.

Nota
No disponible para tareas de sistema. No se puede eliminar una tarea de sistema.

- **Propiedades** - abre la ventana de **Propiedades**, pestaña General, dónde podrá cambiar las opciones de la tarea seleccionada.

Nota
Debido a la particular naturaleza de las **Otras Tareas**, sólo estarán disponibles las opciones **Propiedades** y **Ver Informes de Análisis**.

8.2.3. Creando tareas de análisis

Para crear una tarea de análisis, utilice uno de estos métodos:

- Duplicar una regla existente, cambie su nombre y haga las modificaciones necesarias en la ventana Propiedades.
- Haga clic en **Nueva tarea** para crear una nueva tarea y configurarla.

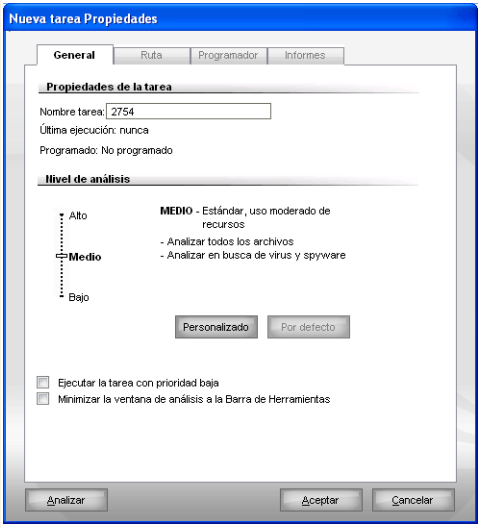
8.2.4. Configurando una Tarea de Análisis

Cada tarea de análisis tiene su ventana de **Propiedades**, donde puede configurar las opciones de análisis, el objeto de análisis, programar la tarea o ver los informes. Para abrir esta ventana haga clic en el botón **Abrir**, situado a la derecha de la tarea (o haga doble clic sobre la tarea y clic en **Abrir**).

Nota
Para más detalles acerca del módulo **Informes**, consulte "*Viendo los Informes del Análisis*" (p. 75).

Configurando las Opciones de Análisis

Para configurar las opciones de análisis de una tarea de análisis, haga clic derecho y seleccione **Propiedades**. Aparecerá la siguiente pantalla:



General

Aquí puede ver información acerca de la tarea (nombre, última ejecución y próxima ejecución programada) y configurar las opciones de análisis.

Seleccionando el nivel de Análisis

Puede configurar fácilmente las opciones de análisis a través del deslizador. Arrastre el deslizador a lo largo de la escala para elegir el nivel de análisis deseado.

Hay 3 niveles de análisis:

Nivel de Protección	*Descripción*
Bajo	Ofrece un nivel razonable de eficacia de detección. El nivel del consumo de recursos es bajo. Sólo los programas se analizan en busca de virus. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.

Nivel de Protección	Descripción
Medio	Ofrece un buen nivel de eficacia de detección. El nivel del consumo de recursos es moderado. Todos los archivos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.
Alto	Ofrece un alto nivel de eficacia de detección. El nivel del consumo de recursos es alto. Todos los archivos comprimidos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.

También hay disponibles una serie de opciones generales para el proceso de análisis:

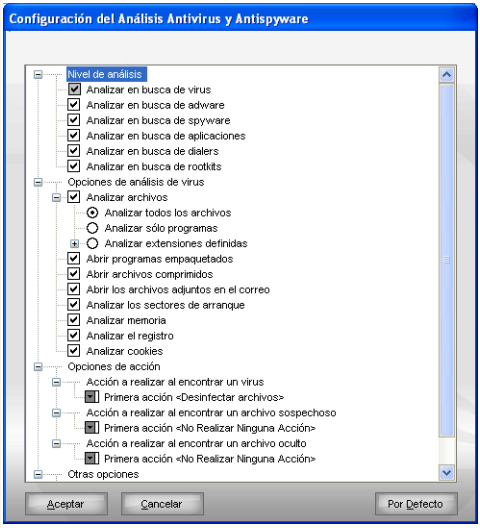
Opción	Descripción
Ejecutar el análisis con prioridad baja	Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
Minimizar ventana de análisis a la barra de tareas	Minimiza la ventana de análisis a la barra de tareas. Para visualizar la ventana haga doble clic en el icono.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Optimizando el nivel de análisis

Los usuarios avanzados querrán aprovechar las opciones de análisis que BitDefender ofrece. El análisis puede configurarse para analizar sólo un tipo de extensiones definidas, para buscar amenazas específicas, o para omitir archivos comprimidos. Esta característica permite disminuir notablemente los tiempos de análisis y mejorar el rendimiento de su equipo durante un análisis.

Haga clic en **Personalizado** para configurar sus propias opciones de análisis. Aparecerá una nueva ventana.



Opciones de análisis

Las opciones de análisis están organizadas en forma de menú extensible, de manera similar a los de Windows. Haga clic en la casilla "+" para desplegar una opción o en "-" para cerrarla.

Las opciones de análisis se agrupan en cuatro categorías:

- **Nivel de Análisis**
- **Opciones de análisis de virus**
- **Opciones de acción**
- **Otras opciones**

- Seleccione el tipo de malware que desea analizar con BitDefender y las opciones deseadas desde la categoría **Nivel de Análisis**.

  Dispone de las siguientes opciones:

Opción	*Descripción*
Analizar en busca de virus	Analizar en busca de virus conocidos.

Opción	Descripción
	BitDefender detecta también cuerpos de virus incompletos, eliminando así cualquier posible amenaza que pueda afectar la seguridad de su sistema.
Analizar en busca de adware	Analiza en busca de adware. Estos ficheros se tratarán como ficheros infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada.
Analizar en busca de spyware	Analiza en busca de spyware. Estos ficheros se tratarán como ficheros infectados.
Analizar en busca de aplicaciones	Analizar en busca de aplicaciones (`.exe` y `.dll`).
Analizar en busca de dialers	Analiza en busca de dialers de números de alta tarificación. Estos ficheros se tratarán como fuesen ficheros infectados. El software que incluya componentes dialer puede dejar de funcionar si esta opción está activada.
Analizar en busca de Rootkits	Analizar en busca de objetos ocultos (ficheros y procesos), generalmente denominados rootkits.

- Especifica el tipo de los objetos a analizar (archivos comprimidos, mensajes de correo electrónico, etc.) y otras opciones. Esto se hace a través de la selección de ciertas opciones desde la categoría **Opciones de análisis de virus**.

  Dispone de las siguientes opciones:

Opción		Descripción
Analizar archivos	**Analizar todos los archivos**	Se analizarán todos los archivos, independientemente de su tipo.
	Analizar sólo programas	Para analizar sólo archivos con las siguientes extensiones: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`;

Opción		Descripción
		chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml and nws.
	Analizar extensiones definidas	Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ";".
Abrir programas empaquetados		Para analizar el interior de los archivos empaquetados.
Abrir archivos comprimidos		Para analizar el contenido de los archivos comprimidos.
Abrir los archivos comprimidos adjuntos en el correo		Para analizar el interior de los archivos comprimidos del correo electrónico.
Analizar los sectores de arranque		Para analizar el sector de arranque del sistema.
Analizar Memoria		Analiza la memoria en busca de virus y otros tipos de malware.
Analizar el registro		Analiza las entradas del registro.
Analizar cookies		Analiza los archivos de las cookies.

- Indique las acciones a realizar sobre los archivos infectados, sospechosos u ocultos detectados, en la categoría **Opciones de acción**. Puede especificar una acción diferente para cada categoría.
  - Seleccione la acción a realizar cuando se detecte un archivo infectado. Dispone de las siguientes opciones:

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los ficheros infectados. Estos ficheros aparecerán en el informe de análisis.
Desinfectar archivos	Desinfecta los archivos infectados.
Eliminar archivos	Elimina los ficheros infectados inmediatamente y sin previa advertencia.
Mover archivos a la Cuarentena	Para trasladar los archivos infectados a la cuarentena.

- Seleccione la acción que desea que se realice al encontrar archivos sospechosos. Dispone de las siguientes opciones:

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los ficheros sospechosos. Estos ficheros aparecerán en el informe de análisis.
Eliminar archivos	Borra los ficheros sospechosos inmediatamente y sin previa advertencia.
Mover archivos a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena.

Nota
Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de BitDefender.

- Seleccione la acción a realizar cuando se detecten objetos ocultos (rootkits). Dispone de las siguientes opciones:

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los ficheros ocultos. Estos ficheros aparecerán en el informe de análisis.
Mover archivos a la Cuarentena	Trasladar los archivos infectados a la cuarentena.
Hacer visible	Muestre los ficheros ocultos para que Usted pueda verlos.

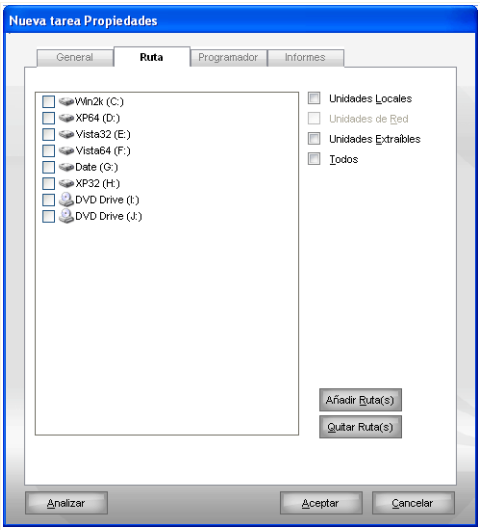
Nota
Si usted elige a ignorar los ficheros infectados o la acción elegida fracasa, tendrá que elegir una nueva acción en el asistente de análisis.

- Una vez finalizado el proceso de análisis se solicitará el envío de los ficheros sospechosos al laboratorio BitDefender. Marque la opción **Enviar archivos sospechosos al Laboratorio BitDefender** desde la categoría **Otras opciones**.

Si hace clic en **Por defecto** cargará la configuración por defecto. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Indicando el Objetivo del Análisis

Para definir el objetivo de análisis de una tarea, haga clic derecho sobre la tarea y seleccione **Cambiar el Objeto de Análisis**. Aparecerá la siguiente pantalla:



Objetivo del Análisis

Puede ver la lista de unidades locales, de red o extraibles, así como las carpetas y los ficheros añadidos anteriormente si existen. Todos los elementos seleccionados serán analizados cuando ejecute la tarea.

Este apartado contiene los siguientes botones:

- **Añadir archivo(s)** - abre una ventana de exploración desde la que podrá seleccionar los archivos o carpetas que desea analizar.

> ***Nota***
> También puede arrastrar y soltar ficheros y carpetas para añadirlos a la lista.

- **Añadir Ruta(s)** - elimina el archivo o carpeta seleccionado de la lista de objetos a analizar.

Nota
Sólo los ficheros y carpetas añadidos posteriormente se podrán eliminar, pero no aquellos "vistos" automáticamente por BitDefender.

Además de los botones citados anteriormente, también hay algunas opciones que le permiten seleccionar ubicaciones de análisis rápidamente.

- **Unidades locales** - para analizar las particiones locales.
- **Unidades de red** - para analizar las particiones de red.
- **Unidades extraíbles** - para analizar las unidades extraíbles (CD-ROM, disqueteras).
- **Todas las unidades** - para analizar todas las particiones, independientemente si son locales, de red o extraíbles.

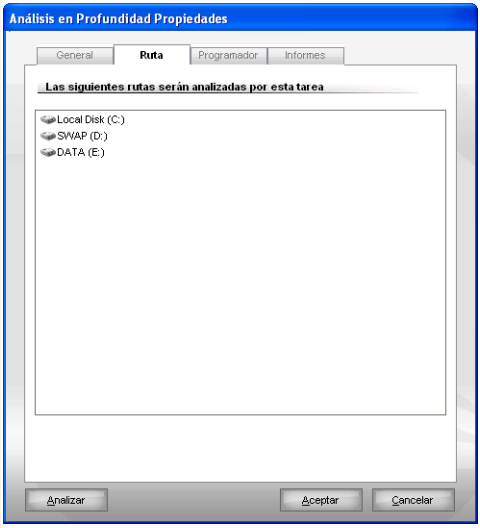
Nota
Si desea analizar todo el sistema en busca de virus, seleccione la casilla correspondiente a **Todas las unidades**.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Visualizando los el Objeto de Análisis de las Tareas del Sistema

No puede modificar los objetos de análisis de las tareas **Tareas del Sistema**. Sólo podrá ver su objeto de análisis.

Para definir el objetivo de análisis de una tarea del sistema, haga clic derecho sobre la tarea y seleccione **Mostrar rutas de las tareas**. Por ejemplo, en la tarea **Análisis Completo**, aparecerá la siguiente ventana:



Objetos de Análisis del Análisis Completo

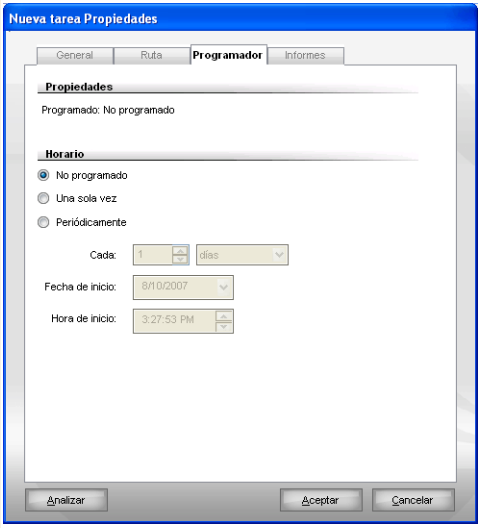
Las tareas **Análisis Completo** y **Análisis en Profundidad** analizarán todas las unidades locales, mientras que la tarea **Análisis Rápido del Sistema** sólo analizará las carpetas `Windows` y `Archivos de Programa`.

Haga clic en **Aceptar** para cerrar la ventana. Para iniciar la tarea, haga clic en **Analizar**.

Programando Tareas de Análisis

Si realiza un análisis complejo, el proceso de análisis llevará bastante tiempo, y funcionará mejor si se cierran todos los otros programas. Por esta razón es aconsejable que programe este tipo de tareas con antelación, para que se inicien en aquellos momentos en el que no utilice el ordenador y éste se encuentre inactivo.

Para ver o modificar la planificación de una tarea, haga clic con el botón derecho y seleccione **Programador**. Aparecerá la siguiente pantalla:



Programador

Puede ver las tareas programadas.

Al programar una tarea, debe seleccionar una de las siguientes opciones:

- **No Programado** - inicia la tarea sólo cuando el usuario lo solicita.
- **Una sola vez** - inicia el análisis sólo una vez, en determinado momento. Indique la fecha y hora de inicio en los campos **Fecha y hora de inicio**.
- **Periódicamente** - inicia un análisis periódicamente, en una hora determinada, y cada cierto intervalo de tiempo (horas, días, semanas, meses, años) empezando por una fecha y hora en concreto.

  Si quiere repetir el análisis cada cierto tiempo, seleccione la casilla **Periódicamente** e indique en **Cada** el número de minutos/horas/días/semanas/meses/años cada cuanto quiere repetir el proceso. También puede indicar la fecha y hora de inicio en los campos **Fecha y hora de inicio**.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

8.2.5. Analizando Objetos

Antes de iniciar el proceso de análisis debe asegurarse de que BitDefender tiene actualizadas las firmas de malware. Analizar su equipo con firmas antiguas puede impedir la detección de nuevo malware. Para comprobar cuando se realizó la última actualización, haga clic en **Actualizar > Actualizar** en la consola de configuración.

Nota

Para hacer un análisis completo de su sistema con BitDefender es necesario cerrar todos los programas abiertos. Especialmente, es importante cerrar su cliente de correo electrónico (por ejemplo: Outlook, Outlook Express o Eudora).

Métodos de Análisis

BitDefender le ofrece cuatro tipo de análisis bajo demanda:

- Análisis Inmediato - ejecuta una de las tareas de análisis del sistema o definidas por el usuario.
- Análisis Contextual - haga clic con el botón derecho en el fichero o carpeta que desee analizar y seleccione la opción BitDefender Antivirus 2008.
- Análisis Arrastrar y Soltar - arrastre y suelte un archivo o la carpeta sobre la Barra de Actividad de Análisis.
- Análisis Manual - utilice el Análisis Manual de BitDefender para seleccionar directamente los archivos y carpetas a analizar.

Análisis Inmediato

Para analizar su sistema o parte del mismo, puede usar las tareas de análisis predeterminadas o crear sus propias tareas de análisis. A esto se le llama análisis inmediado.

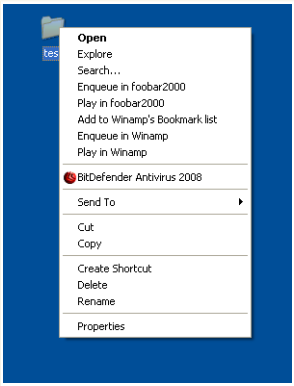
Para iniciar una tarea de análisis, utilice uno de los siguientes métodos:

- haga doble clic en la tarea de análisis que desee.
- haga clic en el botón **Analizar** correspondiente a la tarea.
- seleccione la tarea y haga clic en **Ejecutar Tarea**

Aparecerá BitDefender Scanner y se iniciará el análisis. Para más información, por favor, consulte el capítulo "*BitDefender Scanner*" (p. 70).

Análisis Contextual

Para analizar un archivo o carpeta sin tener que configurar una nueva tarea, puede utilizar el menú contextual. A esto se le llama análisis contextual.



Análisis contextual

Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **BitDefender Antivirus 2008**.

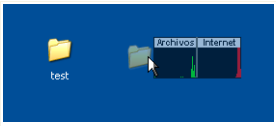
Aparecerá BitDefender Scanner y se iniciará el análisis. Para más información, por favor, consulte el capítulo "*BitDefender Scanner*" (p. 70).

Puede modificar las opciones del análisis o ver los informes en la ventana **Propiedades** de la tarea **Análisis del Menú Contextual**.

Análisis al Arrastrar y Soltar

Arrastre el archivo o la carpeta que desea analizar y suéltelo sobre la **Barra de Actividad del Análisis**, tal y como se puede ver en las siguientes imágenes.

Arrastrar el fichero



Soltar el fichero

Aparecerá BitDefender Scanner y se iniciará el análisis. Para más información, por favor, consulte el capítulo "*BitDefender Scanner*" (p. 70).

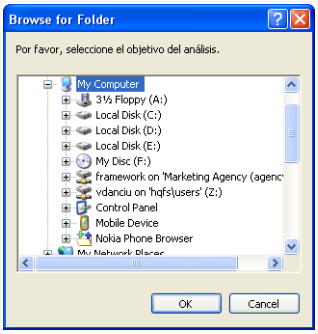
Análisis Manual

El análisis manual consiste en seleccionar directamente los objetos a analizar con la opción de Análisis Manual de BitDefender desde la carpeta de BitDefender en el menú Inicio.

Nota
El análisis manual es muy útil, y puede utilizarse cuando inicie Windows en modo seguro.

Para seleccionar el objeto a analizar, siga estos pasos en el menú Inicio: **Inicio** → **Programas** → **BitDefender 2008** → **Análisis Manual de BitDefender** .

Aparecerá la siguiente pantalla:



Análisis Manual

Seleccione el objeto que desea analizar y haga clic en **Aceptar**.

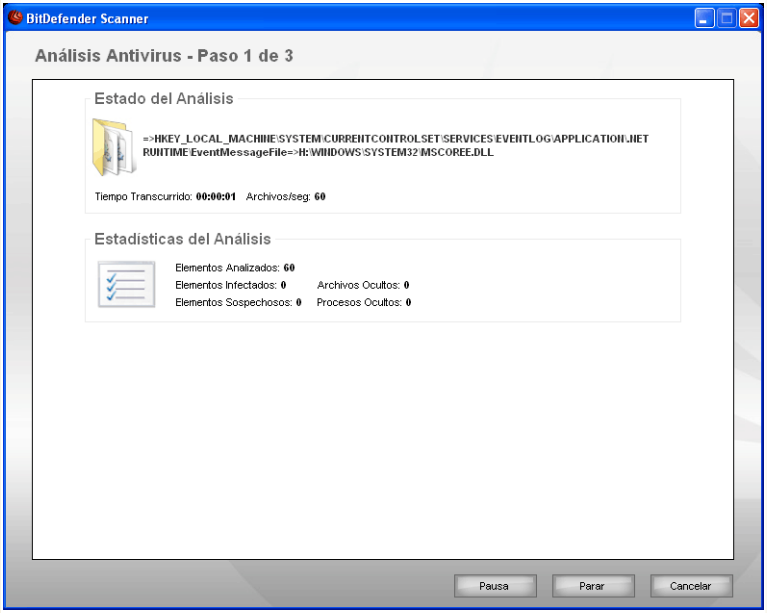
Aparecerá BitDefender Scanner y se iniciará el análisis. Para más información, por favor, consulte el capítulo "*BitDefender Scanner*" (p. 70).

BitDefender Scanner

Cuando inicie un proceso de análisis bajo demanda, aparecerá BitDefender Scanner. Siga el proceso guiado de tres pasos para completar el proceso de análisis.

Paso 1/3 – Analizando

BitDefender analizará los objetos seleccionados.



Analizando

Puede ver el estado y las estadísticas del análisis (velocidad de análisis, número de archivos analizados / infectados / sospechosos / objetos ocultos y otros).

Nota
El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis.

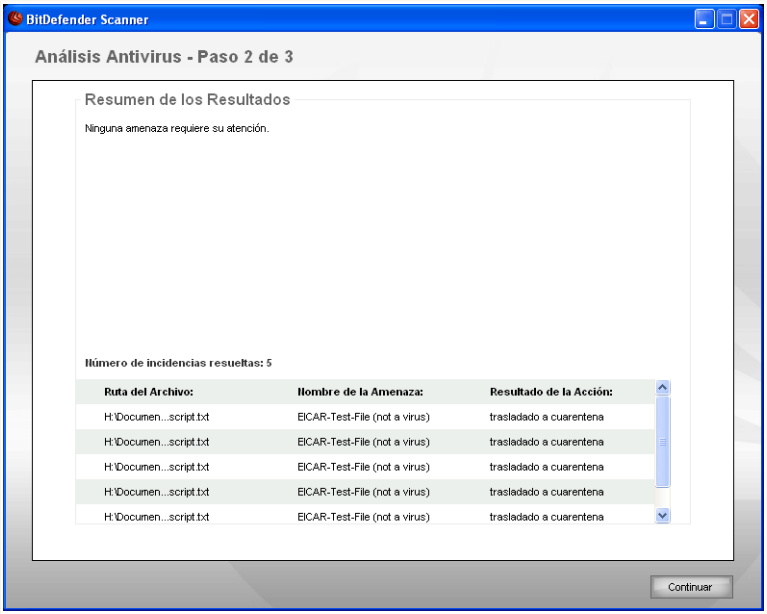
Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

Puede detener el análisis en cualquier momento, haciendo clic en botón **Parar**. Irá directamente al último paso del asistente.

Espere a que BitDefender finalice el análisis.

Paso 2/3 – Seleccionar Acciones

Cuando el análisis haya finalizado, aparecerá una nueva ventana dónde podrá ver los resultados del análisis.



Acciones

Puede ver el número de incidencias que afectan a su sistema.

Los objetos infectados se muestran agrupados en base al malware que los haya infectado. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todos los elementos cada grupo, o bien elegir una opción para cada uno de los elementos.

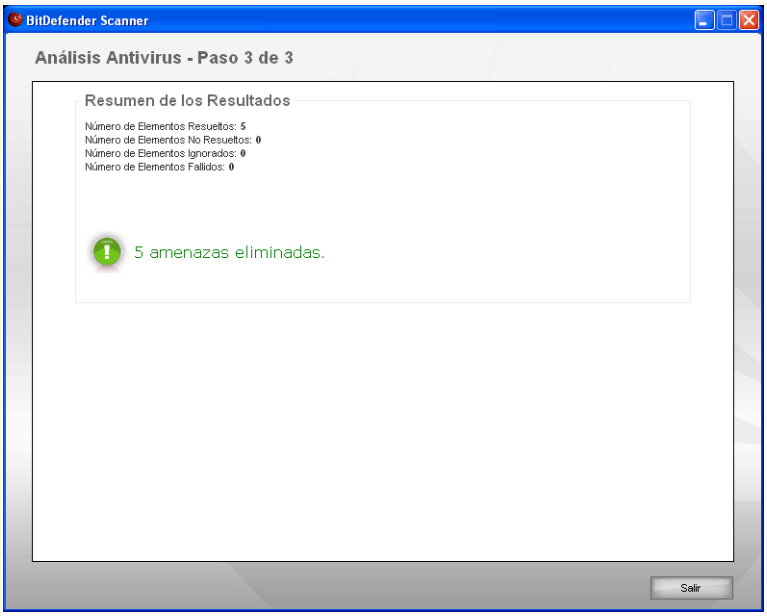
Pueden aparecer las siguientes opciones en el menú:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción sobre los archivos detectados.
Desinfectar	Desinfecta los archivos infectados.
Eliminar	Elimina los archivos detectados.
Hacer visible	Hace visible el objeto oculto.

Haga clic en **Continuar** para aplicar las acciones indicadas.

Paso 3/3 – Ver Resultados

Una vez BitDefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana.



Resumen

Puede ver el resumen de los resultados. El informe se guarda automáticamente en el apartado Informes de la ventana **Propiedades** de la tarea seleccionada.

Importante
En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección.

Haga clic en **Salir** para cerrar la ventana de resultados.

BitDefender No Ha Podido Reparar Algunas Incidencias

En la mayoría de casos, BitDefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, algunas incidencias no pueden repararse.

En estos casos, recomendamos contactar con el equipo de Soporte Técnico en www.bitdefender.es. Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

Elementos Protegidos con Contraseña Detectados por BitDefender

La categoría de elementos protegidos incluye dos tipos de elementos: archivos comprimidos e instaladores. Éstos no representan una amenaza real para la seguridad de su sistema, a no ser que contengan archivos infectados y sólo si estos archivos se ejecutan.

Para asegurarse que estos elementos están limpios:

- Si el elemento protegido con contraseña es un archivo comprimido que ha protegido usted mismo, extraiga los archivos que contiene y analícelos aparte. La manera más fácil de analizar estos elementos es hacer clic con el botón derecho y seleccione la opción **BitDefender Antivirus 2008** en el menú.
- Si el elemento protegido con contraseña es un instalador, asegúrese que la protección en tiempo real está activado antes de ejecutar el instalador. Si el instalador está infectado, BitDefender lo detectará y aislará la infección.

Si no desea que estos objetos sean detectados de nuevo por BitDefender, deberá añadirlos como excepciones del proceso de análisis. Para añadir excepciones, haga clic en **Opciones** para abrir la consola de opciones, y diríjase a **Antivirus > Excepciones**.

Nota
Para más información, por favor diríjase al apartado Objetos Excluidos del Análisis.

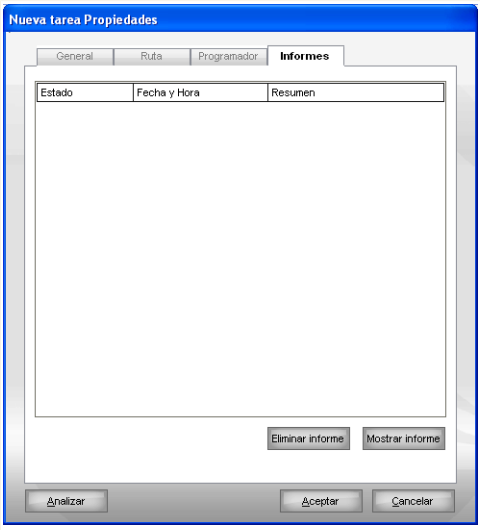
Objetos Sospechosos Detectados por BitDefender

Los archivos sospechosos son archivos detectados por el análisis heurístico como potencialmente infectados con malware, aunque su firma de virus todavía no se ha realizado.

Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de BitDefender. Haga clic en **Aceptar** para enviar estos archivos al Laboratorio de BitDefender para su posterior análisis.

8.2.6. Viendo los Informes del Análisis

Para ver los resultados del análisis al finalizar una tarea, haga clic derecho sobre la tarea y seleccione **Mostrar Informes de Análisis**. Aparecerá la siguiente pantalla:



Informes del análisis

Aquí puede ver los archivos de informe generados cada vez que ejecuta la tarea.

Cada archivo incluye información sobre su estado (infectado/desinfectado), la fecha y hora en que se realizó el análisis y un resumen de los resultados.

Hay dos botones disponibles:

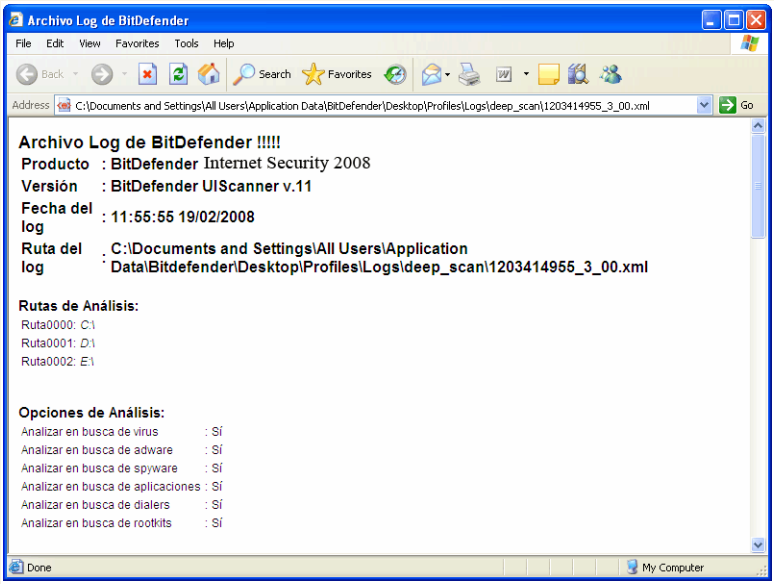
- **Eliminar informe** - para eliminar el archivo de informe seleccionado.
- **Mostrar informe** - para ver el informe seleccionado. El informe del análisis se abrirá en su navegador predeterminado.

Nota
Para ver o eliminar un fichero también pueder hacer clic con el botón derecho encima del fichero, y seleccionar la opción correspondiente en el menú rápido.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Ejemplo de Informe de Análisis

La siguiente imagen representa un ejemplo de informe de análisis:



Ejemplo de Informe de Análisis

El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

8.3. Objetos Excluidos del Análisis

En algunos casos puede necesitar excluir del análisis algunos elementos. Por ejemplo, si desea excluir el archivo del test EICAR del análisis en tiempo real, o los archivos `.avi` del análisis bajo demanda.

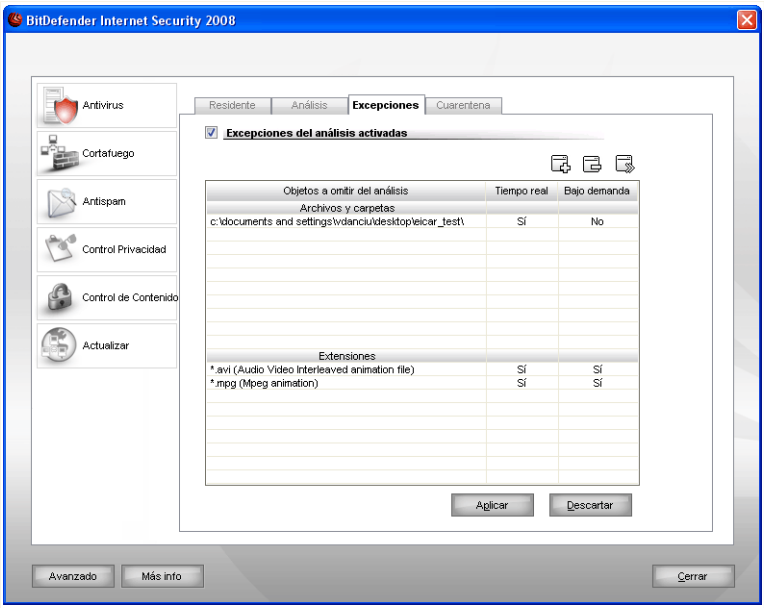
BitDefender permite excluir algunos objetos del análisis bajo demanda, del análisis en tiempo real, o de ambos. Esta característica pretende disminuir el tiempo de análisis y evitar interferencias con su trabajo.

Pueden excluirse del análisis dos tipos de objetos:

- **Ruta** - el archivo o carpeta (incluyendo los objetos que contiene) indicado por la ruta será excluido del análisis.
- **Extensiones** - todos los archivos con la extensión indicada serán excluidos del análisis.

Nota
Los objetos excluidos del análisis en tiempo real no serán analizados, tanto si usted accede al mismo, o bien accede una aplicación

Para ver y administrar los objetos excluidos del análisis, haga clic en **Antivirus > Excepciones** en la consola de configuración. Aparecerá la siguiente pantalla:



Excepciones

Aquí podrá ver todos los objetos (archivos, carpetas, extensiones) que están excluidos del análisis. En cada objeto podrá ver si está excluido del análisis al acceder, bajo demanda, o ambos.

Nota
Las extensiones especificadas aquí NO se aplican al análisis contextual.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**. Aparecerá una nueva ventana donde podrá cambiar la extensión o la ruta a excluir, y el tipo de análisis del que desea excluirlo. Realice los cambios necesarios y pulse **Aceptar**.

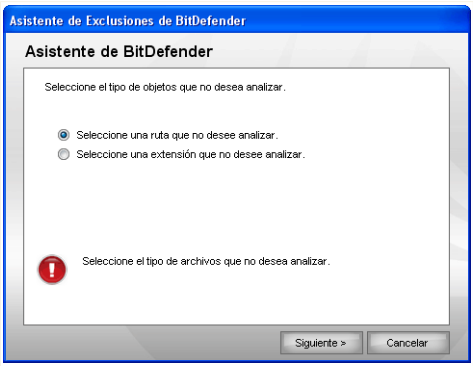
Nota
También puede hacer clic derecho encima del elemento y utilizar las opciones del menú rápido para editarlo o eliminarlo.

Puede hacer clic en **Descartar** para revertir los cambios realizados en la tabla, siempre y cuando no los hay guardado pulsando el botón **Aplicar**.

8.3.1. Excluyendo Rutas del Análisis

Para excluir una ruta del análisis, haga clic en el botón **Añadir**. El asistente de configuración que aparecerá le guiará a través del proceso de exclusión de rutas del análisis

Paso 1/3 – Seleccione Tipo de Objeto

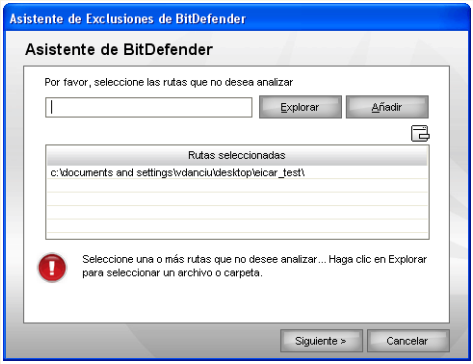


Tipo de Objeto

Seleccione la opción de exclusión de ruta de análisis.

Haga clic en **Siguiente**.

Paso 2/3 – Especificar Rutas a Excluir



Rutas Excluidas

Para indicar las rutas a excluir siga cualquiera de estos métodos:

- Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Añadir**.
- Introduzca la ruta que desea excluir del análisis en el campo editable, y haga clic en **Añadir**.

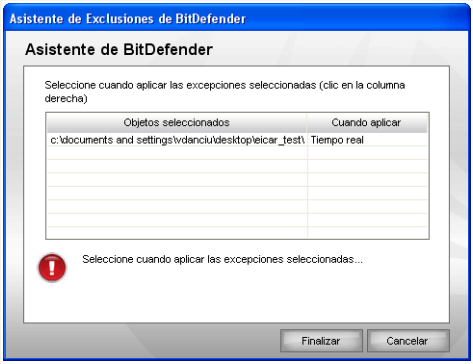
> ***Nota***
> Si la ruta seleccionada no existe, aparecerá un mensaje de error. Haga clic en **Aceptar** y compruebe la validez de ruta.

Las rutas aparecerán en la tabla a medida que las vaya añadiendo. Puede añadir tantas rutas como desee.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Haga clic en **Siguiente**.

Paso 3/3 – Seleccionar Tipo de Análisis



Tipo de Análisis

Puede ver una tabla que contiene las rutas a excluir y el tipo de análisis del que están excluidas.

Por defecto, las rutas seleccionadas se excluyen de los dos tipos de análisis (al acceder y bajo demanda). Si desea modificar el tipo de análisis, haga clic en la columna derecha y seleccione la opción deseada de la lista.

Haga clic en **Finalizar**.

Haga clic en **Aplicar** para guardar los cambios.

8.3.2. Excluyendo Extensiones del Análisis

Para excluir extensiones del análiss, haga clic en el botón **Añadir**. Aparecerá un asistente que le guiará a través del proceso de exclusión de extensiones.

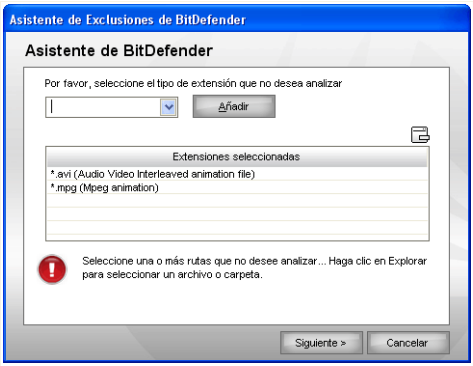
Paso 1/3 – Seleccione Tipo de Objeto

Tipo de Objeto

Seleccione la opción de exclusión del análisis de una extensión.

Haga clic en **Siguiente**.

Paso 2/3 – Especificar Extensiones a Excluir



Extensiones Excluidas

Para especificar las extensiones a excluir del análisis, utilice cualquiera de los siguientes métodos:

- Seleccione, desde el menú, la extensión que será excluida del análisis y a continuación haga clic en **Añadir**.

> ***Nota***
> El menú contiene una lista de todas las extensiones registradas en su sistema. Cuando seleccione una extensión, podrá ver su descripción (si existe).

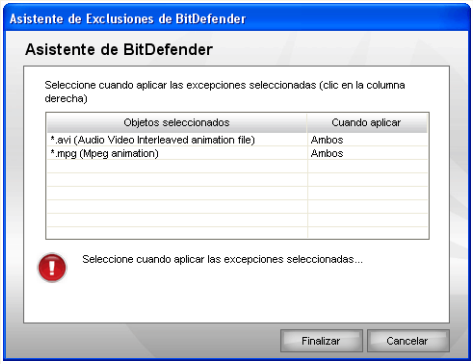
- Introduzca la extensión que desea excluir en el campo editable, y haga clic en **Añadir**.

Las extensiones aparecerán en la tabla a medida que las vaya añadiendo. Puede añadir tantas extensiones como desee.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Haga clic en **Siguiente**.

Paso 3/3 – Seleccionar Tipo de Análisis



Tipo de Análisis

Puede ver una tabla que contiene las extensiones a excluir, y el tipo de análisis del que se ha excluido.

Por defecto, las extensiones seleccionadas se excluyen de los dos tipos de análisis (al acceder y bajo demanda). Si desea modificar el tipo de análisis, haga clic en la columna derecha y seleccione la opción deseada de la lista.

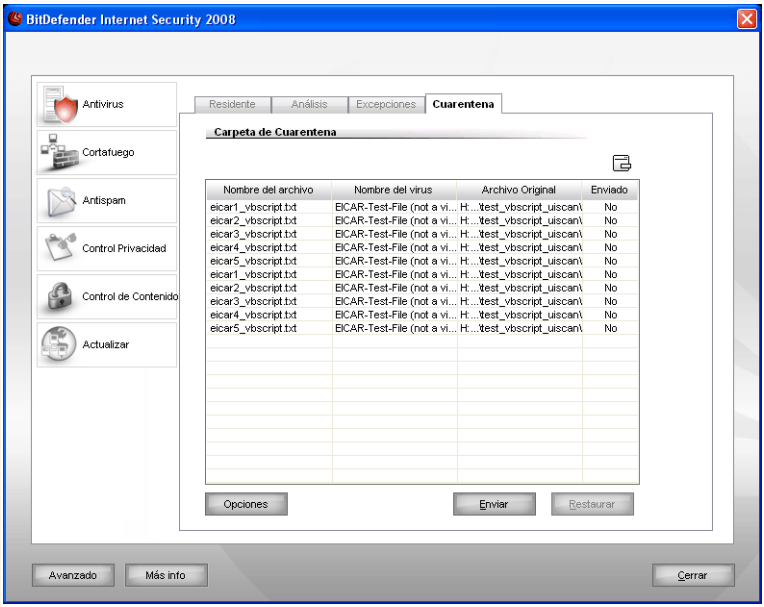
Haga clic en **Finalizar**.

Haga clic en **Aplicar** para guardar los cambios.

8.4. Área de Cuarantena

BitDefender permite aislar los ficheros infectados en una zona de cuarentena. Al aislarlos, el riesgo de infección se reduce considerablemente y, al mismo tiempo, le ofrece la posibilidad de enviar estos ficheros para un análisis adicional en el laboratorio de BitDefender.

Para ver y gestionar los archivos en cuarentena, o configurar las opciones, haga clic en **Antivirus > Cuarentena** en la consola de configuración.



Cuarantena

8.4.1. Administrando los Archivos en Cuarentena

En la imagen puede ver que la ventana **Cuarentena** contiene un listado de los ficheros aislados hasta el momento. Cada fichero contiene ciertos datos: su nombre, nombre del virus detectado, su ruta original y la fecha de envío a los laboratorios.

Nota
Cuando un virus está aislado en cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

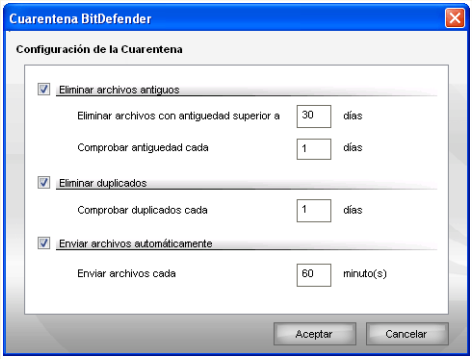
Para eliminar un archivo de la cuarentena haga clic en el botón **Eliminar**. Si quiere restaurar un archivo a su ubicación inicial haga clic en **Restaurar**.

Puede enviar cualquier archivo de la cuarentena a los Laboratorios de BitDefender haciendo clic en **Enviar**.

Menú contextual. A través del menú contextual podrá gestionar los archivos de la cuarentena fácilmente. También puede seleccionar **Actualizar** para actualizar el apartado de Cuarentena.

8.4.2. Configurando las Opciones de Cuarentena

Para modificar la configuración de la Cuarentena, haga clic en **Configurar**. Aparecerá una nueva ventana.



Configurar la Cuarentena

Al utilizar las opciones de la cuarentena conseguirá que BitDefender realice automáticamente las siguientes acciones:

Eliminar archivos antiguos. Para eliminar automáticamente los archivos antiguos de la cuarentena, marque la casilla correspondiente. Debe indicar el número de días tras los cuales se eliminarán los archivos de la cuarentena, y la frecuencia con la que BitDefender comprobará si existen.

Nota
Por defecto, BitDefender comprobará si existen archivos antiguos cada día, y eliminará los más antiguos a 10 días.

Eliminar duplicados. Para eliminar automáticamente los archivos duplicados de la cuarentena, marque la opción correspondiente. Debe indicar el número de días tras los cuales se comprobará si existen duplicados.

Nota
Por defecto, BitDefender comprobará diariamente si hay archivos duplicados en la cuarentena.

Enviar archivos automáticamente. Para enviar automáticamente los archivos en cuarentena, marque la opción correspondiente. Debe indicar la frecuencia con la enviar los archivos.

Nota
BitDefender enviará por defecto, cada 60 minutos, los archivos en cuarentena.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

9. Cortafuego

El Cortafuego protege su sistema de los intentos de conexión externos o internos no autorizados. Es parecido a tener un guardia en su la puerta – vigilará su conexión a Internet y monitorizará todas las conexiones que usted decida autorizar o bloquear.

Nota
Es esencial tener instalado un cortafuego si dispone de una conexión de ancha banda o DSL.

Con el modo Oculto su ordenador "se oculta" del software malintencionado y los hackers. El módulo Cortafuego es capaz de detectar y protegerle automáticamente de los análisis de puertos (flujo de paquetes enviados a una máquina para encontrar "puntos de acceso", y que a menudo son una preparación para un ataque).

El apartado **Cortafuego** de esta guía comprende los siguientes temas:

- Comprensión del Cortafuego
- Estado del Cortafuego
- Protección de Tráfico
- Opciones Avanzadas
- Actividad del Cortafuego
- Zonas de Red

9.1. Comprensión del Cortafuego

El Cortafuego de BitDefender ha sido diseñado para ofrecer la mejor protección a sus conexiones de red / Internet, sin que tenga que configurar nada. No importa si está conectado directamente a Internet, a una o diferentes redes (Ethernet, wireless, VPN u otros tipos de red), de confianza o desconocidas, el cortafuego se auto-configurará para adaptarse a la situación correspondiente.

Por defecto, BitDefender detecta automáticamente la configuración de la red de su ordenador y crea el perfil más apropiado. También añade las redes detectadas en el perfil, como zonas de red de confianza o desconocidas, en función de su configuración.

9.1.1. Qué son los Perfiles del Cortafuego?

Un perfil del cortafuego es un conjunto de reglas que controlan el acceso a la red / Internet de las aplicaciones.

En función de la configuración de la red de su equipo, BitDefender creará automáticamente un tipo de perfil específico. El perfil básico contiene reglas de acceso a la red o reglas elementales de acceso a Internet, necesarias para el sistema y los componentes de BitDefender.

Nota
Se creará un único perfil, independientemente del número de redes a las que esté conectado.

Hay 3 tipos de perfiles básicos:

Perfil	*Descripción*
Conexión Directa	Contiene las reglas de acceso a Internet elementales, recomendadas para una configuración de red que permita la conexión directa a Internet. Las reglas no permiten que los usuarios de red accedan a su equipo, ni que explore la red.
Insegura	Contiene las reglas de acceso recomendadas para una configuración de red asociada con una red insegura. Las reglas le permiten navegar por la red, pero impide el acceso de otros miembros de la red a su equipo.
De confianza	Contiene las reglas de acceso a la red recomendadas para una configuración de red asociada con una red segura. No se imponen restricciones de acceso a la red. Esto significa que tiene acceso a los recursos compartidos, a las impresoras de red y otros recursos. A su vez, los miembros de la red también pueden acceder a sus recursos compartidos.

A medida que las aplicaciones intenten conectarse a Internet, se irán creando las reglas necesarias en su perfil. Puede elegir entre permitir y bloquear el acceso a Internet de las aplicaciones cuyas reglas no han sido configuradas, bien o permitir el acceso a las aplicaciones de la lista blanca y pedir permiso para el resto de aplicaciones.

Nota

Para especificar la política de acceso de las aplicaciones que intenten conectarse a Internet por primera vez, diríjase al apartado Estado y establezca el nivel de protección. Para editar el perfil existente, diríjase al apartado Tráfico y haga clic en **Editar Perfil**.

9.1.2. Qué son las Zonas de Red?

Una zona de red representa a un ordenador o red que está completamente aislada de equipo, o por el contrario, que puede detectar y conectarse a su equipo. En la práctica, una zona es una dirección IP o un rango de IPs que tiene acceso a su equipo o que están bloqueadas.

Por defecto, BitDefender añade automáticamente zonas a cada configuración de red específica. Se añade una zona al crear una regla de acceso apropiada, aplicable a una red entera, en el perfil actual.

Hay 2 tipos de zonas:

Tipo de Zona	Descripción
Zona de Confianza	Los equipos añadidos a la zona de confianza podrán conectarse a su equipo y usted podrá conectarse a ellos. Se permiten todas las conexiones procedentes de esa zona, así como todas las conexiones establecidas desde su ordenador hacia dicha zona. Si agrega una red como zona de confianza, tendrá acceso ilimitado a los recursos de red compartidos, impresoras de red u otros recursos de red. También, los usuarios de su red podrán acceder a sus recursos compartidos.
Zona Insegura	Los equipos que pertenecen a una zona insegura no pueden acceder a su equipo pero tampoco podrá contactar usted con ellos. SE bloquean todos los intentos de conexión procedentes de esa zona, así como todos los intentos de conexión de su ordenador hacia dicha zona. El tráfico ICMP está bloqueado y el Modo Oculto activado. Su ordenador será prácticamente invisible para todos los equipos de esa zona.

Nota

Para editar una zona seleccione la opción Zonas. Para editar la regla correspondiente a esta zona seleccione Tráfico y a continuación clic en **Editar Perfil**.

9.1.3. Funcionamiento del Cortafuego

Al reiniciar el sistema después de la instalación, BitDefender detectará automáticamente su configuración de red, creará un perfil básico adecuado y añadirá zonas en función de la configuración de red detectada.

Nota

Si está conectado directamente a Internet no se creará ninguna zona. Si está conectado a más de una red, se añadirán zonas en función de las respectivas redes.

Cada vez que cambie la configuración de la red se creará un nuevo perfil y se modificarán las zonas acorde con los cambios.

Cuando se crea un perfil de cortafuego, se guarda el perfil antiguo, de manera que podrá cargarlo de nuevo cuando vuelva a la configuración anterior.

BitDefender se volverá a configurar acorde con la configuración de red. Así es cómo el Cortafuego de BitDefender está configurado por defecto:

- Si está conectado directamente a Internet, independientemente de que también esté conectado a otras redes, se creará un perfil de Conexión Directa. De lo contrario, se creará un perfil de red insegura.

  Nota

  Como medida de seguridad, no se crean perfiles de confianza por defecto. Para crear un perfil de confianza, debe reiniciar el perfil existente. Para más información, consulte el capítulo "*Restaurando los Perfiles*" (p. 102).

- Las zonas se añaden en función de la configuración de red.

Tipo de Zona	*Configuración de la Red*
Zona de Confianza	**IP privada sin puerta de enlace** - El equipo forma parte de una red local (LAN) y no se conecta a Internet. Un ejemplo serían las redes domésticas que se crean para compartir archivos, impresoras y otros recursos entre los diferentes miembros de la familia.
	IP privada con Controlador de Dominio - El equipo forma parte de una LAN y está conectado a un dominio. Un ejemplo sería una red de oficina que permite a los usuarios compartir archivos y otros recursos dentro del dominio. Un dominio

Tipo de Zona	Configuración de la Red
	implica la existencia de una serie de políticas que deben cumplir los equipos que forman parte.
Zona Insegura	**Red inalámbrica abierta (no segura)** Un ejemplo sería el acceso gratuito a Internet desde un lugar público.

Nota

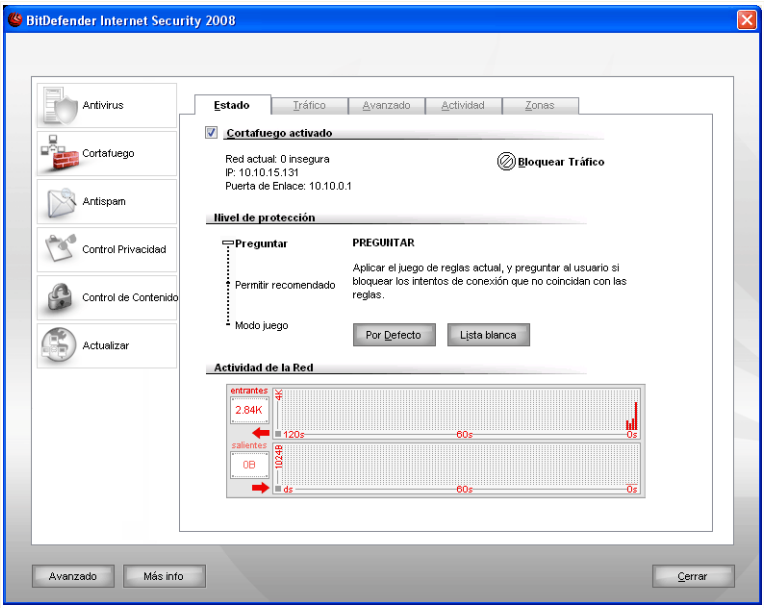
En algunas configuraciones de red no se crean zonas, como en:

- **IP pública (routable)** - el equipo está conectado directamente a Internet.
- **IP privada con puerta de enlace, pero sin Controlador de Dominio** - El equipo forma parte de una LAN, pero sin controlador de dominio, y se conecta a Internet a través de una puerta de enlace. Un ejemplo sería el campus de una escuela que permite a los usuarios compartir archivos y otros recursos.

- El Modo Oculto está desactivado.
- Se permiten conexiones VPN y conexiones remotas.
- La Conexión compartida a Internet no se permite para zonas inseguras.
- Las aplicaciones de la lista blanca tienen acceso, mientras que para las otras aplicaciones se le solicitará permiso la primera vez que intenten conectarse.

9.2. Estado del Cortafuego

Para configurar el cortafuego, haga clic en **Cortafuego > Estado** en la consola de configuración. Aparecerá la siguiente pantalla:



Estado del Cortafuego

En este apartado puede activar o desactivar el **Cortafuego**, bloquear todo el tráfico de red/Internet y determinar el comportamiento predeterminado del Cortafuego en los nuevos eventos.

Importante
Para estar protegido contra los ataques de Internet mantenga el **Cortafuego** activado.

Para bloquear todo el tráfico de red/Internet haga clic en **Bloquear tráfico** y a continuación haga clic en **Si** para confirmar su decisión. Esto aislará a su ordenador de todos los otros ordenadores de la red.

Para desbloquear el tráfico, pulse el botón **Desbloquear Tráfico**.

En la parte de abajo puede ver las estadísticas de BitDefender referentes al tráfico saliente y entrante. El gráfico muestra el volumen de tráfico de internet en los últimos dos minutos.

Nota
El gráfico aparece aunque el **Cortafuego** esté desactivado.

9.2.1. Configurando el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel adecuado de protección.

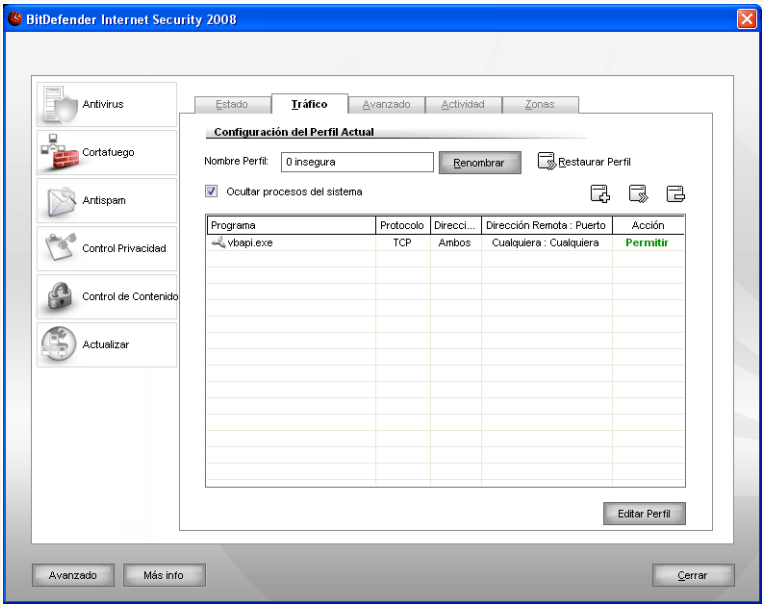
Hay 3 niveles de seguridad:

Nivel de Protección	*Descripción*
Modo Trabajo	Aplica las reglas actuales y permite todo el tráfico que no coincida con las reglas actuales sin preguntar. Esta política no es en absoluto recomendable, pero puede resultar útil para los administradores de red y jugadores.
Permitir recomendados	Aplica las reglas actuales y permite que los programas de la lista blanca puedan establecer conexiones salientes sin preguntarle. Para el resto de intentos de conexión, BitDefender solicitará su permiso. Puede ver las reglas de tráfico en el apartado Tráfico. La lista blanca está formada por las aplicaciones más utilizadas por los usuarios. Esto incluye los navegadores web más comunes, reproductores de audio y vídeo, programas de mensajería instantánea e intercambio de archivos, y también clientes de servidores (Correo, FTP..) o aplicaciones del sistema operativo. Si desea ver los programas que pertenecen a la lista blanca haga clic en **Lista Blanca**.
Preguntar	Aplica las reglas y le consulta sobre el tráfico que no coincide con ninguna de las reglas actuales.

Haga clic en **Por Defecto** para aplicar la política predeterminada (**Permitir recomendado**).

9.3. Control del Tráfico

Para administrar las reglas del cortafuego haga clic en la opción **Cortafuego > Tráfico** en el área de configuración. Aparecerá la siguiente pantalla:



Control del Tráfico

Permite definir qué conexiones entrantes o salientes quiere permitir/bloquear. Puede crear reglas para protocolos específicos, puertos, aplicaciones y/o direcciones remotas.

Las reglas pueden ser introducidas automáticamente (mediante la ventana de alerta) o manualmente (haga clic en **Añadir** y elija los parámetros para la nueva regla).

9.3.1. Añadir Reglas Automáticamente

Con el **Cortafuego** activado, BitDefender le pedirá permiso siempre que se realice una conexión a Internet:

Alerta Cortafuego

En la alerta encontrará la siguiente información: la aplicación que está intentando acceder a Internet, la ruta de la aplicación, el destino, el protocolo utilizado y el puerto al que la aplicación está intentando conectarse.

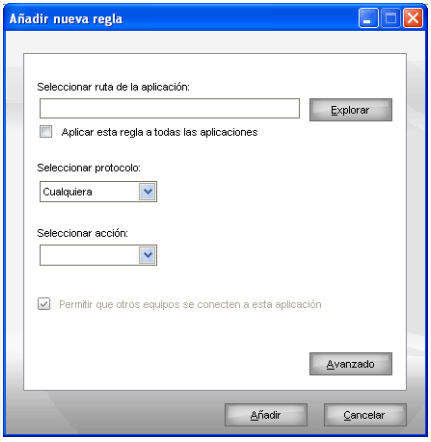
Haga clic en **Permitir** para permitir todo el tráfico (entrante y saliente) generado por las aplicaciones ejecutadas localmente hacia cualquier IP de destino y en todos los puertos. Si selecciona **Bloquear**, se bloqueará el acceso de la aplicación a Internet.

En función de su respuesta, se creará una regla, se aplicará y añadirá a la lista. La próxima vez que la aplicación intente conectarse, se aplicará dicha regla.

Importante
Permita los intentos de conexión entrantes sólo de aquellas IPs y dominios en los que confíe plenamente.

9.3.2. Añadiendo Reglas Manualmente

Haga clic en el botón **Añadir Regla** y seleccione los parametros de la regla. Aparecerá la siguiente pantalla:



Añadir Regla

Para añadir una nueva regla de cortafuego, siga estos pasos:

1. Seleccione la aplicación que se verá afectada por la nueva regla del cortafuego.

   Para seleccionar la aplicación, haga clic en **Explorar**, márquela y a continuación **Aceptar**.

   Si también quiere aplicar esta regla a todas las aplicaciones, marque la opción **Aplicar esta regla a todas las aplicaciones**.
2. Seleccione el protocolo sobre el que debe aplicarse la regla.

   Dispone de una lista con los tipos de protocolo más comunes para ayudarle a seleccionar sólo protocolos concretos. Seleccione el protocolo deseado (en el que se aplicará la regla) desde el menú desplegable correspondiente o seleccione **Cualquiera** para seleccionar todos los protocolos.

   La siguiente tabla enumera los protocolos que puede seleccionar junto con una breve descripción:

Protocolo	*Descripción*
ICMP	Internet Control Message Protocol – es una extensión del Internet Protocol (IP). ICMP soporta paquetes que contengan mensajes de error, control e información. El comando PING, por ejemplo, utiliza ICMP para testear una conexión a Internet.

Protocolo	Descripción
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión) – El protocolo TCP permite establecer una conexión e intercambiar flujos de datos entre dos ordenadores. TCP garantiza la entrega de los datos y también que los paquetes serán entregados en el mismo orden en el que fueron enviados.
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuario) – El protocolo UDP es un transporte basado en IPs y diseñado para un alto rendimiento. Los juegos y otras aplicaciones basadas en vídeo a menudo utilizan el protocolo UDP.

3. Seleccione la acción de la regla de su apartado correspondiente.

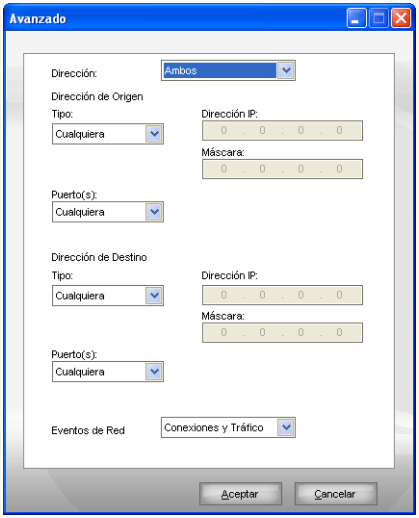
Acción	Descripción
Permitir	Se permitirá el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.
Bloquear	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

4. Si el protocolo previamente seleccionado es TCP o UDP, puede especificar si la regla se aplicará cuando la aplicación actúa como un servidor o no.

   Seleccione **Permitir a otros equipos conectarse a esta aplicación** para aplicar la acción a todos los eventos de la red. Por defecto, permite o denega a la aplicación los permisos para abrir los puertos necesarios.

   Si quiere aplicar las medidas sólo para el tráfico UDP o TCP respectivamente, desmarque las casillas correspondientes.

Si desea configurar más opciones para esta regla, seleccione **Avanzado**. Aparecerá una nueva ventana:



Configuración Avanzada de Reglas

Puede configurar lo siguiente:

- **Dirección** - seleccione la dirección del tráfico.

Tipo	*Descripción*
Saliente	La regla se aplicará sólo para el tráfico saliente.
Entrante	La regla se aplicará sólo para el tráfico entrante.
Ambos	La regla aplicará en ambas direcciones.

- **Dirección de origen** - para especificar la dirección de origen.

  Para especificar la dirección de origen, seleccione el tipo de dirección desde el menú e introduzca los datos solicitados. Dispone de las siguientes opciones:

Tipo	*Descripción*
Cualquiera	La regla se aplicará a cualquier dirección de origen.

Tipo	Descripción
Host	La regla se aplicará sólo si el origen es el host especificado. Debe introducir la dirección IP del host.
Red	La regla se aplicará sólo para el tráfico de la red especificada. Debe introducir la dirección IP y la máscara de la red.
Host Local	La regla se aplicará sólo si el origen es del host local. Si usa más de una interfaz de red, seleccione la interfaz en la que desea aplicar la regla. Si desea que la regla se aplique a todos los hosts locales, seleccione **Cualquiera**.
Red Local	La regla se aplicará sólo si el origen es la red local. Si está conectado a más de una red, seleccione la red en la que desea aplicar la regla. Si desea que la regla se aplique a todas las redes locales, seleccione **Cualquiera**.

Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.

- **Dirección de Destino** - indica la dirección de destino.

Para especificar la dirección de destino, seleccione el tipo de dirección e introduzca los datos necesarios. Dispone de las siguientes opciones:

Tipo	Descripción
Cualquiera	La regla aplicará a cualquier dirección de destino.
Host	La regla se aplicará sólo si el destino es el host indicado. Debe introducir la dirección IP del host.
Red	La regla se aplicará sólo si el destino es la red indicada. Debe introducir la dirección IP y la máscara de la red.
Host Local	La regla se aplicará sólo si el destino es el host local. Si usa más de una interfaz de red, seleccione la interfaz en la que desea aplicar la regla. Si desea que la regla se aplique a todos los hosts locales, seleccione **Cualquiera**.
Red Local	La regla se aplicará sólo si el destino es la red local. Si está conectado a más de una red, seleccione la red en la que desea aplicar la regla. Si desea que la regla se aplique a todas las redes locales, seleccione **Cualquiera**.

Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.

- **Eventos de la Red** - si ha seleccionado el protocolo TCP o UDP, deberá indicar los eventos de la red en los que desea que se aplique la regla.

Haga clic en **Aceptar** para cerrar la ventana de opciones avanzadas.

Haga clic en **Añadir** para añadir la regla del cortafuego.

9.3.3. Administrando Reglas

Puede ver las reglas del perfil creadas hasta el momento en la tabla.

Marque la casilla **Ocultar procesos del sistema** para ocultar las reglas correspondientes a los procesos del sistema o de BitDefender.

Las reglas se listan por prioridad empezando por arriba, lo que significa que la primera regla tiene la prioridad más alta. Haga clic en **Editar Perfil** para entrar en la **Vista detallada** para cambiar su prioridad moviéndolas arriba y abajo.

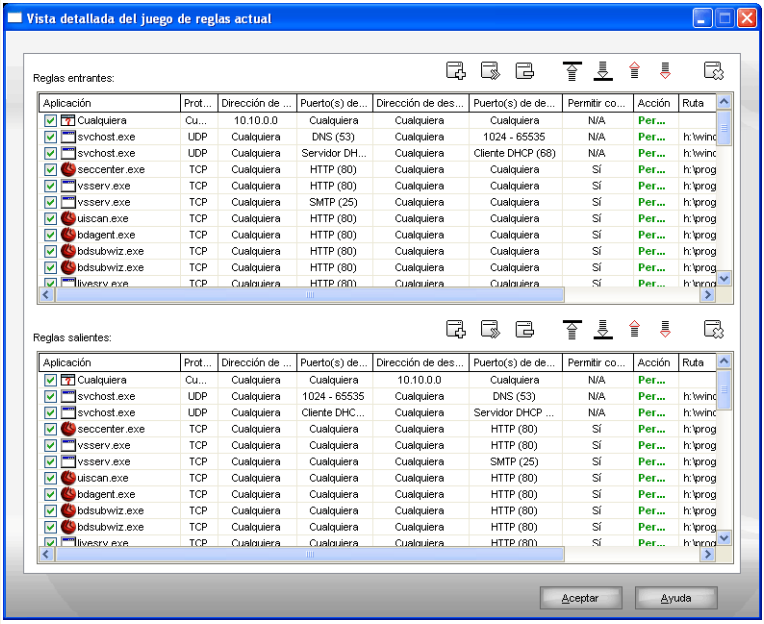
Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar regla**.

Para editar una regla, selecciónela y haga clic en el botón **Editar regla** o simplemente haga doble clic en la regla.

Nota
También dispone de un menú contextual que contiene las siguientes opciones: **Añadir regla**, **Eliminar regla** y **Editar regla**.

9.3.4. Modificando los Perfiles

Puede modificar un perfil haciendo clic en **Editar perfil**. Se le mostrará la siguiente ventana:



Vista Detallada

Las reglas se dividen en dos apartados: reglas entrantes y reglas salientes. Puede ver la aplicación y los parámetros de cada regla (dirección de origen, dirección de destino, puertos de origen, puertos de destino, acción, etc).

Para eliminar una regla, sólo tiene que seleccionarla y hacer clic en el botón **Eliminar Regla**. Para eliminar todas las reglas haga clic en el botón **Vaciar lista**. Para modificar una regla, puede seleccionarla y hacer clic en el botón **Editar Regla** o hacer doble clic sobre la regla. Para desactivar una regla temporalmente, sin eliminarla, desmarque la casilla correspondiente.

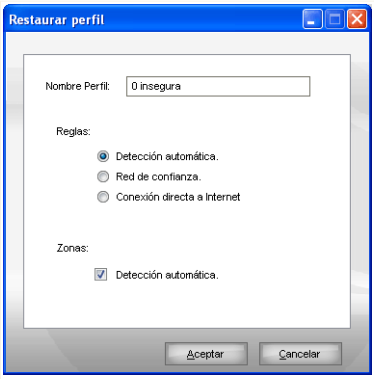
Puede subir o bajar la prioridad de una regla. Haga clic en el botón **Subir** para subir la prioridad de la regla seleccionada, o haga clic en el botón **Bajar** para bajar la prioridad de la regla seleccionada. Para dar la máxima prioridad a una regla, haga clic en el botón **Primera**. Para dar la mínima prioridad a una regla, haga clic en el botón **Última**.

Nota
También existen un menú contextual con las siguientes opciones: **Añadir Regla**, **Editar Regla**, **Eliminar Regla**, **Subir**, **Bajar**, **Primera**, **Última** y **Vaciar lista**.

Haga clic en **Aceptar** para cerrar la ventana.

9.3.5. Restaurando los Perfiles

Los usuarios avanzados pueden volver a configurar el perfil del cortafuego para optimizar la protección del cortafuego o para ajustarlo a sus necesidades. Para restaurar el perfil del cortafuego, haga clic en **Restaurar Perfil**. Aparecerá la siguiente pantalla:



Restaurar Perfil

Puede configurar lo siguiente:

- **Nombre del Perfil** - introduzca un nuevo nombre en el campo editable.
- **Reglas** - indique el tipo de reglas que deben crearse para las aplicaciones del sistema.

  Dispone de las siguientes opciones:

Opción	Descripción
Detección Automática	Deje que BitDefender detecte la configuración de la red y cree el juego de reglas elementales más apropiado.

Opción	Descripción
Red de Confianza	Crea un juego de reglas apropiado para las redes de confianza.
Conexión Directa a Internet	Crea un juego de reglas apropiado para las conexiones directas a Internet.

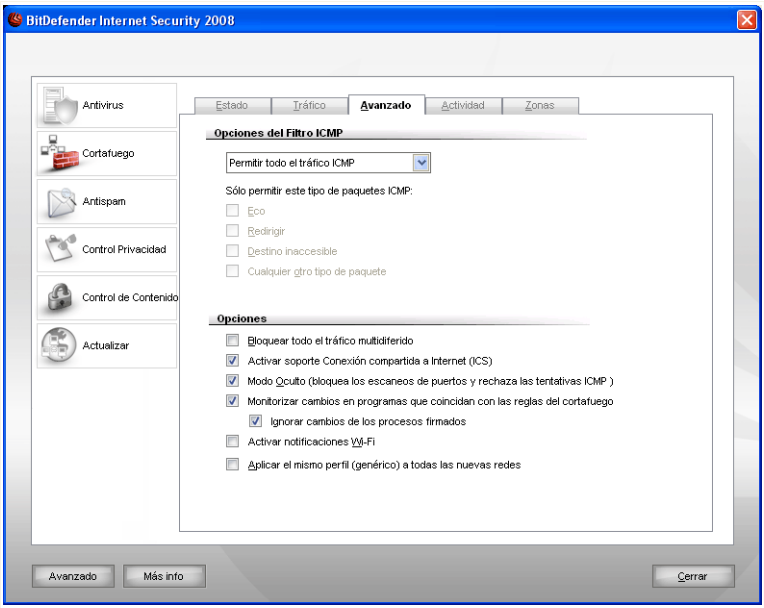
- **Zonas** - marque la casilla **Detección Automática** para dejar que BitDefender cree las zonas apropiadas para las redes detectadas.

Haga clic en **Aceptar** para cerrar la ventana y restaurar el perfil.

Importante
Al restaurar el perfil del cortafuego, se eliminarán todas las reglas que ha añadido en este apartado.

9.4. Opciones Avanzadas

Para modificar las opciones avanzadas del cortafuego de BitDefender, haga clic en **Cortafuego > Avanzado** en la consola de configuración. Aparecerá la siguiente pantalla:



Opciones Avanzadas

En este apartado puede configurar las opciones avanzadas del Cortafuego de BitDefender. Las opciones avanzadas le permiten especificar las reglas de filtrado para el tráfico ICMP (Configuración del Filtro ICMP) y bloquear el tráfico multidiferido, compartir su conexión a Internet o hacer su ordenador invisible para el software malintencionado y los hackers (Configuración).

9.4.1. Configurando las Opciones de Filtrado ICMP

Desde el menú, puede seleccionar una de las siguientes políticas para filtrar el tráfico ICMP:

- **Permitir todo el tráfico ICMP** - permite todo el tráfico ICMP.
- **Bloquear todo el tráfico ICMP** - bloquea todo el tráfico ICMP.
- **Filtro ICMP personalizado** - personaliza la forma de filtrar el tráfico ICMP. Podrá elegir el tipo de paquetes ICMP que desea permitir.

  Dispone de las siguientes opciones:

Opción	Descripción
Eco	Esta opción habilita los mensajes Echo Reply y Echo Request. El Echo Request es un mensaje ICMP que envía un paquete de datos al host y espera a que esos datos sean enviados de vuelta en un Echo Reply. El host debe responder a todos los Echo Request con un Echo Reply que contenga los datos exactos recibidos en el mensaje de petición. El Echo Reply es un mensaje ICMP generado en respuesta a un mensaje ICMP Echo Request, y es obligatorio para todos los hosts y routers.
Redirigir	Este es un mensaje ICMP que informa al host que redireccione su información de ruta (para enviar paquetes en una ruta alternativa). Si el host intenta enviar datos a través de un router (R1) y después a otro router (R2) para alcanzar al host, y existe una ruta directa desde el host hasta R2, la redirección informará al host de tal ruta. El router intentará enviar el datagrama original a la destinación pretendida. En cualquier caso, si el datagrama contiene información de enrutamiento no será enviado incluso si una ruta mejor está disponible.
Destino inaccesible	Se trata de un mensaje ICMP que es generado por el router para informar al cliente de que el host de destino no se puede alcanzar, a menos que el datagrama tenga una dirección multidiferida. Las razones de este mensaje pueden incluir la inexistencia de una conexión física al host (la distancia es infinita), que el protocolo o el puerto indicado no está activo, o que la información debe ser fragmentada pero el marcador “no fragmentar” está activo.
Cualquier otro tipo de paquete	Con esta opción habilitada cualquier otro paquete que no sea **Eco**, **Destino inaccesible** o **Redirigir** pasará.

9.4.2. Modificando las Opciones Avanzadas del Cortafuego

Dispone de las siguientes opciones avanzadas del cortafuego:

- **Bloquear todo el tráfico multidiferido** - con esta opción habilitada cualquier paquete multidiferido recibido será descartado.

  El tráfico multidiferido es el tipo de tráfico que tiene como destino un grupo de una red. Los paquetes son enviados a una dirección especial desde donde los clientes de contenido multidiferido lo pueden recibir si aceptan la petición.

  Por ejemplo, un miembro de una red que posee un sintonizador de televisión puede emitir el flujo de video a cada miembro de la red (broadcast), o a través del tráfico multidiferido a la dirección especial. Los ordenadores que escuchan a esa dirección multidiferida pueden aceptar o rechazar el paquete. Si se acepta, el flujo de video se puede visualizar por los clientes de contenido multidiferido.

  Un exceso de tráfico multidiferido consume ancho de banda y recursos. Con esta opción activada, cualquier paquete multidiferido que reciba será rechazado. Sin embargo, no es recomendable seleccionar esta opción.
- **Activar soporte Conexión compartida a Internet (ICS)** - activa el soporte para Conexión Compartida a Internet (ICS).

  Nota
  Esta opción no activa automáticamente ICS en su ordenador, solamente permite este tipo de conexión en caso de que la active desde su sistema operativo.

  Conexión Compartida a Internet (ICS) permite a los miembros de las redes locales conectarse a Internet a través de su ordenador. Esto es muy útil en caso de que tenga una conexión especial/particular a Internet (ej. conexiones de red inalámbricas) y desea compartirla con los otros miembros de su red.

  Al compartir su conexión a Internet con los miembros de su red local puede experimentar un mayor nivel de consumo de recursos y puede implicar riesgos. También le quita algunos de sus puertos (aquellos abiertos por los miembros que usan su conexión de Internet).
- **Modo oculto** - hace que su ordenador sea invisible para el software malintencionado y los hackers.

  Una manera bastante simple de saber si su ordenador es vulnerable, es conectarse a algunos de sus puertos para ver si se recibe respuesta. Esta técnica se conoce como análisis de puertos.

Tanto los os usuarios malintencionados como el software malintencionado necesitan saber si su equipo existe en la red y qué servicios ofrece. El **Modo Oculto** actuará de manera que su equipo no responda a intentos de detección de puertos abiertos, o intentos de ubicar a su equipo.

- **Monitorizar cambios en programas que coincidan con las reglas del cortafuego** - comprueba cada aplicación que intenta conectarse a Internet para ver si ha sufrido algún cambio desde que se creó la regla de acceso. Si la aplicación ha cambiado, una alerta le preguntará si desea permitir o bloquear el acceso a Internet de esta aplicación.

  A menudo, las aplicaciones cambian debido a actualizaciones. Sin embargo, existe el riesgo de que hayan sido modificadas por aplicaciones de malware con la intención de infectar a su equipo u otros equipos de la red.

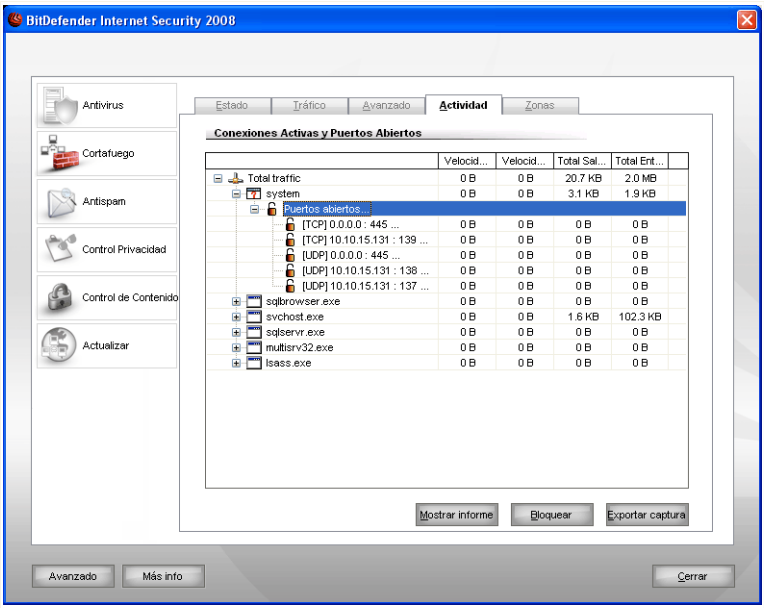
  

  Nota
  Recomendamos mantener marcada esta opción y permitir el acceso sólo a aquellas aplicaciones que imaginaba que habrían cambiado desde la creación de la regla de acceso.

  Las aplicaciones firmadas suelen ser aplicaciones de confianza con un alto grado de seguridad. Puede marcar la opción **Ignorar cambios de los procesos firmados** para permitir el acceso a Internet a aquellas aplicaciones firmadas que hayan sufrido algún cambio, sin recibir ningún mensaje de alerta.
- **Activar notificaciones Wi-Fi** - activa las notificaciones Wi-Fi.
- **Aplicar el mismo perfil (genérico) a todas las nuevas redes** - crea un perfil de cortafuego predeteminado (genérico), llamado `Generic Network`, y lo aplica al detectar una nueva configuración de red. Si vuelve a una configuración de red antigua para la cual ya existe un perfil del cortafuego, se cargará el perfil del cortafuego específico en lugar del genérico.

9.5. Control de Conexiones

Para monitorizar la actividad de red/Internet (sobre TCP o UDP) de las aplicaciones o para abrir el informe del cortafuego, haga clic en **Cortafuego > Actividad** en la consola de configuración. Aparecerá la siguiente pantalla:



Control de Conexiones

Puede ver el tráfico total ordenado por el nombre de las aplicaciones. Para cada aplicación, podrá ver las conexiones y puertos abiertos, así como estadísticas sobre la velocidad del tráfico entrante y saliente o la cantidad de datos enviados / recibidos.

Esta ventana muestra la actividad de red / Internet en tiempo real. Si las conexiones o los puertos están cerrados, verá que las estadísticas correspondientes están oscurecidas y que, finalmente, desaparecen. Lo mismo sucede con todas las estadísticas correspondientes a las aplicaciones que generen tráfico o abran puertos que usted ha cerrado.

Haga clic en **Bloquear** para crear reglas que restrinjan el tráfico de la aplicación, puerto o conexión seleccionada. Se le pedirá que confirme su elección. Las reglas se pueden reconfigurar desde el apartado Tráfico.

Nota

Para bloquear una aplicación, un puerto o una conexión, también puede hacer clic derecho y seleccione **Bloquear**.

Haga clic en **Terminar** para finalizar todas las instancias del proceso seleccionado. Se le pedirá que confirme su elección.

Nota
Para finalizar un proceso, también puede hacer clic derecho y seleccionar **Terminar**.

Haga clic en **Exportar captura** para exportar la lista a un archivo `.txt`.

Para una lista más completa de eventos del módulo de Cortafuego (iniciar/parar el cortafuego, bloqueo del tráfico, activar Modo Oculto, modificar opciones, aplicar un perfil) o de eventos generados por la actividad detectada (análisis de puertos, bloqueo de intentos de conexiones o de tráfico según las reglas) mire el informe del Cortafuego de BitDefender que se puede abrir haciendo clic en **Mostrar Informe**. El archivo está ubicado en la carpeta Archivos Comunes del usuario actual de Windows, en la ruta: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

9.6. Zonas de Red

Una zona es una dirección IP o un rango de IPs para las cuales se crea una regla especial en el perfil. La regla puede permitir acceso ilimitado a su equipo a los miembros de la red (zonas de confianza), o todo lo contrario, aislar completamente su equipo de los usuarios de la red (zona insegura).

Por defecto, BitDefender detecta automáticamente la configuración de la red a la que está conectado y añade una zona en función de su configuración.

Nota
Si está conectado a varias redes, se creará más de una zona red en función de la configuración.

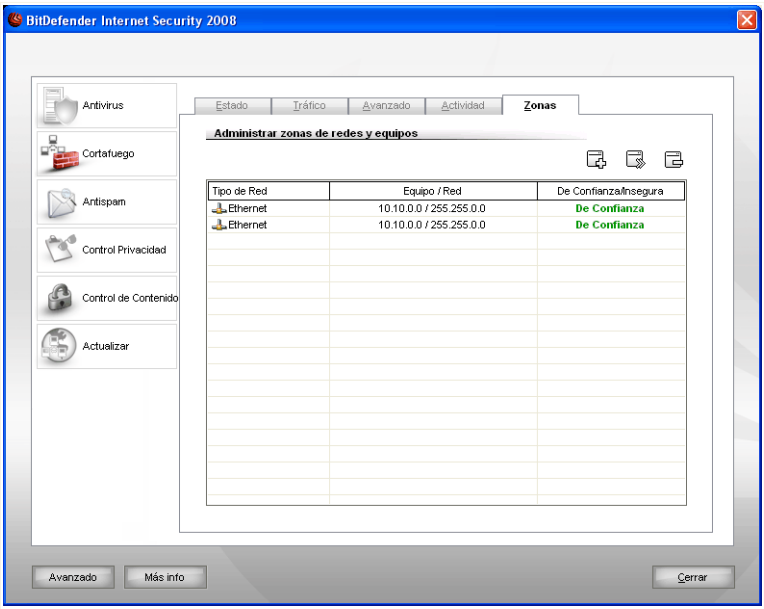
Las zonas de confianza se crean automáticamente al detectar las siguientes configuraciones de red:

- **IP privada sin puerta de enlace** - El equipo forma parte de una red de área local (LAN) y no tiene acceso a Internet.
- **IP privada con Controlador de Dominio** - El equipo forma parte de una LAN y está conectado a un dominio.

Las zonas inseguras se crean automáticamente al detectar las siguientes configuraciones de red:

- **Red inalámbrica abierta (no segura)**

Para gestionar las zonas de red, haga clic en **Cortafuego > Zonas** en la consola de configuración. Aparecerá la siguiente pantalla:



Zonas de Red

En la lista podrá ver las zonas de red correspondientes al perfil actual. En cada zona verá el tipo de red (Ethernet, wireless, PPP y otras), el equipo o red asociado a la zona y el tipo (de confianza / insegura).

Para modificar una zona, selecciónela y haga clic en el botón **Editar Zona**, o haga doble clic encima de la zona.

Nota

Por defecto, BitDefender añade zonas inseguras para las redes inalámbricas abiertas. Si está conectado a una red inalámbrica ad-hoc abierta con ordenadores de confianza (en casa o con amigos), es posible que desee modificar la zona asociada. Para compartir recursos entre los miembros de la red deberá cambiar la zona a 'De Confianza'.

Para eliminar una zona, selecciónela y haga clic en el botón **Eliminar Zona**.

9.6.1. Añadiendo Zonas

Puede añadir zonas manualmente. Esto le permitirá, por ejemplo, compartir archivos sólo con sus amigos dentro de una red inalámbrica abierta (añadiendo sus equipos como zonas de confianza), o bloquear un ordenador en una red de confianza (añadiéndolo como zona insegura).

Para añadir una zona nueva, haga clic en el botón **Añadir Zona**. Aparecerá la siguiente pantalla:

Añadir Zona

Para añadir una zona, siga estos pasos:

1. Especifique el equipo de la red o la red que desea añadir. Puede utilizar cualquiera de estos métodos:
   - Para añadir un equipo concreto, seleccione **Equipo** e introduzca su dirección IP.
   - Para añadir una red concreta, seleccione **Red** e introduzca su dirección IP y máscara.
   - Navegue por la red local para encontrar y añadir un equipo o una red.

     Para navegar por las redes locales, seleccione **Explorar red local** y haga clic en **Explorar**. Aparecerá una nueva ventana dónde podrá ver todas las redes a las que está conectado y todos los miembros de cada red.

     Seleccione el equipo o la red que desea añadir como zona, y haga clic en **Aceptar**
2. Seleccione el tipo de zona que desea crear (de confianza o insegura)
3. Haga clic en **Aceptar** para añadir la zona.

10. Antispam

BitDefender Antispam emplea sorprendentes innovaciones tecnológicas y filtros antispam estándares en la industria para impedir que el spam llegue a su bandeja de entrada.

El apartado **Antispam** de esta guía comprende los siguientes temas:

- Comprensión del Antispam
- Estado del Antispam
- Configuración del Antispam
- Integración en Clientes de Correo

10.1. Comprensión del Antispam

El correo no solicitado se ha convertido en un problema cada vez más agobiante, tanto para los usuarios domésticos como para las empresas. No es agradable, no le gustaría que sus hijos lo viesen, puede dejarle sin trabajo (al perder mucho tiempo con el spam o al recibir contenido pornográfico en su cuenta de correo de la empresa) y no puede hacer nada para detenerlo. Lo mejor del correo no solicitado es, obviamente, dejar de recibirlo. Desgraciadamente, el correo no solicitado llega en una gran variedad de formas y tamaños y siempre en una cantidad increíble.

10.1.1. Los Filtros Antispam

El motor BitDefender Antispam incorpora siete filtros distintos para mantener su Bandeja de Entrada libre de SPAM: Lista de Amigos, Lista de Spammers, Filtro de Caracteres, Filtro de Imágenes, Filtro URL, Filtro NeuNet (heurístico) y Filtro Bayesiano.

Nota
Puede activar/desactivar cada uno de estos filtros desde el apartado Configuración del módulo **Antispam**.

Lista Blanca/Lista Negra

La mayoría de la gente se suele comunicar con el mismo grupo de personas, o recibe mensajes de empresas y organizaciones de la misma área laboral. Al usar la **Lista de Amigos o de Spammers**, podrá distinguir fácilmente entre las personas cuyos mensajes desea recibir independientemente de su contenido (amigos), de aquellas cuyos mensajes no desea recibir más (spammers).

Nota
Las **Listas de Amigos/Spammers** también se conocen como **Lista Blanca (Amigos)/Lista Negra (Spammers)**.

Puede gestionar la **Lista de Amigos/Spammers** directamente desde la Consola de Configuración o desde la barra de herramientas Antispam integrada en los clientes de correo más utilizados.

Nota
Recomendamos añadir los nombres y las direcciones de correo de sus amigos la **Lista de Amigos**. BitDefender no bloquea los mensajes que provienen de esta la lista; de manera que al añadir a sus amigos a esta lista se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.

Filtro de Caracteres

Gran parte del Spam está redactado con caracteres asiáticos o cirílicos. El Filtro de Caracteres detecta este tipo de mensajes y los marca como SPAM.

Filtro de Imágenes

Los Spammers han desarrollado nuevas técnicas para evitar que los filtros de detección heurística marquen sus mensajes como Spam. Como consecuencia, la Bandeja de Entrada se llena cada vez más de mensajes que sólo incluyen una imagen con el contenido no solicitado. Para enfrentarse con este problema creciente, BitDefender ha introducido el **Filtro de Imágenes**, que compara la firma de la imagen del mensaje con las de la base de datos de BitDefender. En caso que coincidan, el mensaje será marcado como SPAM.

Filtro URL

La mayor parte de los mensajes de spam incluyen enlaces a varias páginas web. Estas páginas normalmente contienen más publicidad y la posibilidad de comprar cosas, e incluso a veces, se utilizan para el phishing.

BitDefender mantiene una base de datos con este tipo de links. El Filtro URL comprueba todos los enlaces de los mensajes y comprueba si están incluidos en la base de datos. Si están incluidos en la base de datos, el mensaje se etiquetará como SPAM.

Filtro NeuNet (Heurístico)

El **Filtro NeuNet (Heurístico)** realiza pruebas en todos los componentes del mensaje (por exemplo, no sólo en el encabezado, sino también en el cuerpo del mensaje, tanto en formato texto como HTML). Busca palabras, frases o enlaces característicos del SPAM. Basándose en los resultados del análisis, añade una puntuación de SPAM al mensaje.

El filtro también detecta mensajes y los marca como `SEXUALLY-EXPLICIT:` en el Asunto del mensaje, y los marca como SPAM.

Nota
Desde el 19 de Mayo del 2004, culaquier mensaje Spam que incluya contenido sexual debe incluir la advertencia 'SEXUALLY EXPLICIT:' (SEXUALMENTE EXPLÍCITO) en la línea Asunto; de lo contrario se enfrentarán a multas por violación de la ley federal.

Filtro Bayesiano

El **Filtro Bayesiano** clasifica los mensajes según información estadística referente al número de apariciones de ciertas palabras en los mensajes marcados como SPAM, en comparación con aquellos declarados como NO-SPAM (por el usuario o el filtro heurístico).

Esto significa que, si alguna palabra de cuatro letras (por ejemplo, una que empiece con c) aparece frecuentemente en los mensajes SPAM, es lógico asumir que hay una alta probabilidad para que el siguiente mensaje que incluya esta palabra sea SPAM. Todas las palabras relevantes en un mensaje se toman en cuenta. Al sintetizar la información estadística, se calcula la probabilidad para que el mensaje sea considerado SPAM.

Este módulo también presenta otra característica interesante: puede aprender. Se adapta rápidamente al tipo de mensajes recibidos por el usuario y almacena toda la información. Para que funcione eficazmente, el filtro debe ser "entrenado", es decir, se le tienen que presentar muestras de SPAM y de mensajes legítimos, igual que si pone cebo a un perro de caza para que siga el rastro. A veces el filtro debe ser corregido, cuando su decisión resulta errónea.

Importante
Puede corregir el módulo Bayesiano utilizando los botones **Es Spam** y **No Spam** desde la Barra de Herramientas Antispam.

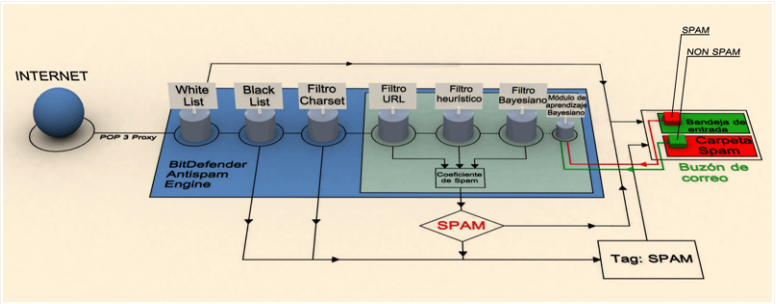
Nota
Cada vez que usted realiza una actualización:

- se añaden nuevas firmas que detectan las imágenes de Spam al **Filtro de Imágenes**.
- se añaden nuevos enlaces al **Filtro URL**.
- se añaden nuevas reglas al **Filtro NeuNet (Heurístico)**;

De esta manera se aumenta la eficiencia de los motores Antispam.
Para protegerle contra los spammers, BitDefender puede realizar actualizaciones automáticas. Mantenga activada la opción **Actualización automática**.

10.1.2. Funcionamiento del Antispam

El esquema de abajo le muestra el modo de funcionamiento de BitDefender.



Funcionamiento del Antispam

Los filtros Antispam del siguiente esquema (Lista de Amigos, Lista de Spammers, Filtro de Caracteres, Filtro de Imágenes, Filtro URL, Filtro NeuNet (Heurístico) y Filtro Bayesiano) se usan conjuntamente para determinar si un mensaje de correo electrónico debería llegar a su **Bandeja de Entrada** o no.

Cualquier mensaje proveniente de Internet pasará primero por los filtros Lista de Amigos/Lista de Spammers filter. Si el remitente se encuentra en la Lista de Amigos el mensaje será trasladado directamente a su **Bandeja de Entrada**.

De lo contrario, el filtro Lista de Spammers verificará si la dirección del remitente se encuentra en su lista. Si la dirección se encuentra en la lista, el mensaje será marcado como SPAM y será trasladado a la carpeta **Spam** (ubicada en Microsoft Outlook).

Si el remitente no se encuentra en ninguna de las dos listas, el Filtro de Caracteres comprobará si el mensaje está escrito con caracteres cirílicos o asiáticos. En tal caso, el mensaje será marcado como SPAM y trasladado a la carpeta **Spam**.

Si el mensaje no está escrito con caracteres cirílicos o asiáticos pasará al Filtro de Imágenes. El **Filtro de Imágenes** detectará todos los mensajes electrónicos que contienen imágenes de spam.

El Filtro URL buscará enlaces y los comparará con los enlaces de la base de datos de BitDefender. En caso que coincida se añadirá una puntuación de SPAM al mensaje.

El Filtro NeuNet (heurístico) realiza prueba en todos los componentes del mensaje, buscando palabras, frases, enlaces u otras características del SPAM. Como resultado, también añade una puntuación de SPAM al mensaje analizado.

Nota
Si el correo está contiene 'SEXUALLY EXPLICIT' en la línea de Asunto, BitDefender lo considerará SPAM.

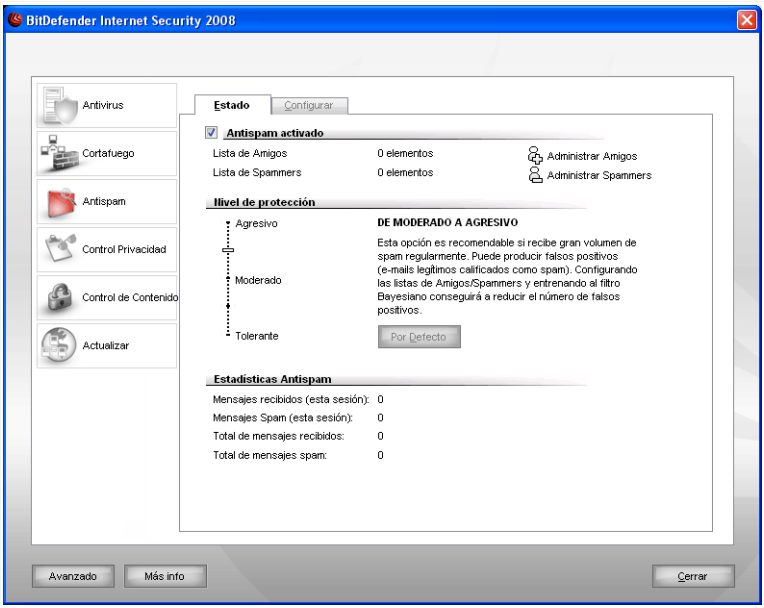
El Filtro Bayesiano clasifica los mensajes según datos estadísticos referentes a la índice de aparición de determinadas palabras en mensajes clasificados como SPAM en comparación con aquellos declarados como NO-SPAM (por el administrador o por el filtro heurístico). Se añadirá una puntuación de SPAM al mensaje analizado.

Si la puntuación total (puntuación de los filtros URL + heurístico + Bayesiano) supera la puntuación máxima de SPAM (establecida por el usuario en el apartado Estado como nivel de tolerancia), entonces el mensaje se considerará SPAM.

Importante
Si utiliza otro cliente de correo que no sea Microsoft Outlook o Microsoft Outlook Express, debería crear una regla para trasladar los mensajes marcados como SPAM a una carpeta de cuarentena. BitDefender añade el prefijo `[SPAM]` al asunto de los mensajes considerados SPAM.

10.2. Estado del Antispam

Para configurar la protección Antispam, haga clic en **Antispam > Estado** en la consola de configuración. Aparecerá la siguiente pantalla:



Estado del Antispam

En este apartado podrá configurar el módulo **Antispam** y también podrá ver la información relacionada con su actividad.

Importante
Para impedir que el spam entre en su **Bandeja de Entrada**, mantenga la protección **Antispam** activada.

En el apartado **Estadísticas** podrá ver las estadísticas del módulo Antispam. Los resultados pueden mostrarse por sesión (desde que inició por última vez el ordenador) o bien ver un resumen de la actividad antispam (desde la instalación de BitDefender).

Para configurar el módulo **Antispam** es necesario seguir estos pasos:

10.2.1. Paso 1/2 - Configurar el Nivel de Tolerancia

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel adecuado de protección.

Hay 5 niveles de tolerancia:

Nivel de tolerancia	Descripción
Tolerante	Ofrece protección para cuentas que reciben muchos mensajes comerciales legítimos. El filtro dejará pasar a la mayoría de los mensajes, pero puede producir falsos negativos (mensajes spam clasificados como legítimos).
De Tolerante a Moderado	Ofrece protección para cuentas que reciben algunos mensajes comerciales legítimos. El filtro dejará pasar a la mayoría de los mensajes, pero puede producir falsos negativos (mensajes spam clasificados como legítimos).
Moderado	Ofrece protección para cuentas habituales. Este filtro bloqueará la mayoría de los mensajes no deseados, mientras evita falsos positivos.
Moderado a Agresivo	Ofrece protección para cuentas que reciben un gran volumen de spam habitualmente. El filtro deja una cantidad muy baja de spam pasar, pero puede generar falsos positivos (mensajes legítimos marcados incorrectamente como spam). Configure las **Listas de Amigos/Spammers** y entrene el **Motor de Aprendizaje** para reducir el número de falsos positivos.
Agresivo	Ofrece protección para cuentas que reciben un gran volumen de spam habitualmente. El filtro deja una cantidad muy baja de spam pasar, pero puede generar falsos positivos (mensajes legítimos marcados incorrectamente como spam).

Nivel de tolerancia	Descripción
	Añade sus contactos a la **Lista de Amigos** para reducir el número de falsos positivos.

Para restaurar el nivel de protección predeterminado (**Moderado a Agresivo**) haga clic en el botón **Por Defecto**.

10.2.2. Paso 2/2 - Rellenar la Lista de Direcciones

Este listado contiene información sobre las direcciones de correo desde las que recibe mensajes legítimos o no solicitados.

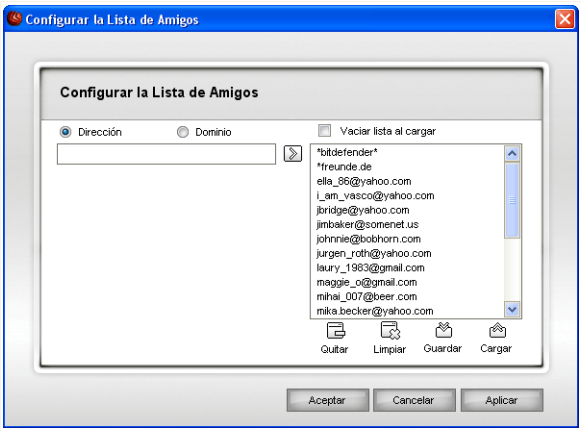
Lista de Amigos

La Lista de Amigos es una lista que contiene todas las direcciones de e-mail de las que quiere recibir mensajes, independientemente de su contenido. Los mensajes de sus amigos no serán marcados como spam, aunque su contenido tenga múltiples características del correo no solicitado.

Nota

Le recomendamos añadir los nombres y las direcciones de correo de sus amigos a la **Lista de Amigos**. BitDefender no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al añadir a sus conocidos en la Lista de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.

Para gestionar la **Lista de Amigos** haga clic en el símbolo (correspondiente a la **Lista de Amigos**) o haga clic en el botón **Amigos** ubicado en la Barra de herramientas Antispam.



Lista de Amigos

Aquí puede añadir o eliminar entradas en la **Lista de Amigos**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego clic en el botón . La dirección aparecerá en la **Lista de Amigos**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Amigos**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *com - todos mensajes con estos sufijos de dominio com llegarán a su **Bandeja de Entrada** independientemente de su contenido;

Para eliminar un objeto de la lista, selecciónelo y haga clic en el botón **Eliminar**. Si hace clic en botón **Limpiar** eliminará todas las entradas de la lista y será imposible recuperarlas.

Use los botones **Guardar**/ **Cargar** para guardar/cargar la **Lista de amigos** en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

Para resetear el contenido de la lista actual cuando carga una lista previamente guardada seleccione **Vaciar lista al cargar**.

Nota
Recomendamos añadir los nombres y las direcciones de correo de sus amigos la **Lista de Amigos**. BitDefender no bloquea los mensajes que provienen de esta la lista; de manera que al añadir a sus amigos a esta lista se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.

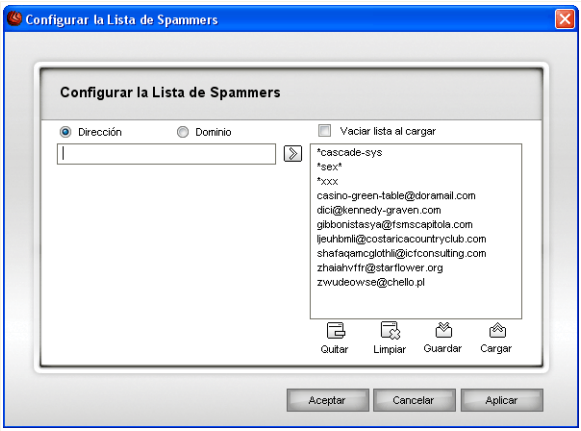
Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar la **Lista de Amigos**.

Lista de Spammers

La **Lista de Spammers** es una lista que contiene todas las direcciones de e-mail cuyos mensajes no desea recibir, independientemente de su contenido.

Nota
Cualquier mensaje proveniente de una dirección incluida en su **Lista de Spammers** será automáticamente marcado como spam.

Para gestionar la **Lista de Spammers** haga clic en el símbolo (correspondiente la **Lista de Spammers**) o haga clic en el botón **Spammers** ubicado en la Barra de herramientas Antispam.



Lista de Spammers

Aquí puede añadir o eliminar entradas en el **Lista de Spammers**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego clic en el botón . La dirección aparecerá en el **Lista de Spammers**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Spammers**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com serán marcados como SPAM;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- *com - todos mensajes con estos sufijos de dominio com serán marcados como SPAM.

Para eliminar un objeto de la lista, selecciónelo y haga clic en el botón **Eliminar**. Si hace clic en botón **Limpiar** eliminará todas las entradas de la lista y será imposible recuperarlas.

Use los botones **Guardar**/ **Cargar** para guardar / cargar la **Lista de Spammers** en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

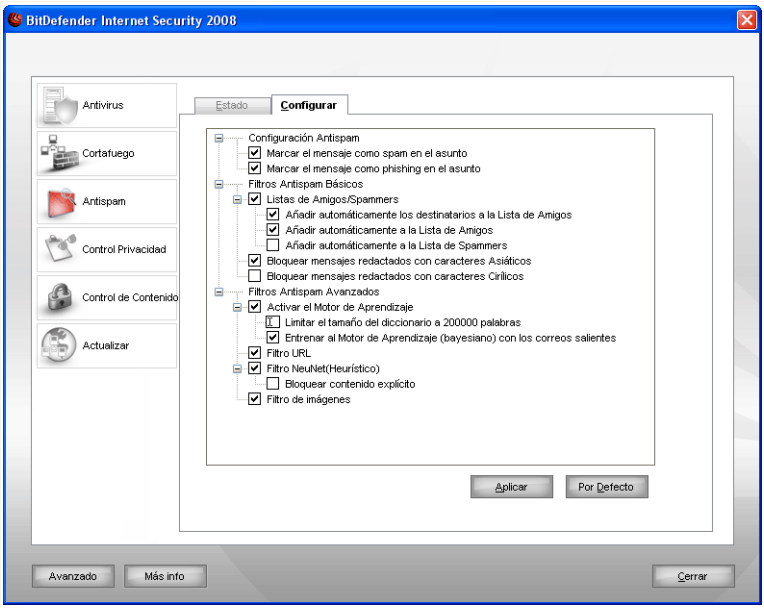
Para resetear el contenido de la lista actual cuando carga una lista previamente guardada seleccione **Vaciar lista al cargar**.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar la **Lista de Spammers**.

Importante
Si quiere reinstalar BitDefender le recomendamos primeramente guardar los listados de **Amigos** / **Spammers** y después de la finalización proceso de reinstalación volver a cargarlos.

10.3. Configuración Antispam

Para modificar la configuración del antispam, haga clic en **Antispam > Configuración** en la consola de configuración. Aparecerá la siguiente pantalla:



Configuración Antispam

Aquí puede activar/desactivar cada uno de los filtros Antispam, y puede modificar otras opciones relativas al módulo Antispam.

Hay 3 categorías de opciones disponibles (**Configuración Antispam**, **Filtros Antispam Básicos** y **Filtros Antispam Avanzados**) organizados en un menú expandible, similar a los menús de Windows.

Nota
Haga clic en la casilla marcada "+" para abrir una categoría, o en la casilla marcada "-" para cerrar una categoría.

10.3.1. Configuración Antispam

- **Marcar el mensaje como spam en el asunto** - si selecciona esta opción todos los mensajes considerados Spam serán marcados con Spam en el asunto.
- **Marcar el mensaje como phishing en el asunto** - todos los correos considerados como phishing se marcarán como SPAM en el Asunto.

10.3.2. Filtros Antispam Avanzados

- **Listados de Amigos / Spammers** - activa/desactiva los filtros basados en los Listados de Amigos / Spammers.
  - **Añadir automáticamente a la Lista de Amigos** - para añadir los remitentes a la **Lista de Amigos**.
  - **Añadir automáticamente a la Lista de Amigos** - la próxima vez que hace clic en el botón **No Spam** de la "*La barra de herramientas Antispam*" (p. 126) el remitente será añadido automáticamente a la **Lista de Amigos**.
  - **Añadir automáticamente a la Lista de Spammers** - la próxima vez que hace clic en el botón **Es Spam** de la "*La barra de herramientas Antispam*" (p. 126) el remitente será añadido automáticamente al **Lista de Spammers**.

Nota
Los botones **No Spam** y **Es Spam** están empleados para educar el filtro Bayesiano.

- **Bloquear mensajes redactados con caracteres Asiáticos** - bloquea los mensajes redactados con caracteres Asiáticos.
- **Bloquear mensajes redactados con caracteres Cirílicos** - bloquea los mensajes redactados con caracteres Cirílicos.

10.3.3. Filtros Antispam Avanzados

- **Activar el Motor de Aprendizaje** - activa/desactiva el Motor de Aprendizaje.
  - **Limitar el tamaño del diccionario a 200000 palabras** - esta opción le ofrece la posibilidad de configurar el tamaño del diccionario Bayesiano - reducido funciona más rápido, enriquecido tiene mayor precisión.

Nota
El tamaño recomendado es de: 200.000 palabras.

  - **Entrenar el Motor de Aprendizaje con correos salientes** - entrena el Motor de Aprendizaje con correos salientes.
- **Filtro URL** - activa/desactiva el Filtro URL.
- **Filtro NeuNet(Heurístico)** - activa/desactiva el Filtro NeuNet(Heurístico).
  - **Bloquear contenido explícito** - activa/desactiva la detección de mensajes con SEXUALLY EXPLICIT en la línea Asunto.
- **Filtro de imágenes** - activa/desactiva el Filtro de imágenes.

Nota
Para activar/desactivar una opción, seleccione/desmarque la casilla correspondiente.

Haga clic en **Aplicar** para guardar los cambios realizados o en **Por defecto** para cargar la configuración inicial.

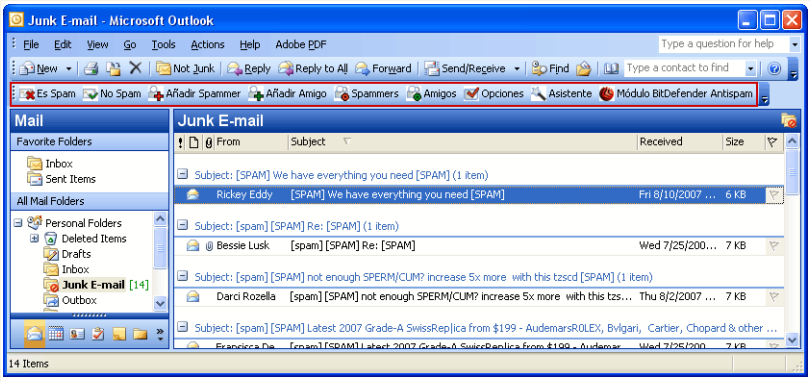
10.4. Integración en Clientes de Correo

BitDefender se integra directamente mediante una intuitiva interfaz y de muy fácil de usar en los siguientes clientes:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

10.4.1. La barra de herramientas Antispam

En la parte superior de su cliente de correo podrá ver la barra de herramientas Antispam.



La barra de herramientas Antispam

Importante
La diferencia principal entre BitDefender Antispam para Microsoft Outlook y Outlook Express / Windows Mail, es que los mensajes SPAM son trasladados a la carpeta

Spam en Microsoft Outlook, y a la carpeta **Elementos Eliminados** en Outlook Express. En ambos casos, los mensajes están marcados como SPAM en el asunto del mensaje.

La carpeta **Spam** creada por BitDefender Antispam para Microsoft Outlook se encuentra listada en el mismo nivel que los elementos del **listado de carpetas**(Calendario, Contactos, etc).

Cada botón será explicado a continuación:

- **Es Spam** - envia un mensaje al módulo Bayesiano indicándole que dicho mensaje es spam. El mensaje seleccionado será trasladado a la carpeta **Spam**.

  Los próximos mensajes con las mismas características serán marcados como SPAM.

  Nota
  Puede seleccionar un mensaje o todos los mensajes que desee.

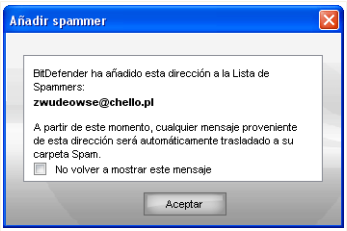
- **No Spam** - envia un mensaje al módulo Bayesiano indicándole que dicho mensaje no es spam y que BitDefender no tendría que marcarlo como tal. El mensaje se moverá de la carpeta **Spam** a la **Bandeja de Entrada**.

  Los próximos mensajes con las mismas características ya no serán marcados como SPAM.

  Nota
  Puede seleccionar un mensaje o todos los mensajes que desee.

  Importante
  El botón **No Spam** se activa al seleccionar un mensaje marcado como spam por BitDefender (normalmente, estos mensajes se almacenan en la carpeta **Spam**).

- **Añadir Spammer** - agrega el remitente de los mensajes seleccionados a la **Lista de Spammers**.



Añadir Spammer

Seleccione **No volver a mostrar este mensaje** si no quiere que se le solicite la confirmación al añadir una nueva dirección a la lista de spammers.

Haga clic en **Aceptar** para cerrar la ventana.

Los próximos mensajes provenientes de esa dirección serán automáticamente trasladados a la carpeta SPAM.

Nota
Puede seleccionar un remitente o todos los remitentes que desee.

- **Añadir Amigo** - agrega el remitente de los mensajes seleccionados a la **Lista de Amigos**.

Añadir Amigo

Seleccione **No volver a mostrar este mensaje** si no quiere que se le solicite la confirmación al añadir una nueva dirección a la lista de amigos.

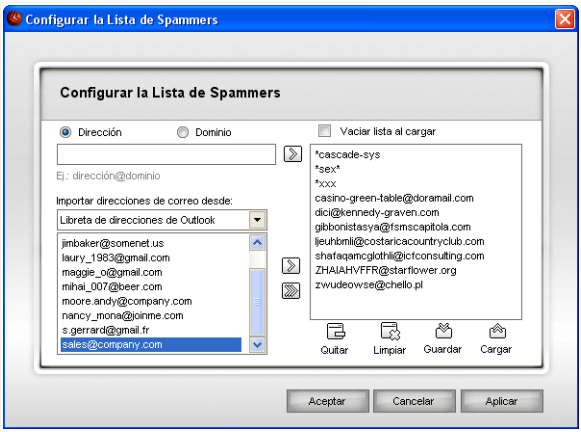
Haga clic en **Aceptar** para cerrar la ventana.

A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.

Nota
Puede seleccionar un remitente o todos los remitentes que desee.

- **Spammers** - haga clic en este botón para administrar la **Lista de Spammers** que contiene todas las direcciones de correo electrónico de las cuales no quiere recibir mensajes, independientemente de su contenido.

Nota
Cualquier mensaje proveniente de una dirección incluida en su **Lista de Spammers** será automáticamente marcado como spam.



Lista de Spammers

Aquí puede añadir o eliminar entradas en el **Lista de Spammers**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego clic en el botón . La dirección aparecerá en la **Lista de Spammers**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Spammers**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com serán marcados como SPAM;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- *com - todos mensajes con estos sufijos de dominio com serán marcados como SPAM.

Para exportar las direcciones de e-mail de la **Libreta de Direcciones de Windows** / **Carpetas de Outlook Express** en **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, seleccione la opción apropiada del menú desplegable **Importar direcciones de correo desde:**.

En **Microsoft Outlook Express / Windows Mail**, aparecerá una nueva ventana desde la que podrá indicar la carpeta que contiene las direcciones de correo que quiere añadir a la **lista de Spammers**. Selecciónela y haga clic en **Seleccionar**.

En ambos casos la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las preferidas y haga clic en para agregarlas a la **Lista de Spammers**. Si hace clic en todas las direcciones de e-mail serán añadidas al listado.

Para eliminar un objeto de la lista, selecciónelo y haga clic en el botón **Eliminar**. Si hace clic en botón **Limpiar** eliminará todas las entradas de la lista y será imposible recuperarlas.

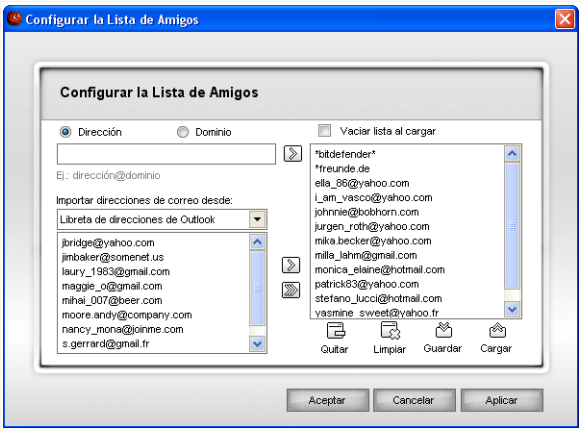
Use los botones **Guardar**/ **Cargar** para guardar / cargar la **Lista de Spammers** en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

Para resetear el contenido de la lista actual cuando carga una lista previamente guardada seleccione **Vaciar lista al cargar**.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar la **Lista de Spammers**.

- **Amigos** - haga clic en este botón para administrar la **Lista de Amigos** que contiene todas las direcciones desde las que siempre quiere recibir mensajes, independientemente de su contenido.

> ***Nota***
> Le recomendamos añadir los nombres y las direcciones de correo de sus amigos a la **Lista de Amigos**. BitDefender no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al añadir a sus conocidos en la Lista de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.



Lista de Amigos

Aquí puede añadir o eliminar entradas en la **Lista de Amigos**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego haga clic en el botón . La dirección aparecerá en la **Lista de Amigos**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en el **Lista de Amigos**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *com - todos mensajes con estos sufijos de dominio com llegarán a su **Bandeja de Entrada** independientemente de su contenido;

Para exportar las direcciones de e-mail de la **Libreta de Direcciones de Windows** / **Carpetas de Outlook Express** en **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, seleccione la opción apropiada del menú desplegable **Importar direcciones de correo desde:**.

En **Microsoft Outlook Express / Windows Mail** aparecerá una nueva ventana desde la que podrá indicar la carpeta que contiene las direcciones de correo que quiere añadir a la **Lista de Amigos**. Selecciónela y haga clic en **Seleccionar**.

En ambos casos la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las preferidas y haga clic en para añadirlas a la **Lista de Amigos**. Si hace clic en todas las direcciones de e-mail serán añadidas al listado.

Para eliminar un objeto de la lista, selecciónelo y haga clic en el botón **Eliminar**. Si hace clic en botón **Limpiar** eliminará todas las entradas de la lista y será imposible recuperarlas.

Use los botones **Guardar**/ **Cargar** para guardar/cargar la **Lista de amigos** en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

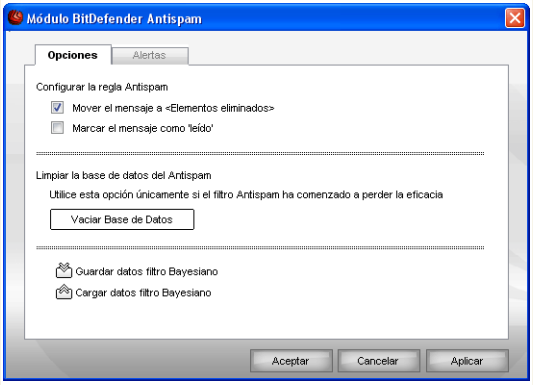
Para resetear el contenido de la lista actual cuando carga una lista previamente guardada seleccione **Vaciar lista al cargar**.

Nota

Recomendamos añadir los nombres y las direcciones de correo de sus amigos la **Lista de Amigos**. BitDefender no bloquea los mensajes que provienen de esta la lista; de manera que al añadir a sus amigos a esta lista se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar la **Lista de Amigos**.

- **Configuración** - abre la ventana **Configuración** en la que puede especificar algunas opciones del módulo **Antispam**.



Configuración

Dispone de las siguientes opciones:

- **Mover el mensaje a Elementos Eliminados** - para trasladar los mensajes Spam a la carpeta **Elementos Eliminados** (sólo para Microsoft Outlook Express / Windows Mail);
- **Marcar el mensaje como 'leído'** - para marcar todos los mensajes Spam como leídos, para que así los nuevos mensajes Spam no le molesten al llegar.

Si su filtro antispam es muy inexacto, es posible que necesite vaciar la base de datos y reeducar el Filtro Bayesiano. Haga clic en **Limpiar la base de datos del Antispam** si quiere restaurar la base de datos del filtro Bayesiano.

Use los botones **Guardar datos filtro Bayesiano**/ **Cargar datos filtro Bayesiano** para guardar/cargar la Base de datos del filtro bayesiana en la ubicación deseada. El archivo tendrá la extensión `.dat`.

Haga clic en la pestaña **Alertas** si quiere acceder al apartado desde dónde puede desactivar la aparición de las ventanas de confirmación de los botones **Añadir Spammer** y **Añadir Amigo**.

Nota

En la ventana de **Alerta** puede activar/desactivar la aparición de la alerta **Por favor seleccione un mensaje de correo**. Esta alerta aparece cuando selecciona un grupo en lugar de un mensaje de correo.

- **Asistente** - haga clic en este botón para que se inicie el asistente que le guiará a través del proceso de educación del Filtro Bayesiano, para así mejorar la eficiencia

de BitDefender Antispam. También puede añadir direcciones de su **Libreta de direcciones** a la **Lista de Amigos** / **Lista de Spammers**.

- **BitDefender Antispam** - haga clic en este botón para abrir la Consola de Administración.

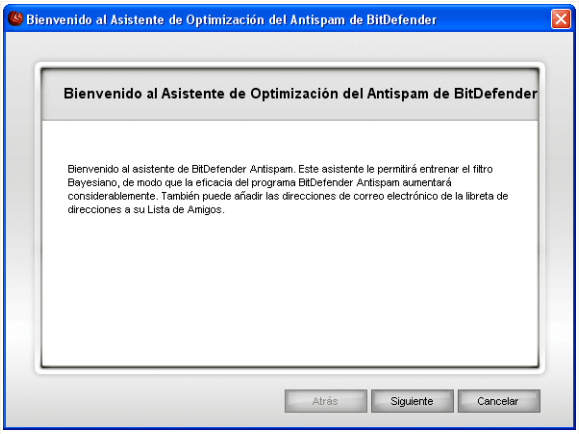
10.4.2. El asistente de configuración Antispam

La primera vez que inicie su cliente de correo después de la instalación de BitDefender, aparecerá un asistente de bienvenida que le ayudará a configurar la Lista de Amigos y Lista de Spammers y entrenar el Filtro Bayesiano, que mejorarán la eficiencia de los filtros Antispam.

Nota

Puede ejecutar el asistente cuando quiera, haciendo click en **Asistente** en la Barra de Herramientas Antispam.

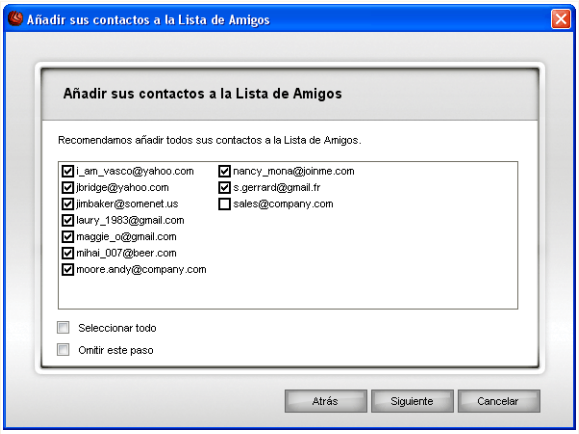
Paso 1/6 - Ventana de bienvenida



Ventana de Bienvenida

Haga clic en **Siguiente**.

Paso 2/6 - Completar la Lista de Amigos



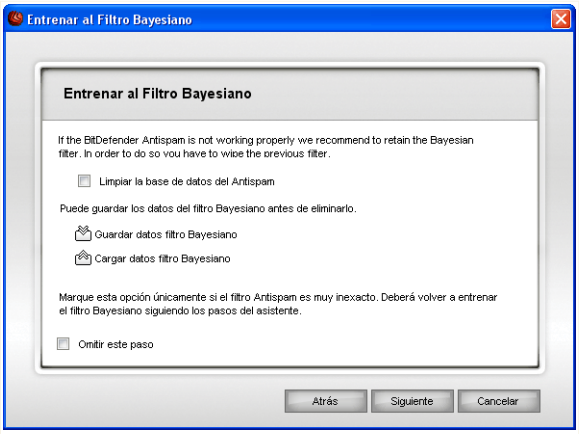
Completar la Lista de Amigos

Aquí puede ver todas las direcciones de su **Libreta de Direcciones**. Por favor seleccione las que quiere añadir a la **Lista de Amigos** (le recomendamos seleccionarlas todas). Recibirá todos los mensajes de estas direcciones, independientemente de su contenido.

Para añadir sus contactos a la Lista de Amigos, compruebe **Seleccionar Todo**.

Seleccione **Omitir este paso** si quiere saltarse este paso. Haga clic en **Atrás** para volver al paso anterior o en **Siguiente** para seguir.

Paso 3/6 - Borrar la base de datos del filtro Bayesiano



Eliminar la base de datos del filtro Bayesiano

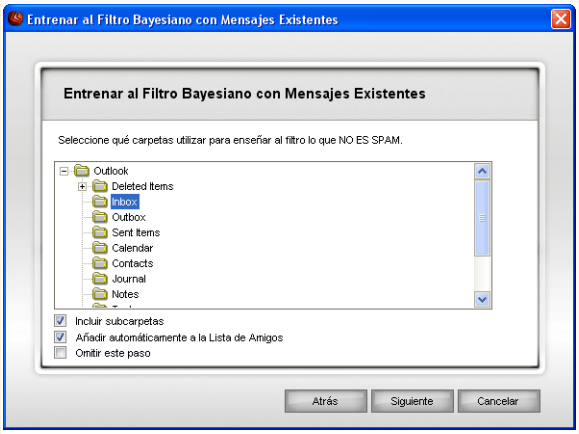
Si nota que su filtro antispam está empezando a perder su eficiencia, esto se puede deber a una educación inadecuada (por ejemplo, usted ha marcado erróneamente un número de mensajes legítimos como Spam, o viceversa). Si su filtro es muy impreciso, talvez tenga que borrar toda la base de datos del filtro y reeducar el filtro siguiendo los pasos indicados por el programa asistente, tal como se describe a continuación.

Seleccione **Limpiar la base de datos del filtro Antispam** si quiere vaciar la base de datos del filtro bayesiano.

Use los botones **Guardar datos filtro Bayesiano**/**Cargar datos filtro Bayesiano** para guardar/cargar la Base de datos del filtro Bayesiano en la ubicación que desee. El archivo tendrá una extensión `.dat`.

Seleccione **Omitir este paso** si quiere saltarse este paso. Haga clic en **Atrás** para volver al paso anterior o en **Siguiente** para seguir.

Paso 4/6 - Entrenar el Motor de Aprendizaje con Mensajes Legítimos



Entrenar el Motor de Aprendizaje con Mensajes Legítimos

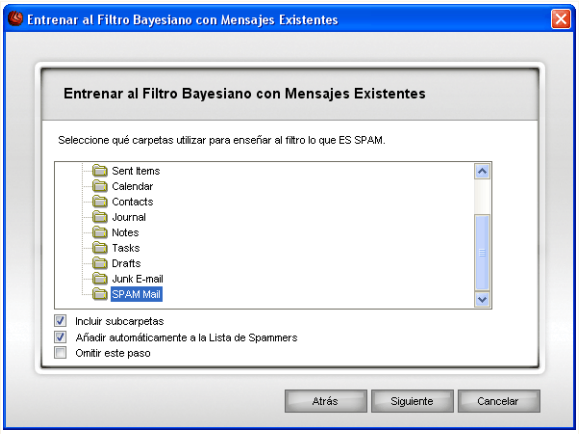
Por favor seleccione una carpeta que contiene mensajes legítimos. Estos mensajes serán utilizados para educar el filtro antispam.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir subcarpetas** - para incluir las subcarpetas en su selección.
- **Añadir automáticamente a la Lista de Amigos** - para añadir los remitentes a la **Lista de Amigos**.

Seleccione **Omitir este paso** si quiere saltarse este paso. Haga clic en **Atrás** para volver al paso anterior o en **Siguiente** para seguir.

Paso 5/6 - Entrenar el Filtro Bayesiano con Spam



Entrenar el Filtro Bayesiano con Spam

Por favor seleccione una carpeta que contiene mensajes Spam. Estos mensajes serán empleados para educar el filtro Antispam.

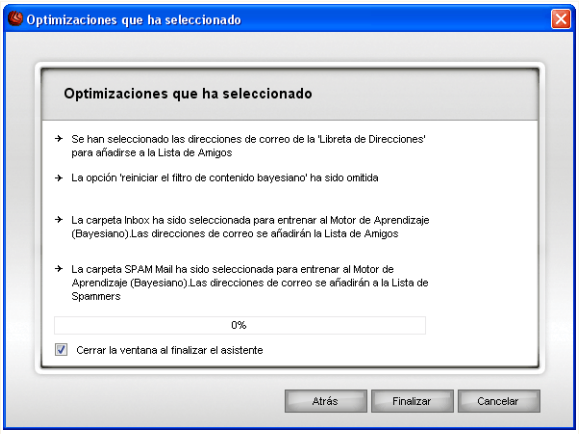
Importante
Por favor asegúrese que la carpeta seleccionada no contiene ningún mensaje legítimo, sino la eficiencia del filtro antispam se verá reducida considerablemente.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir subcarpetas** - para incluir las subcarpetas en su selección.
- **Añadir automáticamente a la Lista de Spammers** - para añadir los remitentes a la **Lista de Spammers**.

Seleccione **Omitir este paso** si quiere saltarse este paso. Haga clic en **Atrás** para volver al paso anterior o en **Siguiente** para seguir.

Paso 6/6 - Epílogo



Resumen

En esta ventana se muestran todas las opciones para el programa asistente. Puede hacer cualquier modificación que considere oportuna, volviendo al paso anterior (haga clic en **Atrás**).

Si no quiere hacer ninguna modificación, haga clic en **Finalizar** para cerrar el asistente.

11. Control de Privacidad

BitDefender monitoriza docenas de puntos clave potenciales en su sistema dónde puede actuar el spyware, y también comprueba cualquier cambio que se haya producido en el sistema o software. Su función es bloquear troyanos u otras herramientas instaladas por hackers, que intenten comprometer su privacidad y envien información personal (como números de tarjetas de crédito) desde su equipo hacia el hacker.

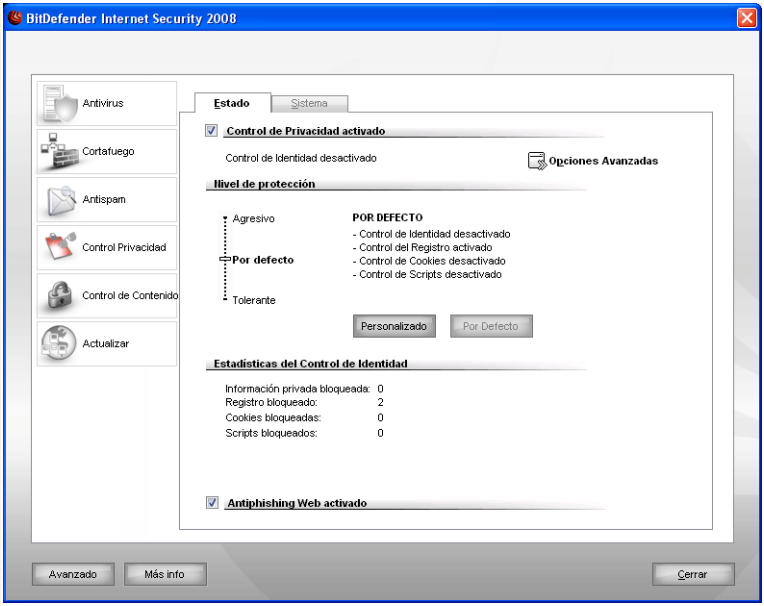
BitDefender también analiza las páginas web que visita y le alerta si detecta alguna amenaza tipo phishing.

El apartado **Control de Privacidad** de esta guía contiene los siguientes temas:

- Estado del Control de Privacidad
- Opciones Avanzadas - Control de Identidad
- Opciones Avanzadas - Control del Registro
- Opciones Avanzadas - Control de las Cookies
- Opciones Avanzadas - Control de Scripts
- Información del sistema
- Barra de Heramientas Antiphishing

11.1. Estado del Control de Privacidad

Para configurar el Control de Privacidad y ver información relacionada con su actividad, haga clic **Control Privacidad > Estado** en la consola de configuración. Aparecerá la siguiente pantalla:



Estado del Control de Privacidad

11.1.1. Control de Privacidad

Importante
Para impedir el robo de datos y proteger su privacidad, mantenga activado el **Control de Privacidad**.

El Control de Privacidad protege su equipo a través de 5 importantes controles de protección:

- Control de Identidad - protege sus datos confidenciales filtrando todo el tráfico HTTP y SMTP saliente según las reglas creadas en el apartado Identidad.

Nota
En la parte inferior de este apartado puede ver las **Estadísticas del Control de Identidad**.

- Control del Registro - le pedirá permiso cada vez que un programa intente modificar un entrada del registro y así ejecutarse cuando inicie Windows.
- Control de Cookies - le pedirá permiso cada vez que una nueva página web intente guardar una cookie.
- Control de Scripts - le pedirá permiso cada vez que una página web intente activar un script u otro tipo contenido activo.

Para configurar las opciones para estos controles haga clic en Opciones Avanzadas.

Configurando el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel adecuado de protección.

Hay 3 niveles de seguridad:

Nivel de Protección	*Descripción*
Tolerante	Sólo el **Control del Registro** está activado.
Por Defecto	El **Control del Registro** y **Control de Identidad** están activados.
Agresivo	El **Control del Registro**, el **Control de Identidad** y el **Control de Script** están activados.

Puede personalizar el nivel de protección haciendo clic en **Personalizado**. En ventana que aparecerá, seleccione los controles de protección que desea activar y haga clic en **Aceptar**.

Haga clic en **Por Defecto** para posicionar el deslizador en el nivel predeterminado.

11.1.2. Protección Antiphishing

El phishing es una actividad criminal que se realiza en Internet y que utiliza técnicas de ingeniería social para engañar a la gente y obtener información personal.

Los intentos de phishing normalmente se originan en correos masivos que fingen provenir de una empresa legítima y conocida. Estos mensajes engañosos se envían con la esperanza de que al menos, alguno de los destinatarios les facilite su información personal.

Los mensajes de phishing normalmente están relacionados con cuentas electrónicas. Intentan convencerle para que haga clic en el enlace que contiene el mensaje. Este enlace supuestamente le dirige a una página web legítima (que en realidad es una falsificación) dónde se le solicitará información privada. Por ejemplo, se le puede solicitar que confirme la información de su cuenta, como el nombre de usuario y la contraseña, su número de la seguridad social o su cuenta bancaria. En otras ocasiones, para ser más convincente, el mensaje pretende hacerle creer que su cuenta ha sido o será suspendida si no hace clic en el enlace incluido en el mensaje.

El phishing también utiliza spyware, como Trojan keyloggers, para robar información directamente desde su ordenador.

Los mayores objetivos del phishing son los clientes de plataformas de pago, como PayPal o eBay, o como los bancos que ofrecen servicios online. Recientemente, los usuarios de las páginas web de redes sociales también han sido objetivo del phishing, obteniendo datos personales de estos usuarios para robar sus identidades.

Para estar protegido contra los intentos phishing cuando navega por Internet, mantenga el módulo **Antiphishing** activado. De esta manera, BitDefender analizará cada una de las páginas web que visite y le alertará de la existencia de cualquier intento de phishing. Puede configurar la Lista Blanca de páginas web que no serán analizadas por BitDefender.

Para poder gestionar fácilmente la protección antiphishing y la Lista Blanca, utilice la barra de herramientas BitDefender Antiphishing integrada en Internet Explorer. Para más información, por favor, consulte el capítulo "*La Barra de Herramientas Antiphishing*" (p. 159).

11.2. Opciones Avanzadas - Control de Identidad

Mantener a salvo los datos personales es una cuestión que nos preocupa a todos. El robo de datos ha ido evolucionando al mismo ritmo que el desarrollo de las comunicaciones en Internet, utilizando nuevos métodos para engañar al usuario y conseguir su información privada.

Tanto si se trata de su dirección de e-mail o de su número de tarjeta de crédito, cuando esta información cae en manos equivocadas, puede ser dañina para usted: puede ahogarse entre una multitud de mensajes de spam o encontrarse vacía su cuenta bancaria.

El **Control de Identidad** le ayuda a mantener a salvo sus datos confidenciales. Analiza el tráfico HTTP o SMTP, o ambos, en busca de la información que indique. Si se

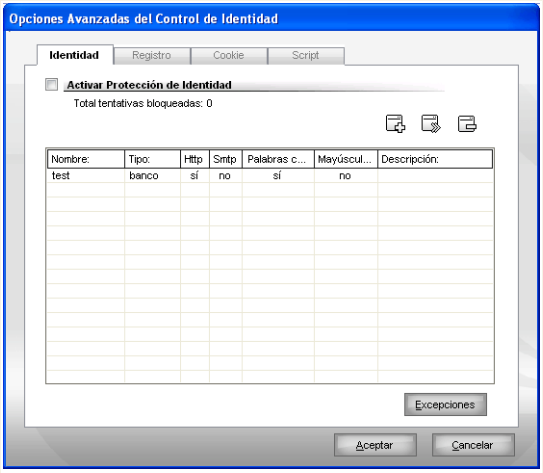
detecta alguna coincidencia, la página web o el mensaje que contenga dicha información correo será bloqueado.

BitDefender incluye soporte multiusuario, para que todos los otros usuarios del sistema puedan configurar sus propias reglas.

Las reglas de privacidad pueden configurarse en el apartado **Identidad**. Para acceder a este apartado, abra la ventana de **Opciones Avanzadas del Control de Privacidad** y haga clic en la pestaña **Identidad**.

Nota

Para abrir la ventana **Opciones Avanzadas del Control de Privacidad**, haga clic en **Control Privacidad > Estado** en la consola de configuración, y haga clic en **Opciones Avanzadas**.



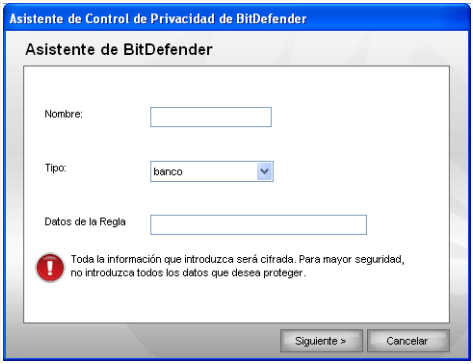
Control de Identidad

11.2.1. Creando Reglas de Identidad

Las reglas se tienen que introducir manualmente (haga clic en el botón **Añadir** y elija los parámetros para la regla). Se iniciará el asistente de configuración.

El asistente de configuración consta de 3 pasos.

Paso 1/3 - Seleccionar el tipo y atos de la regla



Seleccionar el tipo y datos de la regla

Introduzca el nombre de la regla en el campo editable.

Debe configurar los siguientes parámetros:

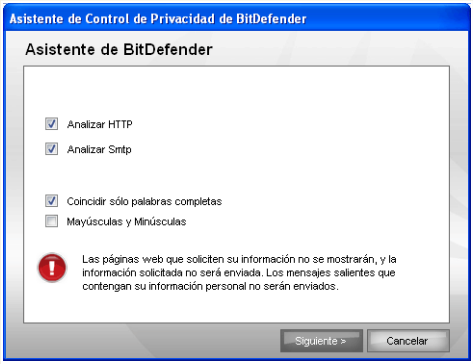
- **Tipo de Regla** - elija el tipo de regla (dirección, nombre, tarjeta de crédito, PIN, SSN etc).
- **Datos de la regla** - introduzca los datos de la regla.

> ***Nota***
> Si introduce menos de tres caracteres, se le pedirá que valide los datos. Recomendamos escribir por lo menos tres caracteres para evitar confusiones durante el bloqueo de mensajes y páginas web.

Todos los datos que introduzca serán cifrados. Para mayor seguridad, no introduzca todos los datos que desee proteger.

Haga clic en **Siguiente**.

Paso 2/3 - Seleccionar Tráfico



Seleccionar Tráfico

Debe seleccionar el tipo de tráfico que BitDefender analizará. Dispone de las siguientes opciones:

- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (mail) y bloquea los mensajes salientes que coinciden con los datos de la regla.

Puede elegir entre aplicar las reglas sólo si los datos de la regla coinciden completamente con las palabras, o si los datos de la regla y la cadena detectada coinciden.

Haga clic en **Siguiente**.

Paso 3/3 – Descripción de la regla

Describa la regla

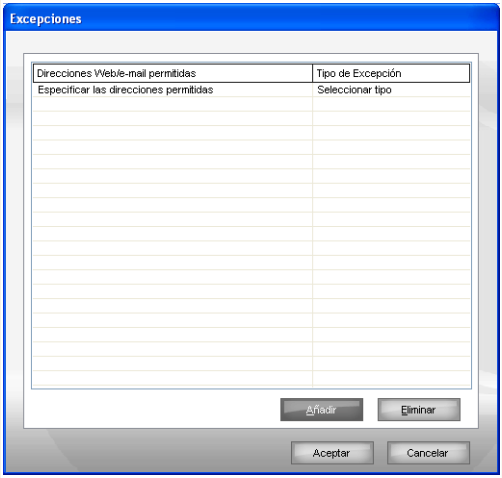
Introduzca una breve descripción de la regla en el campo editable.

Haga clic en **Finalizar**.

11.2.2. Definiendo las Excepciones

En algunos casos, es necesario crear excepciones a las reglas de identidad. Imaginemos que ha creado una regla para impedir el envío de su número de tarjeta de crédito en páginas web. En el momento que su número de tarjeta se envíe a una página web, la página en cuestión se bloqueará. Pero si realmente quisiera comprar una película DVD en una tienda online segura, tendría que crear una excepción para dicha regla.

Para abrir la ventana dónde puede crear excepciones, haga clic en **Excepciones**.



Excepciones

Para añadir una excepción, siga estos pasos:

1. Haga clic en **Añadir** para introducir una nueva entrada en la tabla.
2. Haga doble clic en **Especificar las direcciones permitidas** e introduzca la dirección de la página o correo electrónico que desea añadir como excepción.
3. Haga doble clic en **Seleccionar tipo** y en el menú, seleccione la opción correspondiente al tipo de dirección que ha introducido previamente.
   - Si ha introducido una página web, seleccione la opción **HTTP**.
   - Si ha introducido una dirección de e-mail, seleccione la opción **SMTP**.

Para eliminar una excepción de la lista, selecciónela y haga clic en **Eliminar**.

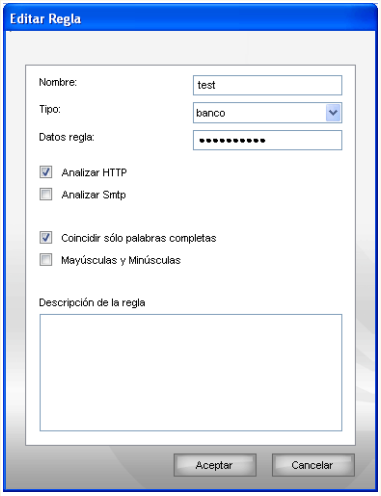
Haga clic en **Aplicar** para guardar los cambios.

11.2.3. Administrando Reglas

Puede ver las reglas listadas en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para desactivar una regla temporalmente sin eliminarla, desmarque la casilla correspondiente a la regla.

Para editar una regla, selecciónela y haga clic en el botón **Editar** o simplemente haga doble clic en la regla. Aparecerá una nueva ventana:



Editar regla

Aquí puede cambiar el nombre, la descripción y los parámetros de la regla (tipo, datos y tráfico). Haga clic en **Aceptar** para guardar los cambios.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

11.3. Opciones Avanzadas - Control del Registro

El **Registro** es un componente muy importante de Windows. El sistema operativo emplea el registro para guardar su configuración, los programas instalados, los datos del usuario etc.

El **Registro** también se utiliza para definir los programas que se deben iniciar automáticamente con cada inicio de Windows. Los virus utilizan esta funcionalidad para ejecutarse automáticamente cuando el usuario reinicia el ordenador.

El **Control del Registro** monitoriza toda la actividad del Registro Windows – acción que puede resultar muy útil para detectar Troyanos. Este módulo le advierte cada vez que un programa intenta modificar una entrada en el registro para poder ejecutarse con cada inicio del sistema.

Aviso de Registro

Para rechazar una modificación del registro, pulse **No**, si quiere permitirla elija **Sí**.

Si desea que BitDefender recuerde su respuesta, debe seleccionar la casilla: **Aplicar siempre esta acción para este programa**. Así, se creará una regla y se aplicará la misma acción cuando este programa intente modificar el registro para ejecutarse cuando inicie Windows.

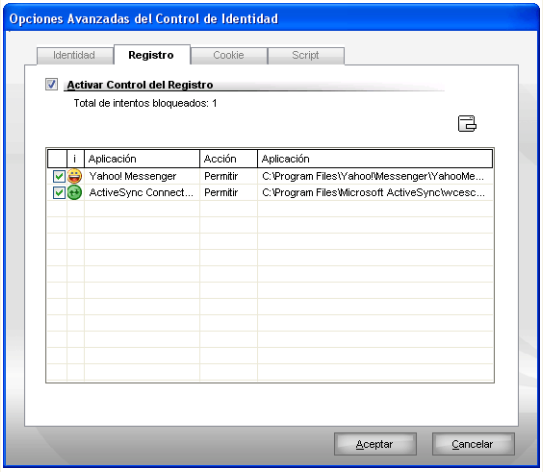
Nota

Generalmente, BitDefender le mostrará alertas cuando instale nuevos programas que necesitan iniciarse la próxima vez que reinicie el equipo. En la mayoría de los casos, estos programas son legítimos y de confianza.

Cada regla guardada puede consultarse en el apartado **Registro**. Para acceder a este apartado, abra la ventana de **Opciones Avanzadas del Control de Privacidad** y haga clic en la pestaña **Registro**.

Nota

Para abrir la ventana **Opciones Avanzadas del Control de Privacidad**, haga clic en **Control Privacidad > Estado** en la consola de configuración, y haga clic en **Opciones Avanzadas**.



Control del registro

Puede ver las reglas listadas hasta el momento en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para desactivar temporalmente una opción sin eliminarla, desmarque la casilla correspondiente.

Para modificar la acción de una regla, haga doble clic en el campo de acción y seleccione la opción apropiada en el menú desplegable.

Haga clic en **Aceptar** para cerrar la ventana.

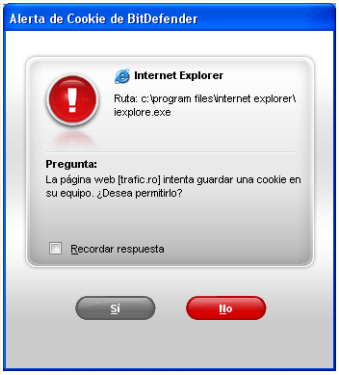
11.4. Opciones Avanzadas - Control de las Cookies

Las Cookies son elementos muy comunes en Internet. Se trata de pequeños ficheros almacenados en su sistema – los sitios web, por ejemplo, crean estas cookies para recoger determinada información sobre sus preferencias.

Las Cookies están hechas para hacerle la vida más fácil. Por ejemplo, pueden ayudar al sitio web "recordar" su nombre y preferencias, para que no tenga que introducir estos datos cada vez que visita aquella página.

Pero las cookies también pueden ser empleadas para comprometer su confidencialidad, al monitorizar sus preferencias mientras navega en Internet.

Para evitar estos casos, use nuestro **Control de cookie**. Si se lo mantiene activado, **Control de cookies** le pedirá la autorización cada vez que un nuevo sitio web intenta enviar una cookie:



Alerta de Cookie

Podrá ver el nombre de la aplicación que trata de enviar la cookie.

Marque la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No**, para crear una nueva regla de permiso, que se aplicará y aparecerá en la tabla de reglas. La próxima vez que se conecte al mismo sitio no recibirá esta notificación.

Esto le ayudará a decidir cuáles son los sitios web de confianza y cuáles no.

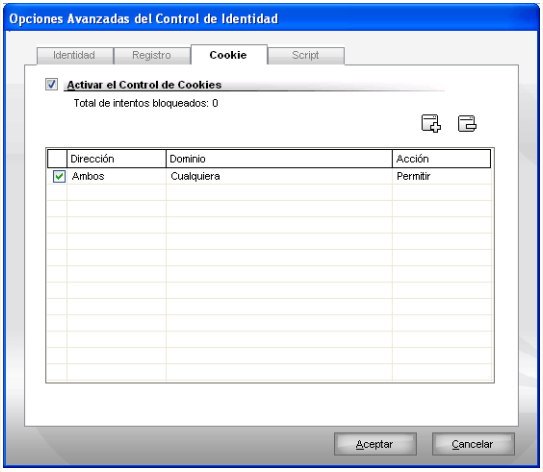
Nota

Debido al gran número de cookies empleadas hoy en día en Internet, el **Control de Cookie** puede resultar un poco molesto al principio. Recibirá muchas preguntas sobre los sitios que intentan enviar cookies a su ordenador. Pero, en cuanto agregue los sitios de confianza al listado de reglas, el proceso de navegación en Internet volverá a ser tan fácil como antes.

Cada regla guardada puede ser modificada desde el apartado **Cookies**. Para acceder a este apartado, abra la ventana de **Opciones Avanzadas del Control de Privacidad** y haga clic en la pestaña **Cookie**.

Nota

Para abrir la ventana **Opciones Avanzadas del Control de Privacidad**, haga clic en **Control Privacidad > Estado** en la consola de configuración, y haga clic en **Opciones Avanzadas**.



Control de las Cookies

Puede ver las reglas listadas hasta el momento en la tabla.

Importante
Las reglas se muestran por orden de prioridad, de mayor a menor prioridad. Puede arrastrar y soltar las reglas para modificar su orden de prioridad.

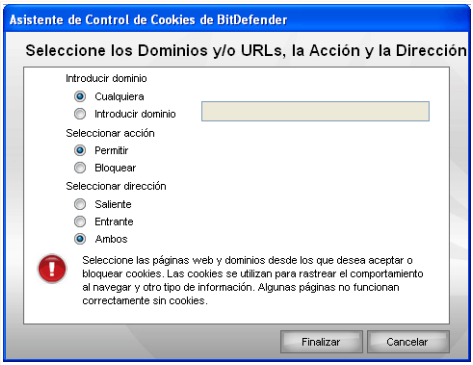
Para eliminar una regla, simplemente selecciónela y pulse **Eliminar**. Para modificar los atributos de una regla, haga doble clic en el campo correspondiente. Para desactivar temporalmente una regla sin eliminarla, desmarque la casilla correspondiente.

Las reglas pueden ser introducidas automáticamente (mediante la ventana de alerta) o manualmente (haga clic en **Añadir** y elija los parámetros para la nueva regla). Aparecerá el programa de configuración.

11.4.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 - Seleccionar los Dominios y/o URLs, Acción y Dirección



Seleccionar los Dominios y/o URLs, Acción y Dirección

Puede configurar los parámetros:

- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

- **Dirección** - seleccione la dirección del tráfico.

Tipo	Descripción
Saliente	La regla será aplicada sólo a las cookies enviadas al sitio web iindicado.
Entrante	La regla será aplicada sólo a las cookies recibidas desde el sitio web indicado.
Ambos	La regla aplicará en ambas direcciones.

Haga clic en **Finalizar**.

Nota
Puede aceptar, cookies pero nunca debe enviarlas. Para bloquear su envío, cambie la acción a **Bloquear** y la dirección a **Saliente**.

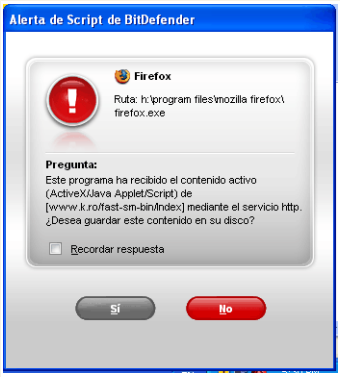
Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

11.5. Opciones Avanzadas - Control de Scripts

Los Scripts y otros códigos, como los Controles ActiveX y los Applets de Java, se utilizan para crear páginas web interactivas, aunque también pueden ser programados para tener efectos dañinos. Los elementos ActiveX, por ejemplo, pueden obtener el acceso total a sus datos y, por consiguiente, pueden leer los datos de su ordenador, borrar información, copiar contraseñas e interceptar mensajes mientras está conectado a Internet. Sólo debería aceptar contenido activo de las webs que conozca y sean de confianza.

BitDefender le permite elegir entre ejecutar o bloquear estos elementos.

Con el **Control del Script** usted decide cuáles son los sitios web de confianza. BitDefender le pedirá una confirmación cada vez que un sitio intente activar un script u otro contenido activos:



Alerta de Script

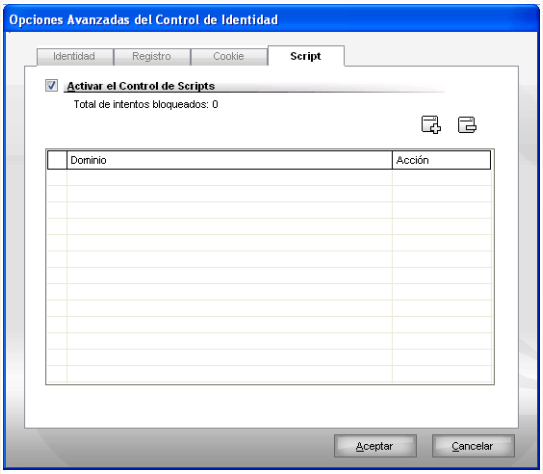
Puede ver el nombre del recurso.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No** para crear una nueva regla de permiso, que será listada en la tabla de reglas. A partir de este momento, no recibirá más notificaciones cuando el mismo sitio intente enviarle contenido activo.

Cada regla guardada puede ser modificada desde el apartado **Script**. Para acceder a este apartado, haga clic en la ventana **Opciones Avanzadas del Control de Privacidad** y haga clic en la pestaña **Scripts**.

Nota

Para abrir la ventana **Opciones Avanzadas del Control de Privacidad**, haga clic en **Control Privacidad > Estado** en la consola de configuración, y haga clic en **Opciones Avanzadas**.



Control de Script

Puede ver las reglas listadas hasta el momento en la tabla.

Importante

Las reglas se muestran por orden de prioridad, de mayor a menor prioridad. Puede arrastrar y soltar las reglas para modificar su orden de prioridad.

Para eliminar una regla, simplemente selecciónela y pulse **Eliminar**. Para modificar los atributos de una regla, haga doble clic en el campo correspondiente. Para desactivar temporalmente una regla sin eliminarla, desmarque la casilla correspondiente.

Las reglas pueden ser introducidas automáticamente (mediante la ventana de alerta) o manualmente (haga clic en **Añadir** y elija los parámetros para la nueva regla). Aparecerá el programa de configuración.

11.5.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 - Seleccione la Dirección y la Acción

Seleccione la Dirección y la Acción

Puede configurar los parámetros:

- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

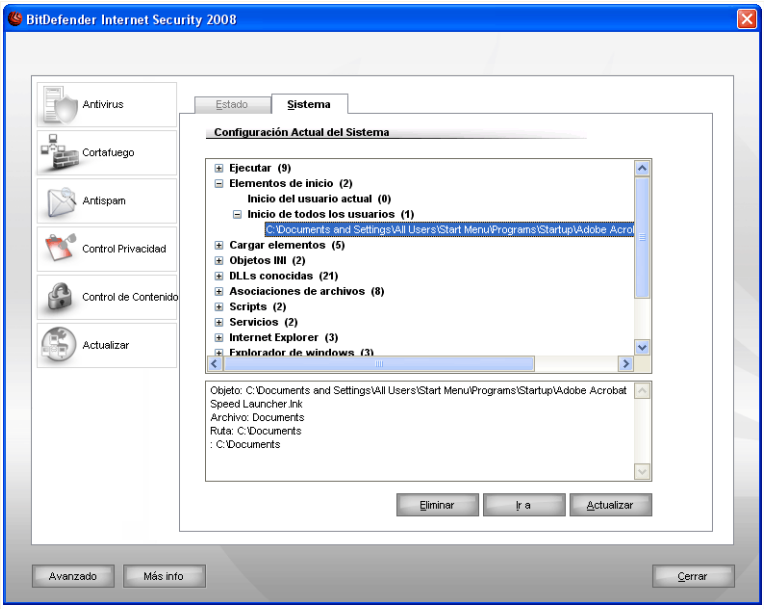
Haga clic en **Finalizar**.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

11.6. Información del Sistema

BitDefender le permite ver, desde una sola ventana, todas las opciones y aplicaciones registradas para ejecutarse al iniciar el sistema. De esta manera, podrá monitorizar la actividad del sistema y de las aplicaciones instaladas, así como identificar posibles infecciones del sistema.

Para obtener información del sistema, haga clic en **Control Privacidad > Sistema** en la consola de configuración. Aparecerá la siguiente pantalla:



Información del Sistema

La lista contiene todos los objetos cargados al iniciar el sistema así como los objetos cargados por diferentes aplicaciones.

Hay tres botones disponibles:

- **Eliminar** - elimina el objeto seleccionado. Debe hacer clic en **Si** para confirmar su elección.

Nota
Si no desea que se le pregunte de nuevo durante la sesión en curso, marque la casilla **No volver a preguntar durante esta sesión**.

- **Ir a** - abre una ventana donde el objeto seleccionado es colocado (el **Registro** por ejemplo).
- **Actualizar** - re-abre el apartado **Sistema**.

Nota
Según el elemento seleccionado, aparecerán uno o los dos botones: **Eliminar** o **Ir a**.

11.7. La Barra de Herramientas Antiphishing

BitDefender le protege contra los intentos de phishing mientras navega por Internet. Analiza las páginas web a las que accede y le alerta si detecta alguna amenaza de phishing. Puede configurar la Lista Blanca de páginas web que no serán analizadas por BitDefender.

Puede administrar de forma fácil y eficaz la protección antiphishing y la Lista Blanca usando la barra de herramientas de BitDefender Antiphishing integrada en Internet Explorer.

La barra de herramientas antiphishing, representada por el **icono de BitDefender**, está situada en la parte superior de Internet Explorer. Haga clic para abrir el menú de la barra de herramientas.

Nota
Si no puede ver la barra de herramientas, abra el menú **Ver**, diríjase a la opción **barras de herramientas** y marque la opción **BitDefender Toolbar**.

La Barra de Herramientas Antiphishing

Dispone de los siguientes comandos en la barra de herramientas:

- **Activar / Desactivar** - activa / desactiva la Barra de Herramientas Antiphishing de BitDefender.

  Nota
  Si decide desactivar la barra de herramientas Antiphishing, no estará protegido contra los intentos de phishing.

- **Opciones** - abre una ventana dónde puede modificar la configuración de la barra de herramientas.

  Dispone de las siguientes opciones:
  - **Activar Análisis** - activa el análisis antiphishing.
  - **Preguntar antes de añadir a la lista blanca** - se le preguntará si está seguro de añadir la página web en la Lista Blanca.

- **Añadir a la Lista Blanca** - añade la página web actual a la Lista Blanca.

  Nota
  Añadir una página web a la Lista Blanca significa que BitDefender no analizará nunca más la página en busca de intentos de phishing. Recomendamos añadir a la Lista Blanca sólo las páginas en las que confíe plenamente.

- **Ver Lista Blanca** - abre la Lista Blanca.

  Puede ver la lista de todas las páginas web que no serán analizadas por los motores antiphishing de BitDefender.

Si desea eliminar una página web de la Lista Blanca, para detectar los posibles intentos de phishing existentes en la página, haga clic en el botón **Eliminar** situado justo al lado.

Puede añadir las páginas en las que confíe a la Lista Blanca, de modo que no sean analizadas por los motores antiphishing. Para añadir una página a la Lista Blanca, escriba la dirección en la casilla correspondiente y haga clic en **Añadir**.

- **Ayuda** - abre el archivo de ayuda.
- **Acerca de** - abre la ventana dónde puede verse información sobre BitDefender y dónde encontrar ayuda en caso necesario.

12. Control de Contenido

El módulo Control de Contenido puede bloquear el acceso a:

- páginas web inapropiadas.
- la conexión a Internet durante determinados periodos de tiempo (como en los momentos de estudio).
- páginas web y mensajes de correo electrónico que contengan determinadas palabras.
- aplicaciones como juegos, chat, aplicaciones de intercambio de archivos u otros.

Importante
Este módulo sólo es accesible y configurable por los usuarios con permisos de administrador (administradores del sistema). Si la configuración está protegida por contraseña, sólo podrán modificarse una vez se haya proporcionado la contraseña. Un administrador no puede imponer un conjunto de reglas a un usuario al que ya se hayan definido las reglas por otro administrador.

El apartado **Control de Contenido** de esta guía de usuario contiene los siguientes temas:

- Protegiendo la Configuración del Control de Contenido
- Estado del Control de Contenido
- Control Web
- Control de Aplicaciones
- Filtro de palabras clave
- Limitador de Tiempo Web

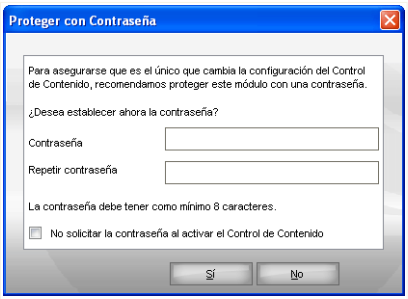
12.1. Protegiendo la Configuración del Control de Contenido

Si no es el único usuario con permisos de administrador que utiliza este ordenador, es recomendable que proteja su configuración del Control de Contenido con una contraseña. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control de Contenido que ha configurado exclusivamente para un usuario concreto.

Cuando active el Control de Contenido, BitDefender le solicitará introducir una contraseña.

Para establecer la protección por contraseña, realice lo siguiente:

1. Introduzca la contraseña en el campo **Contraseña**.
2. Para confirmar la contraseña, introdúzcala de nuevo en el campo **Repetir contraseña**.
3. Haga clic en **Aceptar** para guardar la contraseña y cerrar la ventana.



Establecer la Protección por Contraseña

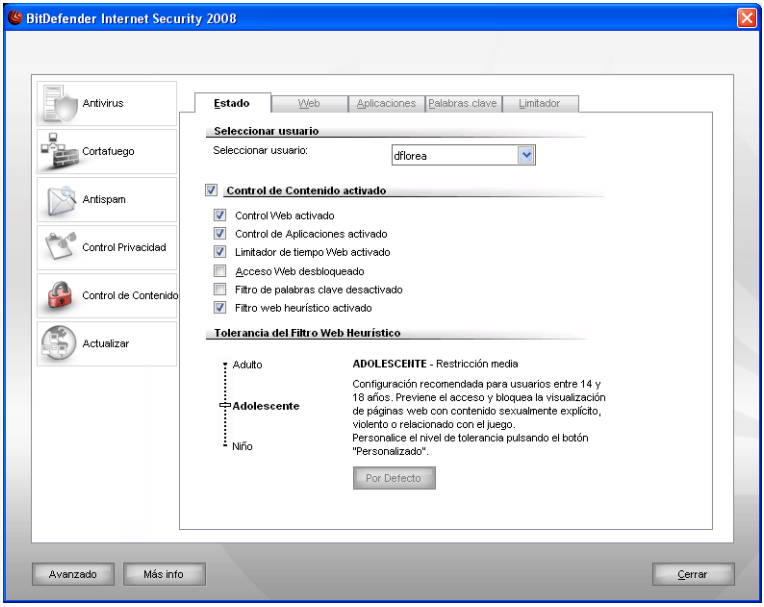
De ahora en adelante, si quiere cambiar la configuración del Control de Contenido, se le solicitará introducir la contraseña. Los otros administradores del equipo (si existen) también tendrán que introducir esta contraseña para cambiar la configuración del Control de Contenido.

Nota
Esta contraseña no protege el resto de configuraciones de BitDefender.

En el caso que no introduzca ninguna contraseña y no desea que vuelva a aparecer esta ventana, marque la casilla **No solicitar la contraseña al activar el Control de Contenido**.

12.2. Estado del Control de Contenido

Para configurar el Control de Contenido, haga clic en **Control de Contenido > Estado** en la consola de configuración. Aparecerá la siguiente pantalla:



Estado del Control de Contenido

Importante
Mantenga el módulo **Control de Contenido** activado para proteger a sus hijos contra el contenido inapropiado usando sus reglas de acceso personalizadas.

12.2.1. Seleccionando los Controles de Protección

Para configurar su nivel de protección primero debe seleccionar el usuario en el que se aplicarán las modificaciones. A continuación configure el nivel de protección usando los siguientes controles.

- **Control Web** - filtra la navegación según las reglas establecidas en el apartado Web.
- **Control de Aplicaciones** - bloquea el acceso a las aplicaciones en su ordenador acorde con las reglas especificadas en el apartado Aplicaciones.
- **Limitador de Tiempo Web** - permite o bloquea el acceso web según el horario especificado en el apartado Limitador

- **Acceso Web** - bloquea el acceso a todas las páginas web (no sólo las que aparecen en el apartado Web).
- **Filtro de palabras** - filtra el acceso web y al correo según las reglas especificadas en el apartado Palabras Clave
- **Filtro Web Heurístico** - filtra el acceso web según las reglas pre-establecidas, basadas en categorías por edad.

Nota

Para sacar el máximo provecho de las características del Control de Contenido, debe configurar los diferentes tipos de Control. Para aprender a configurar este módulo, diríjase a los siguientes temas de este capítulo.

12.2.2. Configurando el Filtrado Heurístico de Webs

El filtro web heurístico analiza las páginas web y bloquea aquellas con contenido potencialmente inapropiado.

Para filtrar el acceso web a partir de unas reglas predeterminadas para diferentes edades, deberá cambiar el nivel de tolerancia. Arrastre el control deslizante a través de la escala para fijar el nivel de protección que considere apropiado para el usuario seleccionado.

Hay 3 niveles de tolerancia:

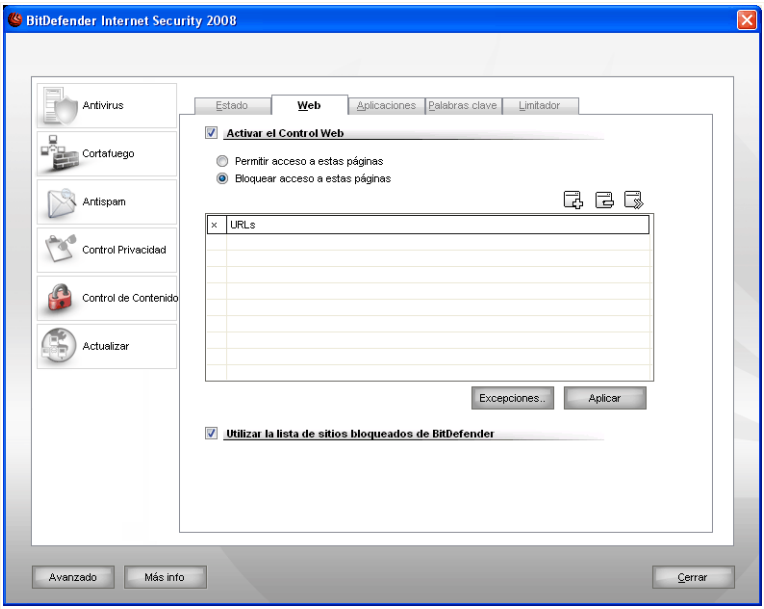
Nivel de tolerancia	Descripción
Niño	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios menores de 14 años. Se bloqueará el acceso a las páginas web con contenido potencialmente dañino para los niños (porno, sexualidad, drogas, hacking, etc).
Adolescente	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios entre 14 y 18 años. Se bloqueará el acceso a las páginas web con contenido sexual, pornográfico o adulto.
Adulto	Ofrece un acceso sin restricción a todas las páginas web, independientemente de su contenido.

Haga clic en **Por Defecto** para posicionar el deslizador en el nivel predeterminado.

12.3. Control Web

El **Control Web** le ayuda a bloquear el acceso a los sitios web con contenido inapropiado. Se le facilitará una lista de páginas web candidatas a bloquearse, que se actualizará a través del proceso de actualización.

Para configurar el Control Web, haga clic en **Control de Contenido > Web** en la consola de configuración. Aparecerá la siguiente pantalla:



Control Web

Para activar esta protección marque la casilla correspondiente a **Activar el control Web**.

Marque la casilla **Permitir acceso a estas páginas**/**Bloquear acceso a estas páginas** para ver la lista de los sitios autorizados/bloqueados. Haga clic en **Excepciones..** para ver la ventana que contiene la lista complementaria.

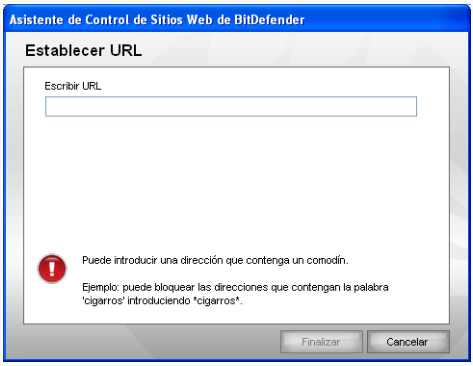
Las reglas pueden introducirse manualmente. En primer lugar, seleccione **Permitir acceso a estas páginas**/**Bloquear acceso a estas páginas** para permitir o bloquear

el acceso a las páginas web indicadas en el asistente. A continuación, haga clic en el botón **Añadir** para iniciar el asistente de configuración.

12.3.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 – Especificar las páginas Web



Especifique las páginas web

Haga clic en **Añadir**, escriba el sitio web para el que se aplicará la regla y haga clic en **Finalizar**.

Importante
Sintaxis:

- `*.xxx.com` - la acción de la regla se aplicará a todos los sitios web que terminen con `.xxx.com`;
- `*porn*` - la acción de la regla se aplicará a todos los sitios web que contengan `porn` en la dirección del sitio web;
- `www.*.com` - la acción de la regla se aplicará a todos los sitios web que tengan el sufijo de dominio `com`;
- `www.xxx.*` - la acción de la regla se aplicará a todos los sitios web que empiecen con `www.xxx.` sin importar el sufijo de dominio.

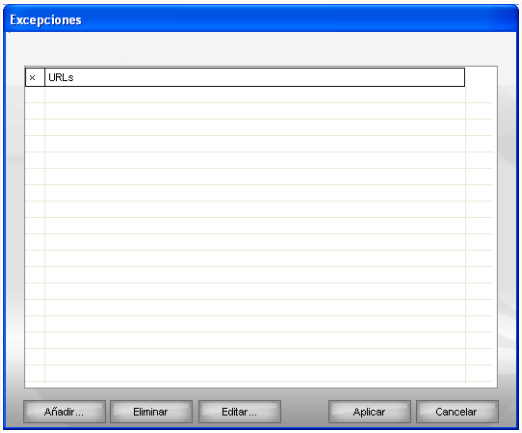
Haga clic en **Aplicar** para guardar los cambios.

Para eliminar una regla, sólo tendrá que seleccionar y hacer clic en el botón **Eliminar Regla**. Para modificar una regla selecciónela y haga clic en el botón **Editar Regla** o haga doble clic sobre la regla. Para desactivar temporalmente una regla, sin eliminarla, desmarque la casilla correspondiente a la regla.

12.3.2. Especificar Excepciones

A veces puede necesitar establecer algunas excepciones a una regla determinada. Por ejemplo, puede crear una regla para que se bloqueen todas las páginas que contienen la palabra "killer" (sintaxis: `*killer*`). Sin embargo, sabe que existe una página llamada `killer-music` donde los visitantes pueden escuchar música online. Para crear una excepción a la regla debe dirigirse a la ventana **Excepciones** y definir una excepción a la regla.

Haga clic en **Excepciones...**. Aparecerá la siguiente ventana:



Especificando Excepciones

Haga clic en **Añadir...** para especificar las excepciones. Aparecerá el Asistente de configuración. Complete los pasos del asistente para crear la excepción.

Haga clic en **Aplicar** para guardar los cambios.

Para borrar una regla, selecciónela y haga clic en **Eliminar**. Para modificar una regla selecciónela y haga clic en **Editar** o haga doble clic en la misma. Para desactivar temporalment una regla sin borrarla, desmarque la casilla correspondiente.

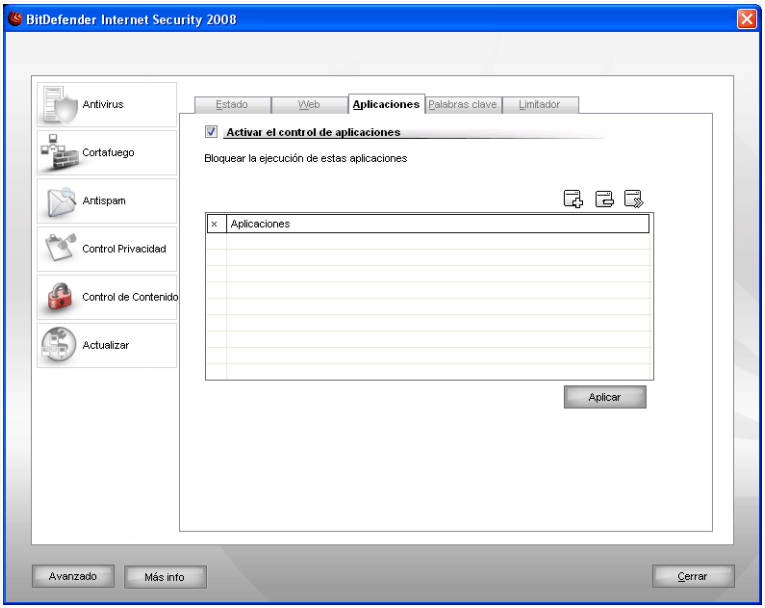
12.3.3. Lista Negra de Webs de BitDefender

Para ayudarle a proteger a sus hijos, BitDefender le proporciona una lista negra de páginas con contenido o posible contenido inapropiado. Para bloquear las páginas que aparecen en esta lista seleccione **Utilizar la lista de sitios bloqueados de BitDefender**.

12.4. Control de Aplicaciones

El **Control de Aplicaciones** ayuda a bloquear la ejecución de cualquier aplicación. Juegos, software de mensajería, u otro tipo de software y malware pueden bloquearse de esta forma. La aplicaciones bloqueadas de esta manera también están protegidas contra modificaciones y no pueden ser copiadas o movidas.

Para configurar el Control de Aplicaciones, haga clic en **Control de Contenido > Aplicaciones** en la consola de configuración. Aparecerá la siguiente pantalla:



Control de Aplicaciones

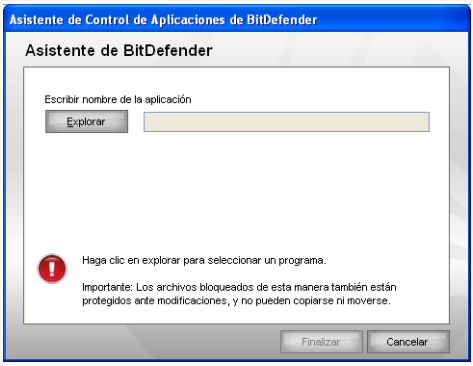
Para activar esta protección marque la casilla correspondiente a **Activar el Control de Aplicaciones**.

Las reglas deben introducirse manualmente. Haga clic en el botón **Añadir** para iniciar el asistente de configuración.

12.4.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 – Seleccionar la aplicación a bloquear



Seleccione la aplicación que desea bloquear

Haga clic en **Añadir**, clic en **Explorar**, seleccione la aplicación a bloquear y haga clic en **Finalizar**.

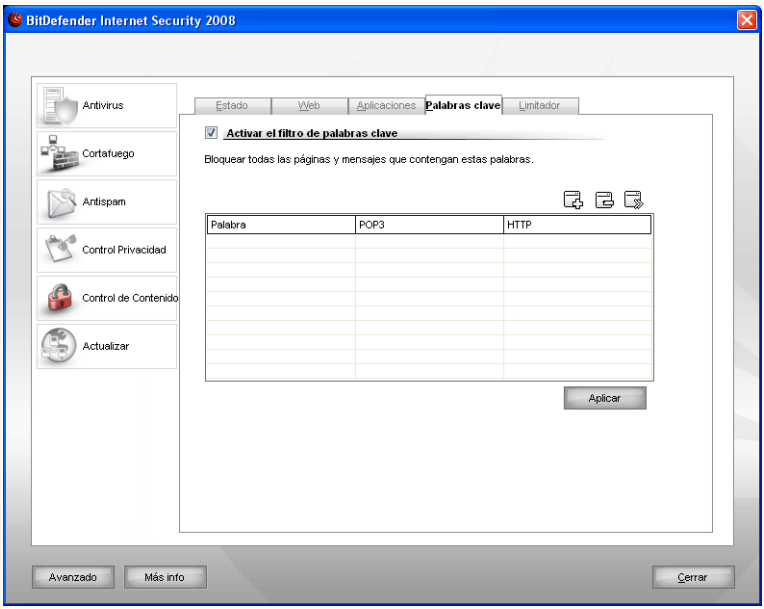
Haga clic en **Aplicar** para guardar los cambios.

Para eliminar una regla, sólo tendrá que seleccionar y hacer clic en el botón **Eliminar Regla**. Para modificar una regla selecciónela y haga clic en el botón **Editar Regla** o haga doble clic sobre la regla. Para desactivar temporalmente una regla, sin eliminarla, desmarque la casilla correspondiente a la regla.

12.5. Filtro de Palabras Clave

El **Filto de palabra clave** le ayuda a bloquear el acceso a los mensajes o páginas web que contengan la(s) palabra(s) especificada(s). De esta manera puede impedir que los usuarios vean frases o palabras inapropiadas.

Para configurar el filtro de palabras clave haga clic en **Control de Contenido > Palabras** desde la consola de configuración. Aparecerá la siguiente pantalla:



Filtro de Palabras Clave

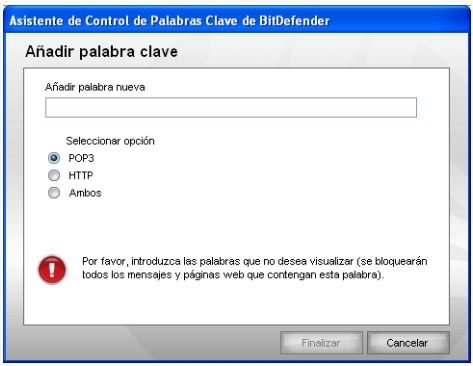
Para activar este tipo de protección marque la casilla correspondiente a **Activar el filtro de palabras clave**.

Las reglas deben introducirse manualmente. Haga clic en el botón **Añadir** para iniciar el asistente de configuración.

12.5.1. Asistente de Configuración

El asistente de configuración es un proceso de 1 paso.

Paso 1/1 - Escribir una palabra clave



Escribir la palabra clave

Debe configurar los siguientes parámetros:

- **Palabra clave** - escriba en el campo editable la palabra o frase que desea bloquear.
- **Protocolo tipo** - seleccione el protocolo que BitDefender debe analizar en busca de la palabra o frase indicada.

  Dispone de las siguientes opciones:

Opción	Descripción
POP3	Los e-mails que contengan la palabra clave serán bloqueados.
HTTP	Las páginas web que contengan la palabra clave serán bloqueados.
Ambos	Tanto los e-mails como las páginas web que contengan la palabra clave serán bloqueados.

Haga clic en **Aplicar** para guardar los cambios.

Para eliminar una regla, sólo tendrá que seleccionar y hacer clic en el botón **Eliminar Regla**. Para modificar una regla selecciónela y haga clic en el botón **Editar Regla**

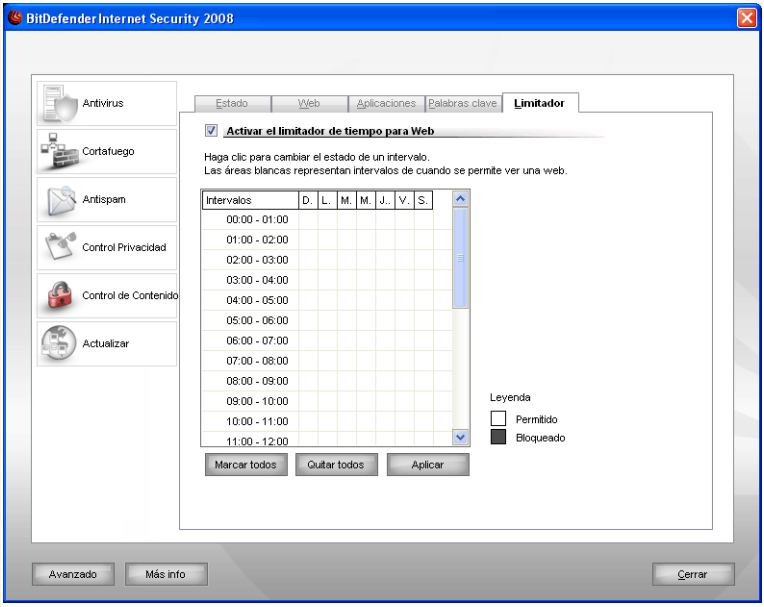
o haga doble clic sobre la regla. Para desactivar temporalmente una regla, sin eliminarla, desmarque la casilla correspondiente a la regla.

12.6. Limitador de Tiempo Web

El **Limitador de Tiempo Web** le ayuda a permitir o bloquear el acceso web a los usuarios o apliaciones durante los intervalos de tiempo indicados.

Nota
BitDefender se actualizará independientemente de la configuración del **Limitador de Tiempo Web**.

Para configurar el limitador de tiempo para Web, haga clic en la opción **Control de Contenido > Limitador** situada en la consola de configuración. Aparecerá la siguiente pantalla:



Limitador de Tiempo Web

Para activar esta protección marque la casilla correspondiente a **Activar el limitador de tiempo para Web**.

Seleccione los intervalos de tiempo en los que se bloquearán todas las conexiones a Internet. También puede hacer clic en **Marcar todos** para seleccionar todas las celdas, y en consecuencia, bloquear todo el acceso a páginas web. Si hacer clic en **Quitar todos**, se permitirá el acceso a webs en todo momento.

Importante
Las casillas coloreadas en gris representan intervalos de tiempo en los que todas las conexiones a internet están bloqueadas.

Haga clic en **Aplicar** para guardar los cambios.

13. Actualización

Cada día se encuentra nuevo malware. Por esta razón es muy importante mantener BitDefender actualizado con las últimas firmas de malware.

Si está conectado a Internet a través de una conexión de banda ancha o ADSL, BitDefender se actualizará sólo. Por defecto, comprueba si existen nuevas actualizaciones al encender su equipo y a cada **hora** a partir de ese momento.

Si se detecta alguna actualización, según las opciones existentes en el apartado Configuración de la actualización automática, o bien se descargará automáticamente o bien deberá confirmar su descarga.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afecta al rendimiento del producto a la vez que se evita cualquier riesgo.

Las actualizciones se presentan de las siguientes maneras:

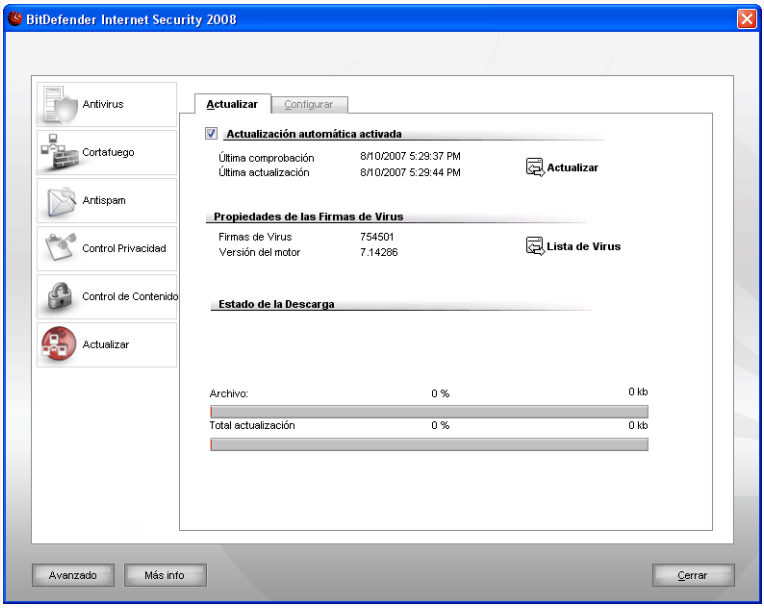
- **Actualización de los motores antivirus** - a medida que se detecten nuevas amenazas, los ficheros que incluyen las firmas de virus deberán actualizarse para asegurar una protección permanente contra los éstos. Este tipo de actualización también se conoce como **Actualización de las firmas de virus**.
- **Actualizaciones de los motores antispam** - se añadirán nuevas firmas a los filtros Heurístico y URL, y nuevas imágenes al filtro de Imágenes. Este tipo de actualizaciones aydarán a aumentar la efectividad del motor Antispam, y se conoce como **Actualización del Antispam**.
- **Actualizaciones para los motores antispyware** - se añadirán nuevas firmas de spyware a la base de datos. Esta actualización también es conocida como **Actualización Antispyware**.
- **Actualizaciones del producto** - cuando aparece una nueva versión del producto, se introducen nuevas características y técnicas de análisis para mejorar el rendimiento del producto. Este tipo de actualización es conocido como **Actualización del producto**.

El apartado **Actualización** de esta guía de usuario contiene los siguientes temas:

- Actualización automática
- Configuración de la Actualización

13.1. Actualización automática

Para ver la información relacionada con las actualizaciones, haga clic en **Actualizar > Actualizar** en la consola de configuración. Aparecerá la siguiente pantalla:



Actualización automática

Desde aquí podrá ver cuando se ha realizado la última comprobación y la última actualización (si se ha realizado con éxito o con errores). Además, también verá información sobre la versión de los motores y el número de firmas de virus.

Puede ver las firmas de malware de BitDefender haciendo clic en **Lista de Virus** y se abrirá un documento HTML con la lista de firmas disponibles. Puede buscar la firma para una amenaza en concreto o pulsar en **BitDefender Virus List** para ir a la base de datos online de BitDefender.

Si abre este apartado durante una actualización podrá ver el estado de la descarga.

Importante
Para estar protegido contra las últimas amenazas mantenga la **Actualización automática** activada.

13.1.1. Solicitando una Actualización

La actualización automática puede realizarse en cualquier momento haciendo clic en **Actualizar**. Este tipo de actualización también se conoce como **Actualización por petición del usuario**.

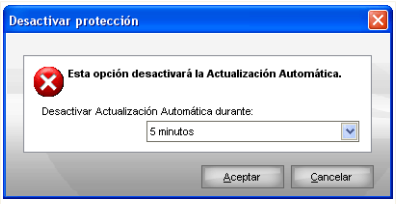
El módulo **Actualizar** se conectará al servidor de actualizaciones de BitDefender y comprobará si hay alguna actualización disponible. Si se detecta una actualización, según las opciones elegidas en el apartado de Configuración de la Actualización Manual se le pedirá que confirme la actualización o bien ésta se realizará automáticamente.

Importante
Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Recomendamos hacerlo lo más pronto posible.

Nota
Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar BitDefender manualmente.

13.1.2. Desactivando la Actualización Automática

Si decide desactivar la actualización automática, aparecerá una ventana de advertencia.



Desactivar la Actualización Automática

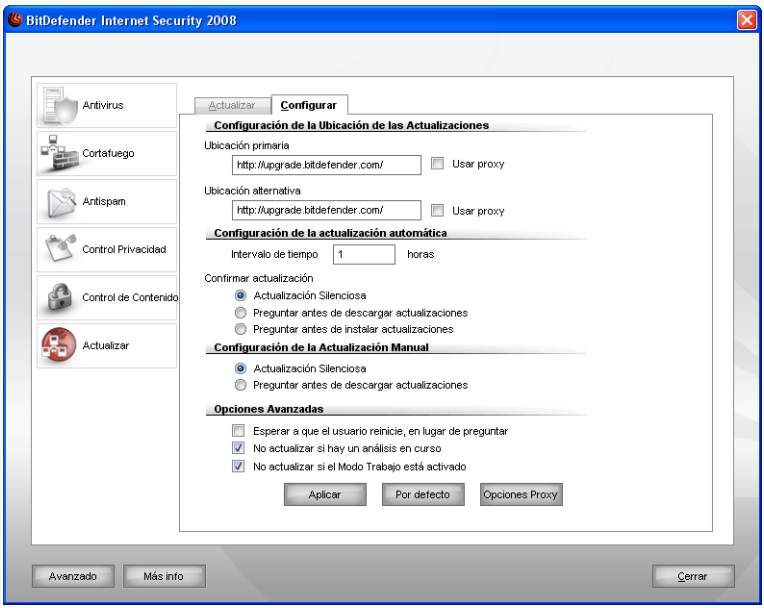
Para confirmar su elección, deberá seleccionar durante cuanto tiempo desea desactivar la actualización. Puede desactivar la actualización durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Mientras la protección esté desactivada, no tendrá protección contra las amenazas de malware más recientes.

13.2. Configuración de la Actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy. Por defecto, BitDefender comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

Para modificar la configuración de la actualización y del proxy, haga clic en **Actualizar > Configurar** en la consola de configuración. Aparecerá la siguiente pantalla:



Configuración de la Actualización

Las opciones de actualización están agrupadas en 4 categorías (**Configuración de la Ubicación de las Actualizaciones**, **Configuración de la Actualización Automática**, **Configuración de la Actualización Manual** y **Opciones Avanzadas**). Cada categoría se describirá por separado.

13.2.1. Configuración de la Ubicaciones de las Actualizaciones

Para modificar las ubicaciones de descarga de las actualizaciones, utilice las opciones de la categoría **Configuración de la Ubicación de las Actualizaciones**.

Nota
Modifique estas opciones sólo si está conectado a una red local que almacene las firmas de malware de BitDefender localmente, o si se conecta a Internet a través de un servidor proxy.

Para conseguir actualizaciones más rápidas y fiables, puede configurar dos ubicaciones de descarga: una **Ubicación primaria** y una **Ubicación alternativa**. Por defecto, estas dos ubicaciones son la misma: `http://upgrade.bitdefender.com`.

Para modificar una de las ubicaciones de descarga, indique la URL del servidor espejo en el campo **URL** correspondiente a la ubicación que desea cambiar.

Nota
Recomendamos poner el servidor espejo local en la ubicación primaria y no cambiar la ubicación alternativa. Así, en caso que falle el servidor local siempre tendrá disponible el servidor de la ubicación alternativa.

Si su empresa utiliza un servidor proxy para conectarse a Internet, marque la casilla **Usar proxy** y haga clic en **Opciones Proxy** para modificar la configuración.

Nota
Para más información, por favor, consulte el capítulo "*Administrando los Proxies*" (p. 181)

13.2.2. Configurando la Actualización Automática

Para configurar el proceso de actualización para que se realice de forma automática, utilice las opciones de la categoría **Configuración de la actualización automática**.

Puede indicar el número de horas entre dos actualizaciones consecutivas en el campo **Intervalo de tiempo**. Por defecto, el tiempo de intervalo es de 1 hora.

Para indicar cómo debe realizarse las actualizaciones automáticas, seleccione una de las siguientes opciones:

- **Actualización silenciosa** - BitDefender descarga e instala las actualizaciones automáticamente.
- **Preguntar antes de descargar actualizaciones** - cada vez que exista una actualización disponible, se le preguntará si desea descargarla.

Nota
Se le preguntará antes de descargar las actualizaciones incluso si ha salido del Centro de Seguridad.

- **Preguntar antes de instalar actualizaciones** - cada vez que se haya descargado una actualización, se le pedirá permiso para instalarla.

Nota
Se le preguntará antes de instalar las actualizaciones incluso si ha salido del Centro de Seguridad.

13.2.3. Configurando la Actualización Manual

Para indicar cómo debe realizarse la actualización manual (actualización por petición del usuario), seleccione una de las siguientes opciones en la categoría **Configuración de la Actualización Manual**:

- **Actualización silenciosa** - la actualización manual se realizará automáticamente en segundo plano, sin la intervención del usuario.
- **Preguntar antes de descargar actualizaciones** - cada vez que exista una actualización disponible, se le preguntará si desea descargarla.

Nota
Se le preguntará antes de descargar las actualizaciones incluso si ha salido del Centro de Seguridad.

13.2.4. Modificando las Opciones Avanzadas

Para impedir que el proceso de actualización de BitDefender interfiera en su trabajo, modifique las opciones en la categoría **Opciones Avanzadas**:

- **Esperar a que el usuario reinicie, en lugar de preguntar** - Si una actualización requiere el reinicio del equipo, el producto funcionará con los archivos antiguos hasta que reinicie el sistema. No se le pedirá al usuario que reinicie, de manera que el proceso de actualización de BitDefender no interferirá con el trabajo de los usuarios.
- **No actualizar si hay un análisis en curso** - BitDefender no se actualizará mientras haya un proceso de análisis en curso. De este modo, la actualización de BitDefender no interferirá en las tareas de análisis.

Nota
Si se actualiza BitDefender mientras se realiza un análisis, el análisis se abortará.

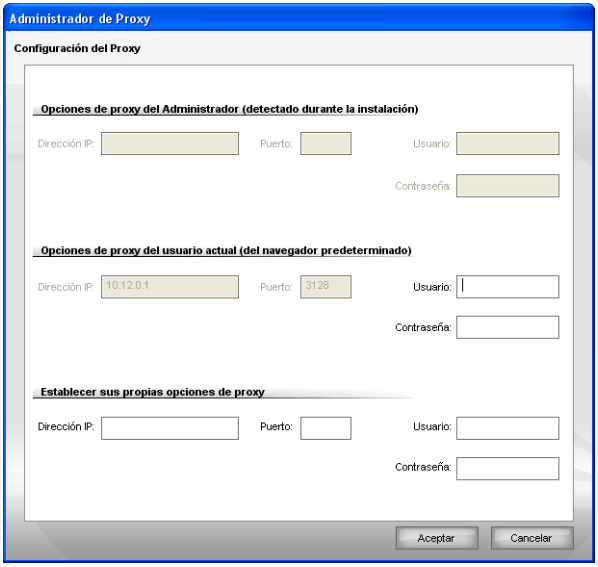
- **No actualizar si el Modo Trabajo está activado** - BitDefender no se actualizará mientras el modo trabajo esté activado. De esta manera podrá minimizar el impacto del producto en el rendimiento del sistema mientras juega.

13.2.5. Administrando los Proxies

Si su empresa utiliza un servidor proxy para conectarse a Internet, deberá introducir la configuración del proxy para que BitDefender pueda actualizarse. En caso contrario, se utilizará la configuración introducida por el administrador, o la configuración indicada en el navegador web.

Nota
La configuración del proxy sólo puede realizarse por los usuarios que tengan permisos de administrador o los usuarios que conozcan la contraseña de configuración del producto.

Para modificar la configuración del proxy, haga clic en **Opciones Proxy**. Aparecerá la ventana **Administrador de Proxy**.



Administrador de Proxy

Existen 3 tipos de configuración de proxy:

- **Opciones de proxy del Administrador (detectado durante la instalación)** - configuración detectada en la cuenta de administrador durante la instalación del producto, pero sólo podrá modificarse si ha iniciado sesión como Administrador. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.
- **Opciones de proxy del usuario actual (del navegador predeterminado)** - configuración de proxy del usuario en uso, extraída directamente del navegador predeterminado. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.

Nota

Los navegadores web soportados son Internet Explorer, Mozilla Firefox y Opera. Si utiliza otro navegador, BitDefender no será capaz de reconocer la configuración de proxy del usuario en uso.

- **Sus propias opciones de proxy** - configuración del proxy que puede modificar si ha iniciado sesión como administrador.

  Deben indicarse las siguientes opciones:
  - **Dirección** - introduzca la IP del servidor proxy.
  - **Puerto** - introduzca el puerto que BitDefender debe utilizar para conectarse con el servidor proxy.
  - **Nombre de Usuario** - introduzca un nombre de usuario válido para el proxy.
  - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

Al intentar conectarse a Internet, se prueba cada una de las configuraciones simultáneamente, hasta que BitDefender consiga conectarse.

En primer lugar se prueba su propia configuración para conectarse a Internet. Si no funciona, se probará la configuración detectada durante la instalación. Finalmente, si tampoco funciona, se importará la configuración desde el navegador predeterminado para intentar conectarse.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Haga clic en **Aplicar** para guardar los cambios realizados, o en **Por defecto** para cargar la configuración inicial.

CD de Rescate de BitDefender

14. General

BitDefender Internet Security 2008 se entrega en un CD de autoarranque (CD de Rescate de BitDefender), que puede utilizarse para desinfectar un sistema antes de que arranque el sistema operativo.

Puede utilizar el CD de rescate BitDefender cada vez que su sistema operativo no funcione correctamente debido a las infecciones de virus. Normalmente se producen este tipo de incidencias cuando no se utiliza un sistema de protección antivirus.

Las actualizaciones de firmas de virus se realizan automáticamente sin la intervención del usuario una vez se inicia el CD de rescate BitDefender.

El CD de Rescate de BitDefender es una distribución de Knoppix remasterizada por BitDefender, que incluye las últimas soluciones de seguridad de BitDefender para Linux en un GNU/Linux Knoppix Live CD, ofreciendo un antivirus para puestos de trabajo que puede analizar y desinfectar los discos duros (incluso las particiones NTFS de Windows). Al mismo tiempo, el CD de Rescate de BitDefender puede utilizarse para restaurar datos importantes cuando no pueda iniciar Windows.

Nota
El CD de Rescate de BitDefender puede descargarse desde la siguiente ubicación: http://download.bitdefender.com/rescue_cd/

14.1. Requisitos del Sistema

Antes de iniciar el CD de Rescate de BitDefender, debe comprobar si el equipo cumple con los siguientes requisitos.

Procesador
Compatible con procesadores x86, mínimo 166 MHz, pero con un bajo redimiento. Un procesador de generación i686, a 800 MHz, es la opción recomendable.

RAM
Mínimo 512 MB de RAM (1 GB recomendado)

CD-ROM
El CD de Rescate de BitDefender arranca desde el CD-ROM, y la BIOS del equipo estar configurada para iniciar el sistema desde el CD.

Conexión de Internet
Aunque el CD de Rescate de BitDefender funcione sin conexión a Internet, el proceso de actualización precisa de un enlace HTTP activo, aunque sea a través

de un servidor Proxy. Por lo tanto la conexión a Internet es un REQUISITO para poder actualizar la protección.

Resolución gráfica
Tarjeta gráfica compatible con SVGA.

14.2. Software Incluido

El CD de Rescate BitDefender incluye los siguientes paquetes de software:

Xedit
Un editor de archivos de texto.

Vim
Potente editor de archivos de texto, que contiene resaltado de sintaxis, interfaz gráfica de usuario, y mucho más. Para más información, consulte la página web de Vim .

Xcalc
Es una calculadora.

RoxFiler
Es un administrador de archivos gráfico muy rápido.

Para más información, consulte la página web de RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) es un administrador de archivos de modo texto.

Para más información, consulte la página web de MC.

Pstree
Pstree muestra los procesos en ejecución.

Top
Top muestra las tareas de Linux.

Xkill
Xkill cierra la aplicaciones basadas en el sistema X.

Partition Image
Partition Image le ayuda a guardar sus particiones de sistemas de archivos EXT2, Reiserfs, NTFS, HPFS, FAT16, y FAT32 en un archivo de imagen. Este programa puede utilizarse para operaciones de copia de seguridad.

Para más información, consulte la página web de Partimage.

GtkRecover

GtkRecover es una versión GTK de la consola de recuperación de programas. Le ayuda a recuperar un archivo.

Para más información, consulte la página web de GtkRecover.

ChkRootKit

ChkRootKit es una herramienta que le ayuda analizar su equipo en busca de rootkits.

Para más información, consulte la página web de ChkRootKit.

Nessus Network Scanner

Nessus es un analizador de seguridad remota para sistemas Linux, Solaris, FreeBSD, y Mac OS X.

Para más información, consulte la página web de Nessus.

Iptraf

Iptraf es un software de monitorización de red IP.

Para más información, consulte la página web de Iptraf.

Iftop

Iftop muestra el uso del ancho de banda en una interfaz.

Para más información, consulte la página web de Iftop.

MTR

MTR es una herramienta de diagnóstico de red.

Para más información, consulte la página web de MTR.

PPPStatus

PPPStatus muestra estadísticas acerca de las conexiones entrantes y salientes del tráfico TCP/IP.

Para más información, consulte la página web de PPPStatus.

Wavemon

Wavemon es una aplicación para monitorizar los dispositivos de las conexiones wireless.

Para más información, consulte la página web de Wavemon.

USBView

USBView muestra información sobre los dispositivos conectados al bus USB.

Para más información, consulte la página web de USBView .

Pppconfig

Pppconfig ayuda a configurar automáticamente una conexión ppp por módem.

DSL/PPPoe

DSL/PPPoe configura la conexión PPPoE (ADSL).

I810rotate

I810rotate controla la salida de vídeo del hardware i810 a través de i810switch(1).

Para más información, consulte la página web de I810rotate.

Mutt

Mutt es un cliente de correo de texto basado en MIME.

Para más información, consulte la página web de Mutt.

Mozilla Firefox

Mozilla Firefox es un navegador web muy conocido.

Para más información, consulte la página web de Mozilla Firefox.

Elinks

Elinks es un navegador web de modo texto.

Para más información, por favor, consulte la página web de Elinks .

15. Como Utilizar el CD de Rescate de BitDefender

Este capítulo contiene información sobre cómo iniciar y detener el CD de Rescate de BitDefender, analizar su equipo o guardar datos importantes en una unidad extraíble. Sin embargo, si utiliza las aplicaciones que se incluyen en el CD podrá realizar más tareas de las que se detallan en esta guía.

15.1. Iniciar el CD de Rescate de BitDefender

Para iniciar el CD, debe configurar la BIOS de su equipo para que el equipo arranque desde el CD y a continuación reinicie el equipo. Asegúrese que su equipo puede arrancar desde el CD.

Espere que se inicie el equipo desde el CD de Rescate de BitDefender.

Ventana de inicio de Boot

Durante la carga del sistema, se actualizan las firmas de virus automáticamente. Esta operación puede llevar un tiempo.

Una vez finalizado el inicio del CD, podrá ver el Escritorio y utilizar el CD de Rescate de BitDefender.

El Escritorio

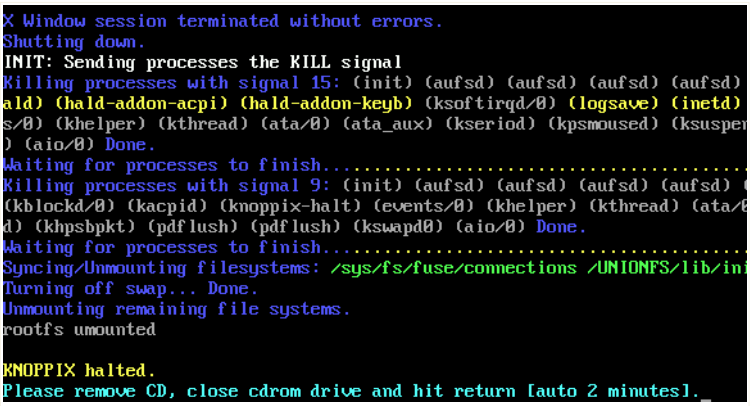
15.2. Detener el CD de Rescate de BitDefender

Puede apagar su equipo de forma segura seleccionado la opción **Exit** desde el menú contextual (clic derecho para abrirlo) o introduciendo el comando **halt** en la terminal de comandos.

Seleccione "EXIT"

Cuando el CD de Rescate de BitDefender haya cerrado todos los programas, le mostrará una ventana como la siguiente. Entonces, deberá retirar el CD de la unidad

de CD-Rom para iniciar el equipo desde su disco duro. Ahora ya puede apagar el equipo o reiniciarlo.



Espere este mensaje cuando apaga el equipo

15.3. Cómo realizar un análisis antivirus?

Aparecerá un asistente cuando finalice el proceso de carga, desde el que podrá analizar completamente su equipo. Sólo tiene que hacer clic en el botón **Start**.

Nota
Si su resolución de pantalla no es lo suficientemente alta, se le preguntará si desea iniciar el análisis en modo texto.

Siga el proceso guiado de tres pasos para completar el proceso de análisis.

1. Puede ver el estado y las estadísticas del análisis (velocidad de análisis, número de archivos analizados / infectados / sospechosos / objetos ocultos y otros).

   Nota
   El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis.

2. Puede ver el número de incidencias que afectan a su sistema.

   Las incidencias se muestran agrupadas en grupos. Haga clic en "+" para abrir un grupo o en "-" para cerrar un grupo.

Puede elegir una opción global que se aplicará a todos los elementos cada grupo, o bien elegir una opción para cada uno de los elementos.
3. Puede ver el resumen de los resultados.

Si desea analizar únicamente una carpeta, siga estos pasos:

Navegue por sus carpetas, haga clic derecho en el fichero o carpeta deseado y seleccione **Send to**. A continuación seleccione **BitDefender Scanner**.

También puede utilizar el siguiente comando estando conectado como root en la terminal. **BitDefender Antivirus Scanner** comenzará a analizar los ficheros o las carpetas seleccionados.

```
# bdscan /path/to/scan/
```

15.4. ¿Cómo puedo actualizar BitDefender sobre un servidor proxy?

Si existe algún servidor proxy entre su equipo e Internet, puede cambiar algunas opciones para poder realizar las actualizaciones.

Para actualizar BitDefender sobre un servidor proxy, siga estos pasos:

1. Haga clic derecho en el Escritorio y aparecerá el menú contextual del CD de Rescate de BitDefender.
2. Seleccione **Terminal (as root)**.
3. Escriba el siguiente comando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Escriba el comando: **mcedit bdscan.conf** para editar este archivo con GNU Midnight Commander (mc).
5. Descomente la siguiente línea: `#HttpProxy =` (simplemente elimine el carácter `#`) e indique el dominio, nombre de usuario, contraseña y puerto del servidor proxy. Por ejemplo, la línea resultante debería parecerse a la siguiente:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Pulse **F2** para guardar el archivo, confirme que desea guardarlo, y pulse **F10** para cerrarlo.
7. Escriba el comando: **bdscan update**.

15.5. Cómo guardar mis datos?

Imaginemos que no puede iniciar Windows debido a algunos problemas desconocidos, pero que necesita desesperadamente acceder a algunos datos importantes de de su equipo. En este tipo de situaciones es dónde el CD de Rescate de BitDefender resulta sumamente útil.

Para guardar sus datos del ordenador en un dispositivo extraíble, como una memoria USB, sólo tiene que seguir estos pasos:

1. Introduzca el CD de Rescate de BitDefender en la unidad de CD, la memoria USB en la ranura USB correspondiente, y reinicie el ordenador.
2. Espere a que el CD de Rescate de BitDefender se cargue. Aparecerá la siguiente ventana:

Ventana del Escritorio

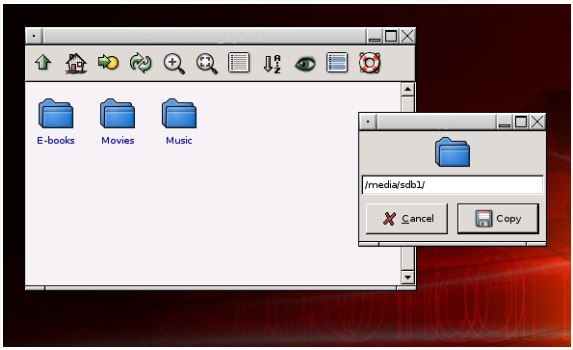
3. Haga doble clic en la partición donde están almacenados los datos que desea guardar (por ej: `[sda3]`).

Nota

Cuando trabaje con el CD de Rescate de BitDefender, los nombres de las particiones aparecerán en formato Linux. De tal manera que, `[sda1]` probablemente

corresponderá con la partición `(C:)` de Windows, `[sda3]` con `(F:)`, y `[sdb1]` con la memoria USB.

4. Navegue entre sus carpetas y abra el directorio deseado. Por ejemplo, `Mis Datos` que contiene las subcarpetas `Películas`, `Música` y `E-libros`.
5. Haga clic con el botón derecho sobre la carpeta deseada y seleccione **Copiar**. Aparecerá la siguiente ventana:



Guardando Datos

6. Introduzca `/media/sdb1/` en la casilla de texto correspondiente y haga clic en **Copiar**.

Conseguir Ayuda

16. Soporte

Como cualquier compañía orientada a satisfacer las necesidades de sus clientes, BitDefender asegura un soporte técnico rápido y eficiente a sus clientes. El centro de soporte técnico está permanentemente al tanto de las últimas apariciones y descripciones de virus, y está siempre preparado para responder a sus dudas y problemas, de manera que obtenga cuanto antes la información necesaria.

En BitDefender, el interés por ahorrar tiempo y dinero a nuestros clientes facilitándoles los productos más avanzados al mejor precio siempre ha sido una prioridad. Además, pensamos que para tener un negocio de éxito es necesaria una comunicación eficiente y el compromiso de ofrecer excelentes servicios a nuestros clientes.

Puede contactar con nosotros por correo elctrónico a través de la siguiente dirección soporte@bitdefender.es. Para mejorar el tiempo de respuesta es recomendable enviar una descripción del problema, información acerca del sistema, la solución BitDefender utilizada y una descripción de los pasos a seguir para reproducir la incidencia de la forma más detallada posible.

16.1. BitDefender Knowledge Base

BitDefender Knowledge Base es una librería de información sobre los productos BitDefender. En este apartado se muestran consejos de productos y de prevención de virus, bugs solucionados, consejos de configuración etc.

BitDefender Knowledge Base es de acceso público y pueden consultarse gratuitamente. La amplia información que contiene es otro medio de proporcionar a los clientes de BitDefender el soporte técnico y la conocimiento que necesitan. Las peticiones de información general o bugs de nuestros clientes se incluyen en la BitDefender Knowledge Base en forma de solución a dichos bugs, instrucciones de depuración de errores o artículos informativos como apoyo de los archivos de ayuda de los distintos productos.

Puede acceder a BitDefender Knowledge Base a través del navegador, en la siguiente dirección web http://kb.bitdefender.com.

16.2. Solicitando Ayuda

16.2.1. Ir a la Web de Ayuda On-Line

¿Tiene alguna duda? No se preocupe, nuestros expertos en seguridad estarán disponibles para atenderle a través del teléfono, email o chat 24 horas al día durante los 7 días de la semana, sin ningún coste.

Por favor, siga los siguientes enlaces:

Inglés

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2195/

Alemán

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2195/

Francés

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2195/

Rumano

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2195/

Español

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2195/

16.2.2. Abrir un ticket de soporte

Si desea abrir un ticket de soporte y recibir ayuda a través del correo electrónico, siga cualquiera de estos enlaces:

Inglés: http://www.bitdefender.com/site/Main/contact/1/
Alemán: http://www.bitdefender.de/site/Main/contact/1/
Francés: http://www.bitdefender.fr/site/Main/contact/1/
Rumano: http://www.bitdefender.ro/site/Main/contact/1/
Español: http://www.bitdefender.es/site/Main/contact/1/

16.3. Información de Contacto

BITDEFENDER valora todas las sugerencias e ideas que desee comunicarnos respecto a mejoras en el producto, o sobre la calidad de nuestros servicios. Así mismo, si tiene información referente a nuevos virus esperamos sus descripciones. Por favor no dude en contactar con nosotros.

16.3.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Soporte técnico: soporte@bitdefender.es
Documentación: documentation@bitdefender.com
Programa de Partners: partners@bitdefender.es
Marketing: marketing@bitdefender.es
Relaciones con la Prensa: prensa@bitdefender.es
Oportunidades de Trabajo: jobs@bitdefender.es
Envío de Virus: virus@bitdefender.es
Envío de Spam: spam_submission@bitdefender.com
Notificar abuso: abuso@bitdefender.es
Página del producto: http://www.bitdefender.es
Productos en ftp: ftp://ftp.bitdefender.com/pub
Distribuidores locales: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

16.3.2. Filiales

Las oficinas de BitDefender están listas para responder cualquier pregunta relativa a sus áreas de operación, tanto a nivel comercial como en asuntos generales. Sus direcciones y contactos están listados a continuación.

Estados Unidos

BitDefender, LLC
c/ Balmes 191 2ª planta
08006 Barcelona, España
Web: http://www.bitdefender.com
Soporte Técnico:

- E-mail: support@bitdefender.com
- Tel:

- 1-888-868-1873 (Sólo para Usuarios Registrados; sólo accesible desde Estados Unidos)
- 1-954-776-6262 (Sólo para Usuarios Registrados)

Servicio de Atención al Cliente:

- E-mail: customerservice@bitdefender.com
- Tel:
  - 1-888-868-1873 (Sólo para Usuarios Registrados; sólo accesible desde Estados Unidos)
  - 1-954-776-6262 (Sólo para Usuarios Registrados)

Alemania

BitDefender GmbH
Headquarter Europa Occidental
Karlsdorferstrasse 56
88069 Tettnang
Alemania
Teléfono: +49 7542 9444 60
Fax: 07542/94 44 99
E-mail: info@bitdefender.com
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com
Soporte técnico: support@bitdefender.com

Reino Unido e Irlanda

One Victoria Square
Birmingham
B1 1BD
Teléfono: +44 207 153 9959
Fax: +44 845 130 5069
E-mail: info@bitdefender.com
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.co.uk
Soporte técnico: soporte@bitdefender.es

España

Constelación Negocial, S.L

C/ Balmes 191, 2ª planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender.es
Comercial: comercial@bitdefender.es
Teléfono: (+34) 93 218 96 15
Fax: (+34) 93 217 91 28
Página web del producto: http://www.bitdefender.es

Rumania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Soporte técnico: soporte@bitdefender.es
Comercial: sales@bitdefender.com
Teléfono: +40 21 4085600
Fax: +40 21 2330763
Página del producto: http://www.bitdefender.es

Glosario

ActiveX

ActiveX es un modelo para escribir programas de manera que otros programas y el sistema operativo puedan usarlos. La tecnología ActiveX se utiliza con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y se comporten como programas más que páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, apretar botones, interaccionar de otra manera con la página web. Los controles de ActiveX normalmente están escritos en Visual Basic.

ActiveX destaca por la ausencia absoluta de controles de seguridad; los expertos de seguridad desaprueban el uso de ActiveX en Internet.

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y, en algunos casos, afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Archivo comprimido

Disco, cinta o carpeta que contiene ficheros almacenados.

Fichero que contiene uno o varios ficheros en formato comprimido.

Backdoor

Agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. La causa de estos agujeros no es siempre siniestra; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos de servicio o para los responsables del mantenimiento del producto.

Sector de arranque

Sector situado al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). En los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Virus de boot

Virus que infecta el sector de arranque de un disco fijo o disquete. Si se inicia el sistema desde un disco infectado con un virus de boot, el virus se activará en la memoria. A partir de ese momento, cada vez que se inicie el sistema el virus estará activo en memoria.

Navegador

Abreviación de Navegador de Páginas Web, es la aplicación utilizada para para visualizar páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer, ambos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como texto. Además, la mayoría de los navegadores modernos incluyen información multimedia: sonido e imágenes, aunque requieren plugins para mostrar ciertos formatos.

Línea de comando

En una interfaz con línea de comandos, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros que contienen información sobre los ordenadores de cada persona, que se pueden ser analizados y utilizados por publicistas para determinar los intereses y los gustos online de los usuarios. La tecnología de las cookies se desarrolla con la intención de personalizar los mensajes publicitarios que visualiza para que coincidan con los intereses manifestados. Es un arma de doble filo, porque por un lado, es más eficiente que vea publicidad relacionadas con sus intereses. Pero por otro lado, implica seguir cada paso y cada clic que usted haga. Por consiguiente, es normal que haya un debate sobre la privacidad y mucha gente se siente ofendida por la idea de ser vista como "número SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Descarga

Para copiar información (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

E-mail

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Extensión de un fichero

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Varios sistemas operativos usan extensiones de ficheros (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Podemos indicar "c" para el lenguaje C, "ps" para PostScript, "txt" para un texto arbitrario.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de los virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva versión de un virus ya existente. Sin embargo, ocasionalmente puede notificar sobre la existencia de unos códigos sospechosos en los programas normales, generando el "falso positivo".

IP

Internet Protocol - pertenece a la gama de protocolos TCP/IP y es responsable. Toda la comunicación en Internet se realiza mediante los dos protocolos para el intercambio de información: El Transmission Control Protocol (TCP, o Protocolo de Control de Transmisión) y el Internet Protocol (IP, o Protocolo de Internet). Estos protocolos son conocidos, en forma conjunta, como TCP/IP. No forman un único protocolo sino que son protocolos separados, pero sin embargo están estrechamente comunicados para permitir una comunicación más eficiente.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Virus de Macro

Es un tipo de virus informático que se encuentra codificado como una macro incluida en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir una macro en un documento y también que la macro se ejecute cada vez que se abra el documento.

Cliente de Correo

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico

Este método de análisis se basa en firmas de virus especificas. La ventaja del análisis no heurístico es que no se le puede engañar por algo que parecería ser un virus. Por consiguiente, no genera alarmas falsas.

Programas empaquetados

Son ficheros en un formato comprimido. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un fichero para que ocupe menos espacio en memoria. Por ejemplo: tiene un fichero de texto que contiene diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios.

En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Ruta

Las direcciones exactas de un fichero en un ordenador, generalmente descritas mediante un sistema jerárquico: se empieza por el límite inferior, mostrando un listado que contiene la unidad de disco, el directorio, los subdirectorios, el fichero mismo, la extensión del fichero si tiene alguna. Esta suma de información es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Fichero de informe

Es un fichero que lista las acciones ocurridas. BitDefender mantiene un fichero de informe (log) que contiene un listado de las rutas analizadas, las carpetas, el número de archivos comprimidos y ficheros analizados, el número de ficheros infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y hacía referencia a herramientas recompiladas que proporcionaba permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricoa, si éstos incorporan el software apropiado.

Los rootkits no son malicisosos por naturaleza. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

Es otro término para macro o fichero batch y consiste en una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o los posts basura en los grupos de noticias. Generalmente conocido como correo no solicita.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos en startup

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Bandeja del sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la parte de debajo de la pantalla, al lado del reloj y contiene iconos miniaturales para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los Troyanos arrastraran el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron del hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo a sus compatriotas entrar y capturar Troya.

Actualización

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la

instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

BitDefender tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.