bitdefender

INTERNET SECURITY 2009

Guía de usuario

bitdefender

BitDefender Internet Security 2009

Guía de usuario

publicado 2008.08.22

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 2009** como solución de seguridad para sus ordenadores. La información presentada en este libro no sólo está dirigida a los usuarios avanzados, sino a todas aquellas personas que trabajan con Windows.

Este manual le describirá el uso de **BitDefender Internet Security 2009**, 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 2009**, cómo actualizarlo, evaluarlo y personalizar la configuración. En resumen, aprenderá a sacarle el máximo provecho a BitDefender.

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. xiv)	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
Este tipo de advertencias requieren su atención y no es recomendable saltárselas. Normalmente proporcionan información importante aunque no extremadamente crítica.

Aviso
Los avisos le promocionan información crítica que debería tratar con extremada cautela. No se producirá ningún problema si sigue las indicaciones. Debería leer y entender este tipo de advertencias porque describen operaciones de riesgo.

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 un equipo. Se trata de un extenso tutorial sobre la instalación de **BitDefender Internet Security 2009**. Empezando por los pre-requisitos para una instalación exitosa, se le conducirá a través del proceso de instalación por completo. Finalmente, también se describirá el proceso de desintalación en caso que necesite desinstalar BitDefender.

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

Administración Avanzada. Una presentación detallada de las opciones de seguridad de BitDefender. 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).

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

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.

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 este manual. Hemos comprobado y verificado toda la información contenida en este documento de la mejor forma posible. Por favor, escríbanos para comentarnos cualquier error que encuentre en este manual así como sugerencias para mejorarlo y 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. Requisitos del Sistema

Sólo podrá instalar BitDefender Internet Security 2009 en aquellos equipos que dispongan de los siguientes sistemas operativos:

- Windows XP con Service Pack 2 (32/64 bit) o superior
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1
- Windows Home Server

Antes de instalar el producto, compruebe que el equipo reúne los siguientes requisitos del sistema:

Nota
Para averiguar el sistema operativo que utiliza su equipo e información sobre el hardware, haga clic derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** en el menú.

1.1. Requisitos de Hardware

Para Windows XP

- Procesador de 800 MHz o superior
- 256 MB de Memoria RAM (1 GB recomendado)
- 170 MB de espacio libre en disco (200 MB recomendado)

Para Windows Vista

- Procesador de 800 MHz o superior
- 512 MB de Memoria RAM (1 GB recomendado)
- 170 MB de espacio libre en disco (200 MB recomendado)

Para Windows Home Server

- Procesador de 800 MHz o superior
- 512 MB de Memoria RAM (1 GB recomendado)
- 170 MB de espacio libre en disco (200 MB recomendado)

1.2. Requisitos de Software

- Internet Explorer 6.0 (o superior)
- .NET Framework 1.1 (disponible en el paquete de instalación)

Protección Antispam disponible para todos los clientes de correo POP3/SMTP. Sin embargo, la barra de herramientas de BitDefender Antispam sólo se integra con los siguientes clientes:

- Microsoft Outlook 2000 / 2002 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 1.5 y 2.0

Protección Antiphishing disponible sólo para:

- Internet Explorer 6.0 o superior
- Mozilla Firefox 2.0
- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

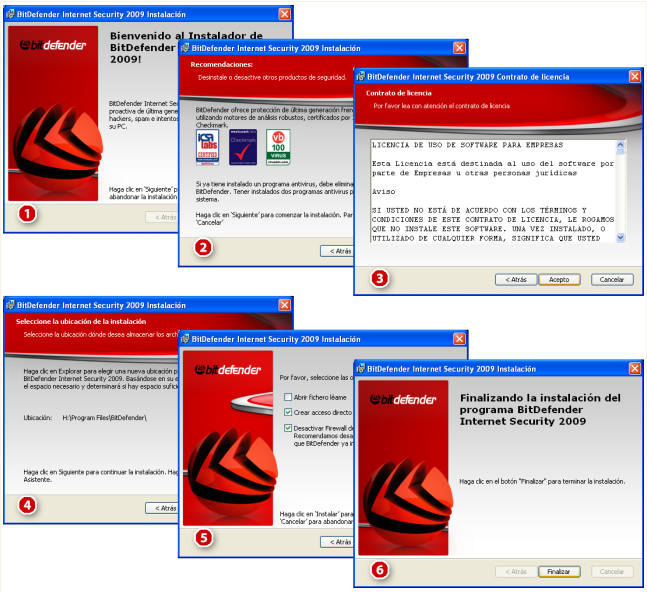
Cifrado de Mensajería Instantánea (IM) disponible sólo para:

- Yahoo! Messenger 8.1
- Windows Live (MSN) Messenger 8.5

2. Instalando BitDefender

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 2009:

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 2009 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
   Se recomienda encarecidamente desinstalar los productos antivirus detectados antes de iniciar la instalación de BitDefender. Ejecutar dos antivirus a la vez puede provocar inestabilidad en el sistema.

3. Por favor, lea los términos del Contrato de Licencia y si está de acuerdo con las condiciones previstas, haga clic en **Acepto**.

   Importante
   Si no está de acuerdo con la condiciones, haga clic en **Cancelar**. Abandonará el proceso de instalación y saldrá del asistente.

4. Por defecto, BitDefender Internet Security 2009 se instalará en `C:\Archivos de programa\BitDefender\BitDefender 2009`. Si desea cambiar la ruta de instalación, haga clic en **Explorar** y seleccione la carpeta donde desea instalar BitDefender Antivirus 2009.

   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 situar un acceso directo de BitDefender Internet Security 2009 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

Recomendamos desactivar el Firewall de Windows puesto que BitDefender Internet Security 2009 ya incluye un cortafuego avanzado. Ejecutar dos cortafuegos en el mismo equipo 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. En caso de no disponer de .NET Framework 1.1, BitDefender empezará con la instalación de este componente.

Espere hasta que la instalación se complete.

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

Importante

Al finalizar el proceso de instalación y tras reiniciar el equipo, aparecerá un Asistente de Registro y un Asistente de Configuración. Complete los pasos de estos asistentes para registrar y configurar BitDefender Internet Security 2009 y crear una Cuenta de BitDefender.

Si ha seleccionado la ruta de instalación predeterminada, se creará una nueva carpeta llamada `BitDefender` dentro de `Archivos de Programa`, que a su vez contiene otra subcarpeta llamada `BitDefender 2009`.

2.1. Asistente de Registro

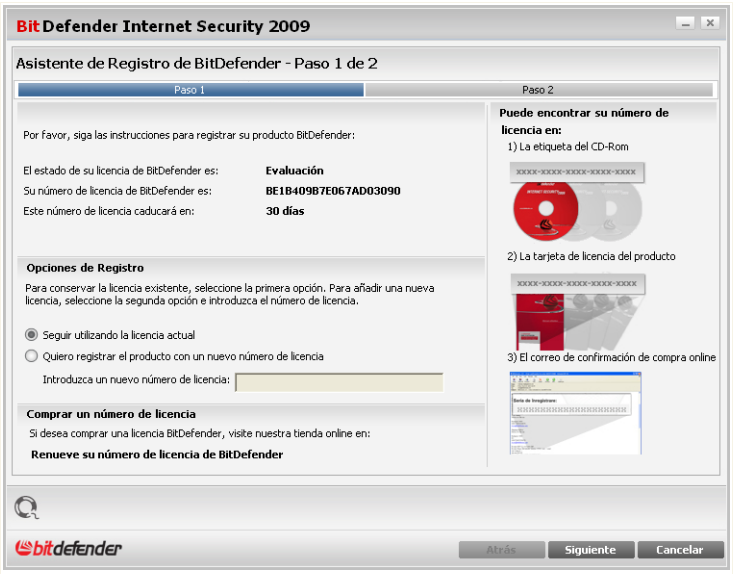
La primera vez que reinicie el equipo tras la instalación, aparecerá un Asistente de Registro. Este asistente le ayudará a registrar BitDefender y a configurar una cuenta de BitDefender.

La cuenta de BitDefender da acceso al soporte técnico gratuito, ofertas especiales y promociones. En caso de pérdida del número de licencia, puede recuperarlo iniciando sesión en http://myaccount.bitdefender.com.

Nota

Si no desea completar los pasos de este asistente, haga clic en **Cancelar**. Puede abrir el Asistente de Registro en cualquier momento haciendo clic en el enlace **Registrar**, situado en la parte inferior de la interfaz de usuario.

2.1.1. Paso 1/2 - Registrar BitDefender Internet Security 2009



Registro

Puede ver el estado del registro de BitDefender, el número de licencia actual y los días restantes hasta la fecha de caducidad de la licencia.

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

Para registrar BitDefender Internet Security 2009:

1. Seleccione la opción **Quiero registrar el producto con un nuevo número de licencia**.
2. Introduzca el número de licencia en el campo editable.

Nota

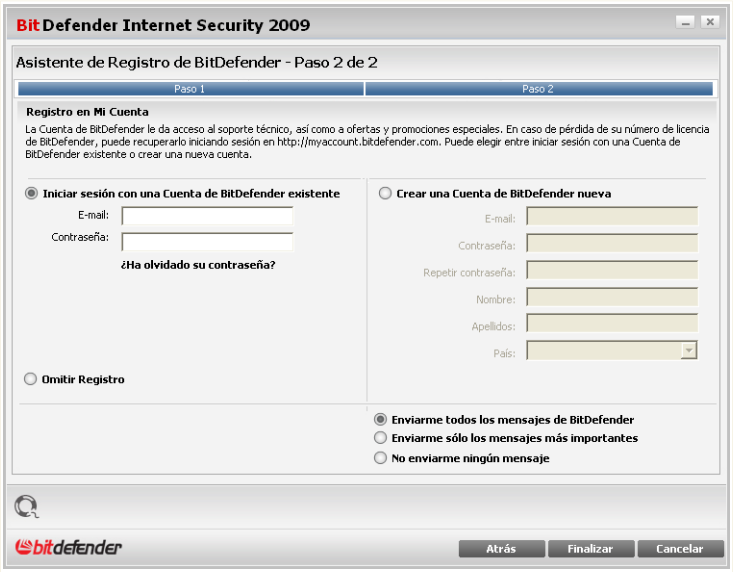
Puede encontrar su número de licencia en:

- la etiqueta del CD.
- la tarjeta de licencia del producto.
- el mensaje de confirmación de compra online.

Si no dispone de ningún número de licencia de BitDefender, haga clic en el enlace indicado para dirigirse a la tienda online de BitDefender y adquirir una.

Haga clic en **Siguiente** para continuar.

2.1.2. Paso 2/2 - Crear una Cuenta de BitDefender



Creación de la Cuenta

Si no desea crear ninguna cuenta de BitDefender por el momento, haga clic en **Omitir Registro** y a continuación haga clic en **Finalizar**. De lo contrario, siga los pasos indicados según su situación actual:

- "No tengo una cuenta de BitDefender" (p. 9)
- "Ya tengo una cuenta de BitDefender" (p. 9)

No tengo una cuenta de BitDefender

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. La contraseña debe contener 6 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 que aparecen en el mensaje enviado por el servicio de registro de BitDefender.

Opcionalmente, BitDefender puede informarle sobre ofertas especiales y promociones a través de la dirección de correo de su cuenta. Seleccione una de las opciones disponibles:

- **Enviarme todos los mensajes de BitDefender**
- **Enviarme sólo los mensajes importantes**
- **No enviarme ningún mensaje**

Haga clic en **Finalizar**.

Ya tengo una cuenta de BitDefender

BitDefender detectará automáticamente si previamente ha registrado una cuenta de BitDefender en su equipo. En este caso, introduzca la contraseña de su cuenta.

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.

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

Opcionalmente, BitDefender puede informarle sobre ofertas especiales y promociones a través de la dirección de correo de su cuenta. Seleccione una de las opciones disponibles:

- **Enviarme todos los mensajes de BitDefender**
- **Enviarme sólo los mensajes importantes**
- **No enviarme ningún mensaje**

Haga clic en **Finalizar**.

2.2. Asistente de Configuración

Cuando complete el Asistente de Registro, aparecerá un Asistente de Configuración. Este asistente le ayudará a personalizar las opciones de algunos módulos del producto y a configurar BitDefender para que realice algunas tareas de seguridad importantes.

No es obligatorio completar los pasos de este Asistente; sin embargo, recomendamos hacerlo para ganar tiempo y garantizar la seguridad de su sistema incluso antes que BitDefender Internet Security 2009 esté instalado.

Nota

Si no desea completar los pasos de este asistente, haga clic en **Cancelar**. BitDefender le informará sobre aquellos componentes que deben configurarse cuando abra la interfaz de usuario.

2.2.1. Paso 1/9 - Intro

Ventana de Bienvenida

Haga clic en **Siguiente** para continuar.

2.2.2. Paso 2/9 - Seleccione el Modo de Vista

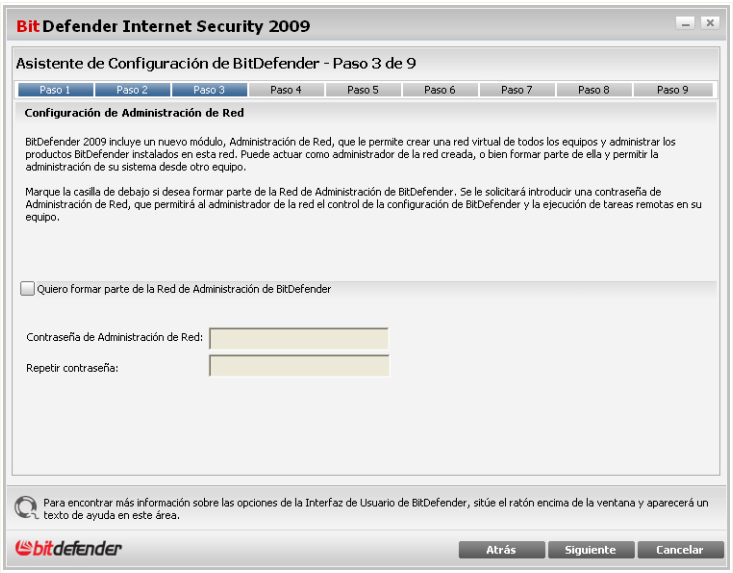
Modos de Vista

Elija entre las dos interfaces de usuario en función de su experiencia como usuario de BitDefender:

- **Vista Básica.** Interfaz muy simple, adecuada tanto para principiantes como para aquellos usuarios que deseen realizar tareas básicas y solucionar los problemas con rapidez. Deberá estar pendiente de las advertencias y alertas críticas de BitDefender, así como reparar las incidencias que vayan apareciendo.
- **Vista Avanzada.** Interfaz avanzada, adecuada para usuarios más técnicos que deseen configurar el producto por completo. Podrá configurar cada uno de los componentes del producto, así como realizar tareas avanzadas.

Haga clic en **Siguiente** para continuar.

2.2.3. Paso 3/9 - Configure la Red de Administración



Configuración de la Red de BitDefender

BitDefender le permite crear una red virtual de los equipos y administrar los productos BitDefender instalados en ésta.

Si desea que este equipo forme parte de la Red de Administración de BitDefender, siga estos pasos:

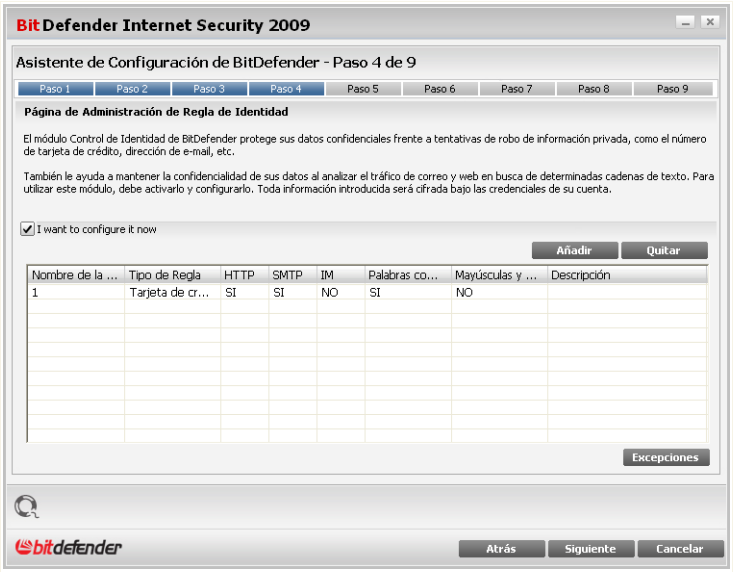
1. Seleccione la opción **Quiero formar parte de la Red de Administración de BitDefender**.
2. Introduzca la misma contraseña de administración en cada uno de los campos editables.

Importante

Esta contraseña permite que un usuario administrador gestione el producto BitDefender desde otro equipo.

Haga clic en **Siguiente** para continuar.

2.2.4. Paso 4/9 – Configure el Control de Identidad



Configuración del Control de Identidad

El Control de Identidad le protege del robo de información personal mientras está conectado a Internet. En función de las reglas que cree, el Control de Identidad analizará el tráfico web, e-mail y mensajería instantánea que sale de su equipo en busca de las cadenas de texto indicadas (por ejemplo, su número de tarjeta de crédito). En caso de coincidencia, se bloqueará la página web, correo o mensaje instantáneo correspondiente.

Si desea usar el Control de Identidad, siga estos pasos:

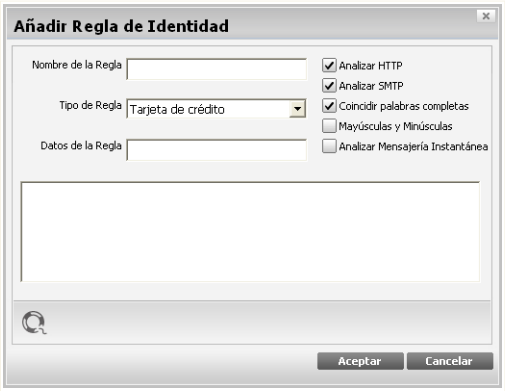
1. Seleccione la opción **Quiero usar el Control de Identidad**.
2. Cree las reglas necesarias para proteger su información personal. Para más información, por favor, consulte el apartado “Creando Reglas del Control de Identidad” (p. 15) de esta guía.

3. En caso necesario, puede definir excepciones a las reglas que ha creado. Para más información, por favor, consulte el apartado “Definiendo las Excepciones del Control de Identidad” (p. 16).

Haga clic en **Siguiente** para continuar.

Creando Reglas del Control de Identidad

Para crear una regla del Control de Identidad, haga clic en **Añadir**. Aparecerá la ventana de configuración.



Regla del Control de Identidad

Debe configurar los siguientes parámetros:

- **Nombre de la Regla** - introduzca el nombre de la regla en este campo editable.
- **Tipo de Regla** - elija el tipo de regla (dirección, nombre, tarjeta de crédito, PIN, etc).
- **Datos de la Regla** - introduzca los datos que desee proteger en este campo editable. Por ejemplo, si quiere proteger su número de tarjeta de crédito, introduzca toda la secuencia de números, o parte de ésta, en este campo.

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.

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 de texto detectada coinciden en mayúsculas y minúsculas.

Para identificar rápidamente la información que bloquea cada regla, introduzca una descripción en este campo de texto.

Para indicar el tipo de tráfico que debe analizarse, configure estas opciones:

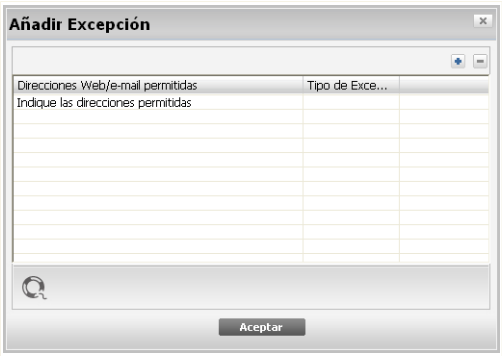
- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (correo) y bloquea los mensajes salientes que coinciden con los datos de la regla.
- **Analizar Mensajería Instantánea** - analiza el tráfico de Mensajería Instantánea y bloquea los mensajes de chat salientes que coinciden con los datos de la regla.

Haga clic en **Aceptar** para añadir la regla.

Definiendo las Excepciones del Control de Identidad

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 del Control de Identidad

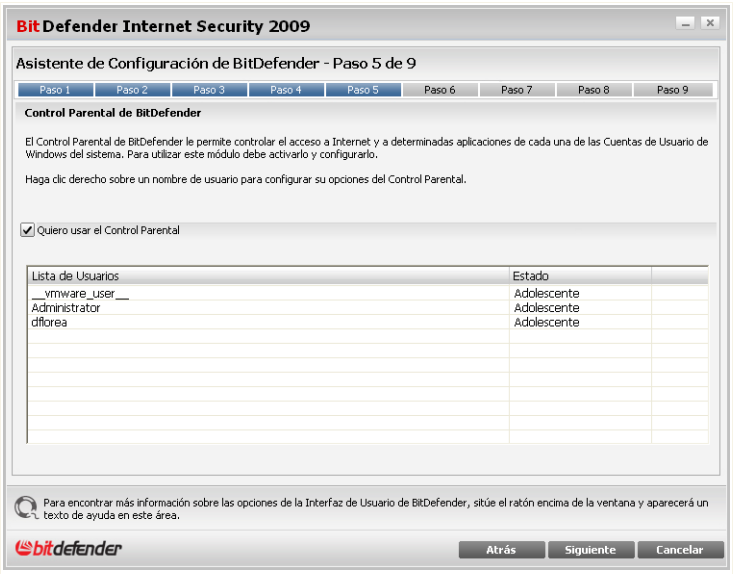
Para añadir una excepción, siga estos pasos:

1. Haga clic en el botón **Añadir** para añadir 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, selecciónela y haga clic en el botón **Eliminar**.

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

2.2.5. Paso 5/9 – Configure el Control de Contenido



Configuración del Control de Contenido

Nota
Acest modul este disponibil doar pentru produsele BitDefender Internet Security 2009, respectiv BitDefender Total Security 2009.

El Control de Contenido de BitDefender le permite controlar el acceso a Internet y a determinadas aplicaciones de cada una de las cuentas de usuario de Windows del sistema.

Si desea usar el Control de Contenido, siga estos pasos:

1. Seleccione la opción **Quiero usar el Control de Contenido**.
2. Haga clic derecho en el nombre de cada una de las cuentas de Windows y seleccione el perfil del Control de Contenido que desee aplicar.

Perfil	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.

Nota

Para configurar por completo el Control de Contenido o desactivarlo en determinadas cuentas de Windows, abra BitDefender, cambie a la Vista Avanzada y diríjase al apartado Control de Contenido. Puede configurar Control de Contenido para que bloquee:

- páginas web con contenido inadecuado.
- la conexión a Internet durante determinados periodos de tiempo (por ejemplo, en las horas de estudio).
- páginas web, mensajes de correo y conversaciones de mensajería instantánea que contengan determinadas palabras clave.
- aplicaciones como juegos, chat, aplicaciones de intercambio de archivos u otros.
- mensajes enviados por contactos de mensajería instantánea que no provengan de los contactos permitidos.

Haga clic en **Siguiente** para continuar.

2.2.6. Paso 6/9 - Configure el Informe de Virus en Tiempo Real

Configuración del Informe de Virus en Tiempo Real

BitDefender puede enviar a los Laboratorios BitDefender informes anónimos sobre los virus detectados en su equipo, y así poder detectar nuevas epidemias de virus.

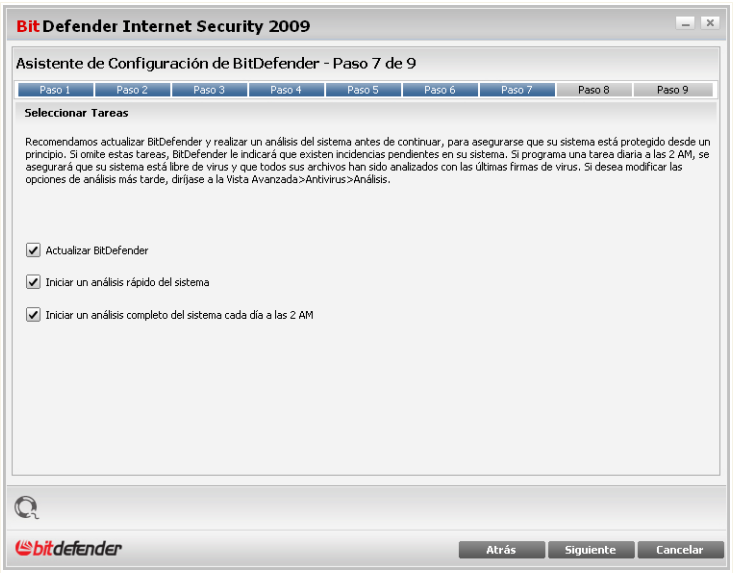
Puede configurar las siguientes opciones:

- **Enviar Informes de Virus** - envía a los Laboratorios BitDefender informes acerca de los virus identificados en su equipo.
- **Activar Detección de Epidemias de BitDefender** - envía a los Laboratorios BitDefender informes sobre potenciales epidemias de virus.

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

Haga clic en **Siguiente** para continuar.

2.2.7. Paso 7/9 – Seleccione la Tarea a Ejecutar



Selección de la Tarea

Configure BitDefender Internet Security 2009 para que realice 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 archivos de las carpetas `Windows` y `Archivos de Programa` no están infectados.
- **Programar un análisis completo del sistema cada día a las 02:00 AM** - ejecuta un análisis completo del sistema cada día a las 2 AM.

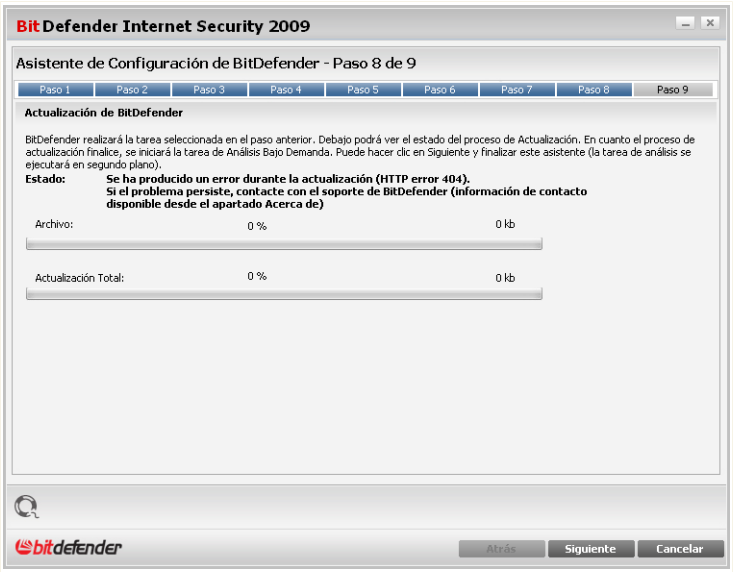
Importante

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.

2.2.8. Paso 8/9 - Espere a que Finalicen las Tareas

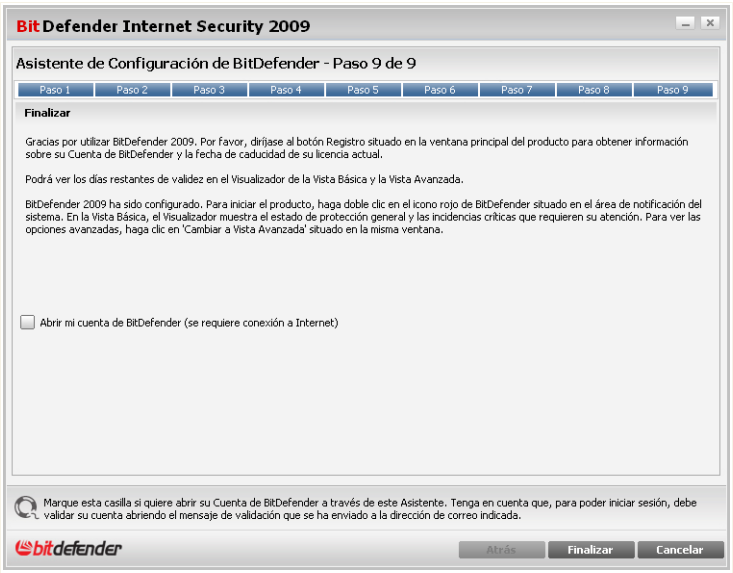


Estado de la Tarea

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.

2.2.9. Step 9/9 - Finalizar



Finalizado

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

Haga clic en **Finalizar**.

3. Reparar o Desinstalar BitDefender

Si desea reparar o desinstalar **BitDefender Internet Security 2009**, siga estos pasos en el menú Inicio de Windows: **Inicio → Programas → BitDefender 2009 → Reparar o Desinstalar**.

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

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

  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 2009.

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

- **Eliminar** - para eliminar todos los componentes instalados.

  Nota
  Recomendamos seleccionar 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 2009 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

4. Primeros Pasos

Una vez tenga BitDefender instalado, su equipo estará protegido.

4.1. Iniciar BitDefender Internet Security 2009

El primer paso para sacar el máximo provecho a BitDefender es iniciar la aplicación.

Para acceder a la interfaz de BitDefender Internet Security 2009, haga clic en el menú Inicio de Windows y siga estos pasos **Inicio** → **Programas** → **BitDefender 2009** → **BitDefender Internet Security 2009**, o bien haga doble clic en el **icono de BitDefender** situado en el área de notificación del sistema.

4.2. Modo de Vista de la Interfaz de Usuario

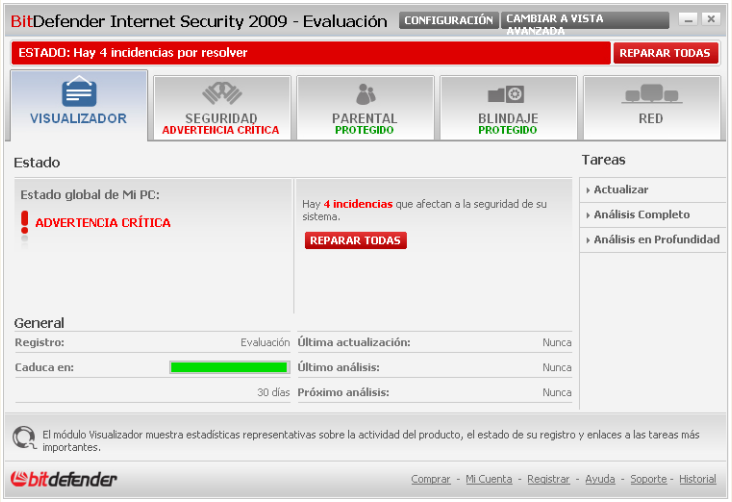
BitDefender Internet Security 2009 satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. En consecuencia, la interfaz de usuario está diseñada para adaptarse a cada categoría de usuarios.

Puede elegir entre la vista Básica y la Avanzada, en función de su experiencia como usuario con nuestro producto.

Nota
Puede alternar fácilmente entre estos modos de vista haciendo clic, respectivamente, en el botón **Vista Básica** o **Vista Avanzada**.

4.2.1. Vista Básica

La Vista Básica es una sencilla interfaz que le permite acceder a todos los módulos a un nivel muy básico. Deberá estar pendiente de las advertencias y alertas críticas, así como reparar las incidencias no deseadas.



Vista Básica

- En la parte superior de la ventana se encuentran dos botones y una barra de estado.

Elemento	*Descripción*
Configuración	Abre una ventana desde la que podrá activar o desactivar módulos de seguridad importantes con suma facilidad (Cortafuego, Modo Oculto, Actualización Automática, Modo Trabajo, etc.).
Vista Avanzada	Abre la ventana de Vista Avanzada. Desde aquí podrá ver una lista de todos los módulos y podrá configurar en detalle cada uno de los componentes. BitDefender recordará esta opción la próxima vez que acceda a la interfaz de usuario.
Estado	Contiene información sobre las incidencias relacionadas con la seguridad de su equipo y le ayuda a repararlas.

- En la parte central de la ventana encontrará cinco pestañas.

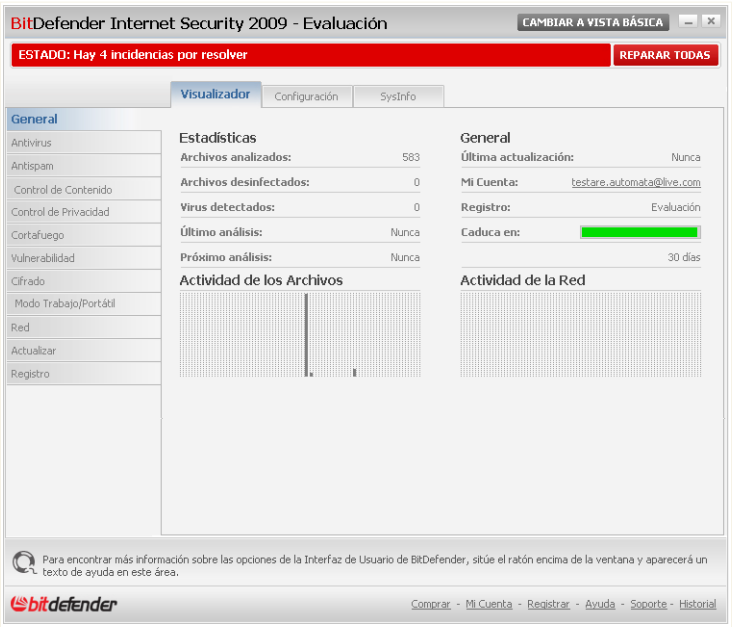
Pestaña	Descripción
Visualizador	Muestra estadísticas representativas sobre la actividad del producto, el estado de su registro y enlaces a las tareas bajo demanda más importantes.
Seguridad	Muestra el estado de los módulos de seguridad (antivirus, antiphishing, cortafuego, antispam, cifrado de IM, privacidad, comprobación de vulnerabilidades y actualización) junto con enlaces a tareas antivirus, actualización y comprobación de vulnerabilidades.
Parental	Muestra el estado del módulo que le permite restringir el acceso a Internet o a determinadas aplicaciones por parte de otros usuarios del sistema.
Administrador de Archivos	Muestra el estado de los módulos blindaje de archivos, así como enlaces a tareas de relacionadas con éste.
Red	Muestra la estructura de la red de administración.

- Además, la ventana de Vista Básica contiene algunos accesos directos que pueden resultarle útiles.

Enlace	Descripción
Mi Cuenta	Le permite crear o iniciar sesión con su cuenta de BitDefender. La cuenta de BitDefender le da acceso gratuito al soporte técnico.
Registrar	Le permite introducir un nuevo número de licencia o ver el número de licencia actual y su estado de registro.
Ayuda	Abre el archivo de ayuda que le enseñará cómo utilizar BitDefender.
Soporte	Le permite ponerse en contacto con el equipo de soporte de BitDefender.
Historial	Le permite ver un historial detallado sobre las tareas que BitDefender ha realizado en su sistema.

4.2.2. Vista Avanzada

La Vista Avanzada le da acceso a cada uno de los diferentes componentes del producto BitDefender. Podrá configurar las opciones y características avanzadas.



Vista Avanzada

- En la parte superior de la ventana se encuentra un botón y una barra de estado.

Elemento	Descripción
Vista Básica	Abre la ventana de Vista Básica. Desde aquí podrá ver la interfaz básica de BitDefender y los principales módulos (Seguridad, Optimizador, Administrador de Archivos, Red) y el Visualizador. BitDefender recordará esta opción la próxima vez que acceda a la interfaz de usuario.

Elemento	Descripción
Estado	Contiene información sobre las incidencias relacionadas con la seguridad de su equipo y le ayuda a repararlas.

- En la parte izquierda de la ventana hay un menú que contiene todos los módulos de seguridad.

Módulo	Descripción
General	Le permite acceder a la configuración general o ver el visualizador e información del sistema.
Antivirus	Le permite configurar la protección antivirus en tiempo real y operaciones de análisis, establecer excepciones y configurar el módulo cuarentena.
Antispam	Le permite configurar en detalle el módulo antispam y así mantener su bandeja de entrada libre de Spam.
Cortafuego	Le permite proteger su sistema frente a los intentos de conexión externos o internos no autorizados. Algo parecido a tener un guardia en su puerta – vigilará su conexión a Internet y monitorizará todas las conexiones que decida autorizar o bloquear.
Control de Privacidad	Le ayuda a impedir el robo de datos de su equipo y protege su privacidad mientras está conectado a Internet.
Control de Contenido	Le permite impedir el acceso a contenido inapropiado a través de reglas de acceso personalizadas.
Cifrado	Le permite cifrar las conversaciones de Yahoo y Windows Live (MSN) Messenger, así como cifrar sus archivos, carpetas o particiones críticos.
Vulnerabilidad	Le permite tener actualizado el software crucial de su PC.
Modo Trabajo/Portátil	Le permite posponer tareas de análisis o copia de BitDefender cuando su portátil funcione con batería y desactivar todas las alertas mientras juega.
Red	Le permite configurar y administrar los equipos de una pequeña red de usuarios.

Módulo	Descripción
Actualización	Le permite obtener información sobre las últimas actualizaciones, actualizar el producto y configurar el proceso de actualización en detalle.
Registrar	Le permite configurar BitDefender Internet Security 2009, cambiar el número de licencia o crear una cuenta de BitDefender.

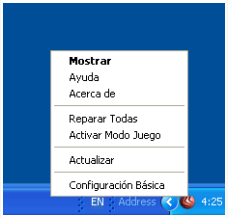
- Además, la ventana de Vista Avanzada contiene algunos accesos directos que pueden resultarle útiles.

Enlace	Descripción
Mi Cuenta	Le permite crear o iniciar sesión con su cuenta de BitDefender. La cuenta de BitDefender le da acceso gratuito al soporte técnico.
Registrar	Le permite introducir un nuevo número de licencia o ver el número de licencia actual y su estado de registro.
Ayuda	Abre el archivo de ayuda que le enseñará cómo utilizar BitDefender.
Soporte	Le permite ponerse en contacto con el equipo de soporte de BitDefender.
Historial	Le permite ver un historial detallado sobre las tareas que BitDefender ha realizado en su sistema.

4.3. Icono de BitDefender en el Área de Notificación del Sistema

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

Si hace doble clic en este icono se abrirá la interfaz de BitDefender. Si hace clic derecho sobre el icono, aparecerá un menú contextual desde el que podrá administrar rápidamente el producto BitDefender.



Icono de BitDefender

- **Mostrar** - abre BitDefender.
- **Ayuda** - abre el archivo de ayuda en el que se explica el funcionamiento y uso de BitDefender Internet Security 2009.
- **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.
- **Actualizar** - realiza una actualización inmediata. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización.
- **Configuración básica** - le permite activar o desactivar fácilmente los módulos de seguridad más importantes. Aparecerá una nueva ventana desde la que podrá activar / desactivar los módulos con un simple clic.

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

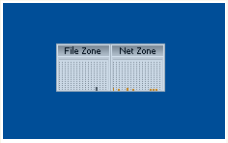
Si hay incidencias críticas que afectan a la seguridad de su sistema, aparecerá una marca de exclamación encima del icono de BitDefender. Puede situar el cursor encima del icono para ver el número de incidencias que afectan a la seguridad de su sistema.

4.4. 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 grises (**Archivos**) representan el número de archivos analizados por segundo, en una escala de 0 a 50.

Las barras narajas mostradas en la zona **Internet** representan el número de KBytes transferidos (enviados y recibidos por Internet) por segundo, en 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. Para más información, por favor, consulte el "*Análisis al Arrastrar y Soltar*" (p. 172) de esta guía de usuario.

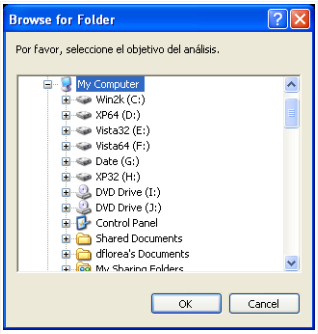
Para ocultar la barra de actividad haga clic derecho encima y seleccione **Ocultar**. Para ocultar completamente esta ventana, siga estos pasos:

1. Haga clic en **Vista Avanzada** (si está usando la **Vista Básica**).
2. Haga clic en el módulo **General** del menú situado a la izquierda.
3. Haga clic en la pestaña **Configuración**.
4. Desmarque la casilla **Activar barra de Actividad del Análisis (gráfico sobre la actividad del producto)**.

4.5. 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, diríjase al menú Inicio de Windows y siga estos pasos: **Inicio → Programas → BitDefender 2009 → Análisis Manual de BitDefender** Aparecerá la siguiente pantalla:



Análisis Manual de BitDefender

Sólo tiene que navegar entre sus carpetas, seleccionar la carpeta que desea analizar y hacer clic en **Aceptar**. Aparecerá el Analizador de BitDefender y le guiará a través del proceso de análisis.

4.6. Modo Trabajo

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

- Minimiza el consumo de procesador y memoria
- Pospone las tareas de análisis y actualización
- Elimina todas las alertas y ventanas emergentes
- Analiza sólo los archivos más importantes

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

4.6.1. Usando el Modo Trabajo

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

- Clic derecho en el icono de BitDefender de la Bandeja del Sistema y seleccione **Activar Modo Trabajo**.
- Pulse `Ctrl+Shift+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.

4.6.2. Cambiando el Atajo de Teclado del Modo Trabajo

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

1. Haga clic en **Vista Avanzada** (si está usando la **Vista Básica**).
2. Haga clic en **Modo Trabajo/Portátil** del menú de la izquierda.
3. Haga clic en la pestaña **Modo Trabajo**.
4. Haga clic en el botón **Opciones Avanzadas**.
5. Debajo de la opción **Usar Atajos de Teclado**, configure la combinación de teclas deseada:

- Elija las teclas que desea utilizar seleccionado alguna de las siguientes: 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 correspondiente a **Usar Atajos de Teclado**, desactivará la combinación de teclas.

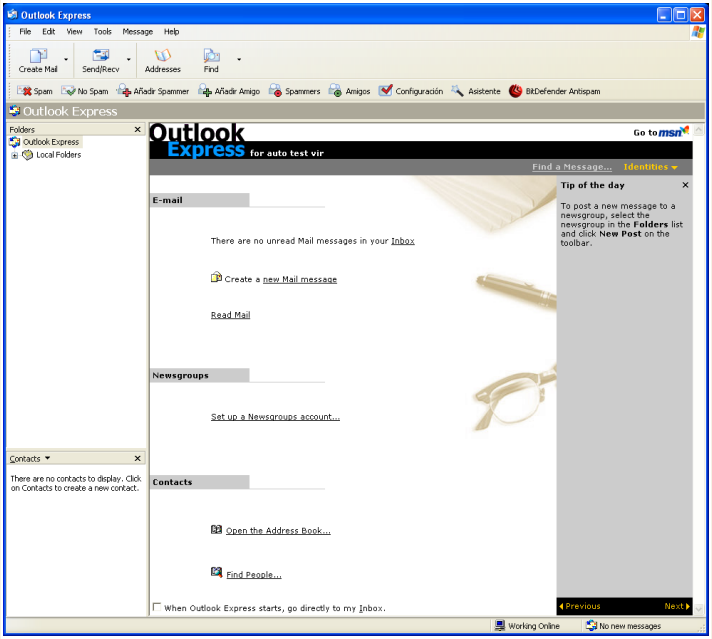
4.7. Integración en Clientes de Correo

BitDefender se integra a través de una barra de herramientas muy intuitiva y fácil de usar en los siguientes clientes de correo:

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

4.7.1. 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).

A continuación se explican las funciones de los botones de la Barra de Herramientas de BitDefender:

- **Es Spam** - envía 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** - envía 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

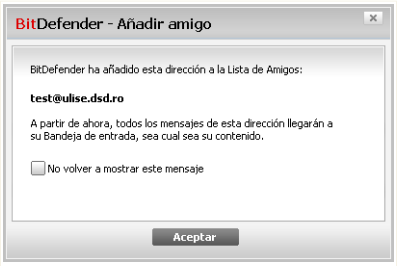
Seleccione **No volver a mostrar este mensaje** si no quiere que se le solicite la confirmación al añadir una nueva dirección a la lista de spammers.

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** - abre 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 en el 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 direcciones que desee y haga clic en para añadirlasa la **Lista de Spammers**. Si hace clic en se añadirán todas las direcciones de correo 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 al cargar una lista previamente guardada seleccione **Vaciar lista al cargar**.

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

- **Amigos** - abre la **Lista de Amigos** que contiene todas las direcciones desde las que siempre quiere recibir mensajes, independientemente de su contenido.

> ***Nota***
> Cualquier mensaje que provenga de una dirección incluida en la **Lista de Amigos** llegará directamente 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 en el 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 direcciones que desee y haga clic en to add them to the **Lista de Amigos**. Si hace clic en se añadirán todas las direcciones de correo 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 al cargar 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 volver a entrenar al 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 el que puede desactivar las ventanas de confirmación de los botones **Añadir Spammer** y **Añadir Amigo**.

Nota

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

- **Asistente** - abre el asistente que le guiará a través del proceso de entrenamiento del Filtro Bayesiano, para así mejorar la eficacia de BitDefender Antispam. También podrá añadir direcciones de su **Libreta de Direcciones** a la **Lista de Amigos** / **Lista de Spammers**.
- **BitDefender Antispam** - abre la interfaz de usuario de BitDefender.

4.7.2. Asistente de Configuración Antispam

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

Nota
Puede iniciar el asistente cuando quiera, haciendo clic en el botón **Asistente** de 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

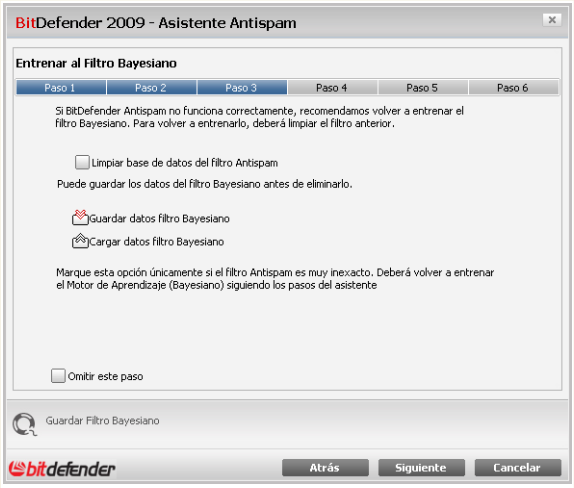
Completar la Lista de Amigos

Aquí puede ver todas las direcciones de su **Libreta de Direcciones**. Por favor seleccione las direcciones que desee añadir a la **Lista de Amigos** (recomendamos seleccionarlas todas). Recibirá todos los mensajes que provengan 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

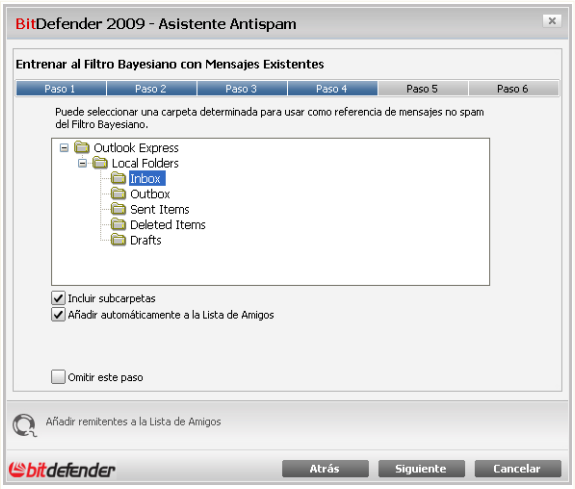
Si nota que su filtro antispam está empezando a perder eficacia, puede ser debido un entrenamiento inadecuado del filtro Bayesiano (por ejemplo, marcar erróneamente mensajes legítimos como Spam, o viceversa). Si su filtro es muy impreciso, tal vez tenga que borrar la base de datos del filtro y volver a entrenar el filtro siguiendo los pasos indicados por el asistente.

Seleccione la opción **Limpiar la base de datos del filtro Antispam** si desea reiniciar 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 contenga mensajes legítimos. Estos mensajes serán utilizados para entrenar el filtro antispam.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir subcarpetas** - para incluir las subcarpetas a 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 contenga mensajes de Spam. Estos mensajes serán utilizados para entrenar el filtro antispam.

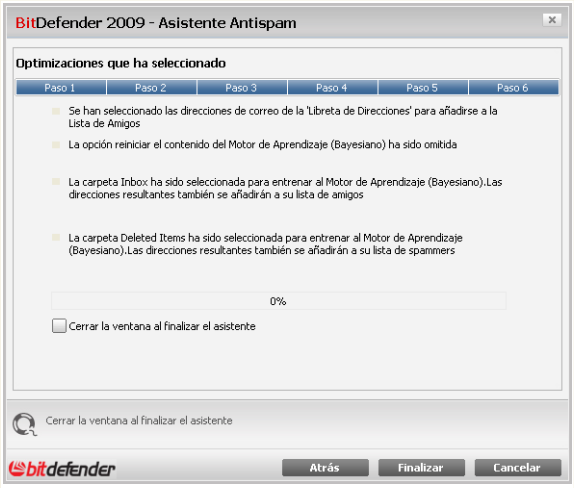
Importante
Por favor, asegúrese que la carpeta seleccionada no contiene ningún mensaje legítimo, sino la eficacia del filtro antispam se verá reducida considerablemente.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir subcarpetas** - para incluir las subcarpetas a 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 del Asistente de Configuración. Puede hacer cualquier modificación que considere oportuna, volviendo al paso anterior (clic en **Atrás**).

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

4.8. Integración con Navegadores Web

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.

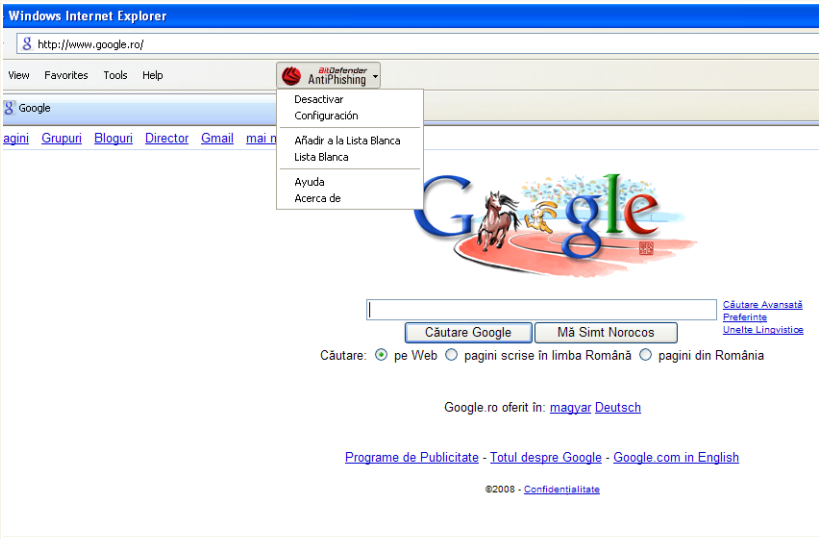
BitDefender se integra a través de una barra de herramientas muy intuitiva y fácil de usar en los siguientes navegadores:

- Internet Explorer
- Mozilla Firefox

Puede administrar la protección antiphishing y la Lista Blanca fácilmente a través de la barra de herramientas de BitDefender Antiphishing, integrada en los navegadores citados anteriormente.

La barra de herramientas antiphishing, representada por el **icono de BitDefender**, está situada en la parte superior del navegador. 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**.



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.

4.9. Integración con Programas de Mensajería

BitDefender ofrece funciones de cifrado para proteger sus documentos confidenciales y las conversaciones de mensajería instantánea a través de Yahoo Messenger y MSN Messenger.

Por defecto, BitDefender cifra todas sus sesiones de chat por mensajería instantánea siempre y cuando:

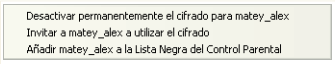
- Su contacto de chat tenga instalada una versión de BitDefender que soporte el Cifrado de IM, y esta función esté activada para la aplicación utilizada para conversar.
- Su contacto de chat utilice Yahoo Messenger o Windows Live (MSN) Messenger.

Importante
BitDefender no cifrará la conversación si su contacto utiliza una aplicación web para chatear, como Meebo, u otras aplicaciones que soportan Yahoo Messenger o MSN.

Puede configurar fácilmente el cifrado de la mensajería instantánea usando la barra de herramientas de BitDefender en la ventana de chat.

Haciendo clic derecho en la barra de herramientas de BitDefender se le mostrarán las siguientes opciones:

- Activar / desactivar permanentemente el cifrado de determinado contacto de chat
- Invitar a determinado contacto de chat a utilizar el cifrado
- Eliminar determinado contacto de chat de la lista negra del Control de Contenido

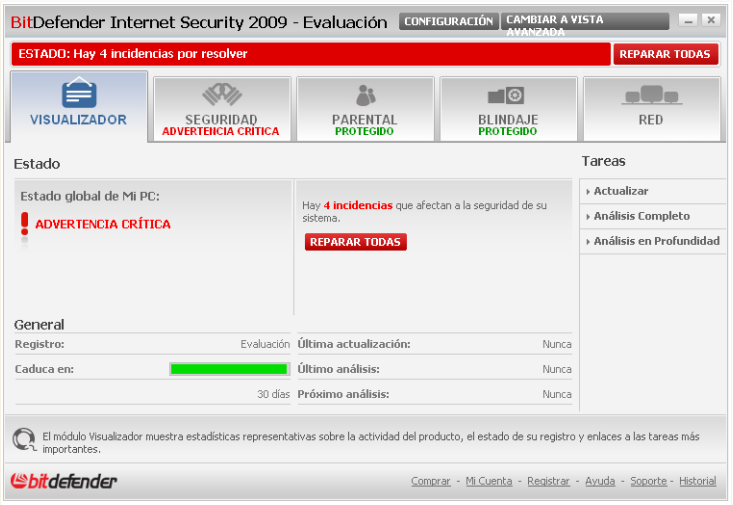


Opciones de Cifrado de Mensajería Instantánea (IM)

Haga clic una de las opciones citadas anteriormente para utilizarlas.

5. Visualizador

Al hacer clic en la pestaña Visualizador, se le mostrarán estadísticas representativas sobre la actividad del producto, el estado de su registro y enlaces a las tareas más importantes.



Visualizador

5.1. General

Aquí puede ver un resumen de las estadísticas relacionadas con el estado de la actualización, el estado de su cuenta e información sobre el registro y la licencia.

Elemento	Descripción
Última actualización	Indica la fecha en la que el producto BitDefender se actualizó por última vez. Por favor, realice actualizaciones regularmente para estar completamente protegido.

Elemento	Descripción
Mi Cuenta	Indica la dirección de correo que puede utilizar para acceder a su cuenta de copia online, para recuperar su licencia o para beneficiarse del soporte de BitDefender u otros servicios.
Registro	Le indica el tipo de licencia utilizada y su estado. Para mantener su equipo protegido, debería renovar o actualizar su licencia de BitDefender una vez haya caducado.
Caduca en	Indica el número de días restantes hasta que caduque la licencia.

Para actualizar BitDefender, simplemente haga clic en el botón **Actualizar** situado en el área de tareas.

Para crear o iniciar sesión con su cuenta de BitDefender, siga estos pasos:

1. Haga clic en el enlace **Mi Cuenta** situado en la parte inferior de la ventana. Se abrirá una página web.
2. Introduzca su nombre de usuario y contraseña, y haga clic en el botón **Login**.
3. Para crear una cuenta de BitDefender, seleccione **¿No tiene una cuenta?** e introduzca la información solicitada.

Nota
Los datos que introduzca aquí serán confidenciales.

Para registrar BitDefender Internet Security 2009, siga estos pasos:

1. Haga clic en el enlace **Mi Cuenta** situado en la parte inferior de la ventana. Se abrirá el Asistente de Registro.
2. Seleccione la opción **Quiero registrar el producto con un nuevo número de licencia**.
3. Introduzca el número de licencia en el campo de texto correspondiente.
4. Haga clic en **Finalizar**.

Para comprar una nueva licencia, siga esto pasos:

1. Haga clic en el enlace **Mi Cuenta** situado en la parte inferior de la ventana. Se abrirá el Asistente de Registro.
2. Haga clic en el enlace **Renueve su número de licencia de BitDefender**. Se abrirá una página web.

3. Haga clic en el botón **Comprar**.

5.2. Tareas

Tareas - Le muestra enlaces a las tareas de seguridad más importantes: análisis del sistema, análisis en profundidad y actualización.

Dispone de los siguientes botones:

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

5.2.1. 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
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.

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

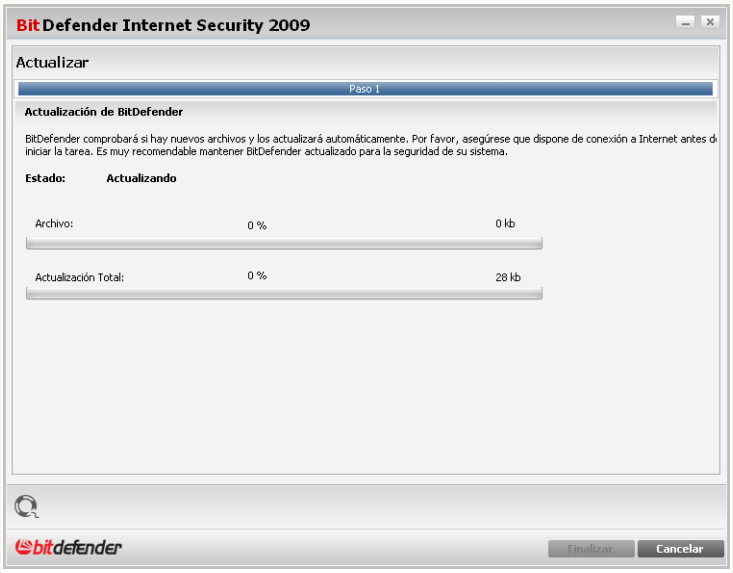
Cuando inicia un proceso de análisis bajo demanda, ya sea rápido o completo, aparecerá el Analizador de BitDefender.

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

5.2.2. 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 equipo y **cada hora** a partir de ese momento. 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 **Cancelar**. 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.

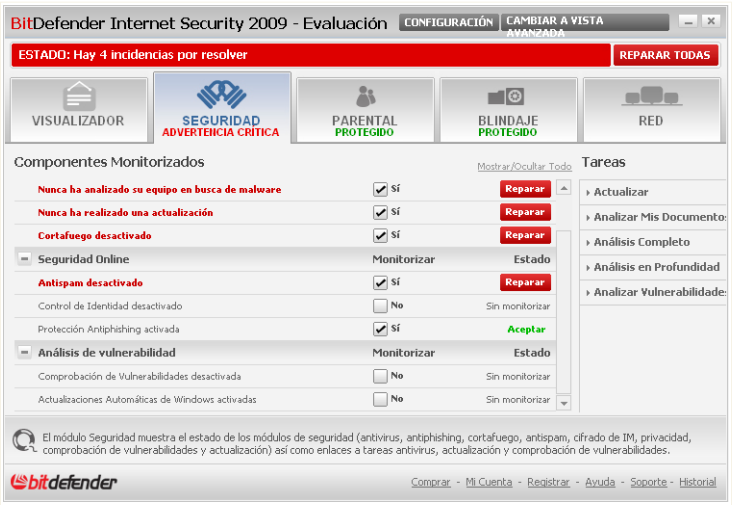
Haga clic en **Reiniciar** para reiniciar el equipo inmediatamente.

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

6. 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**.



Seguridad

El módulo Seguridad consta de dos apartados:

- **Componentes Monitorizados** - Le permite ver la lista completa de todos los componentes monitorizados de cada módulo de seguridad. Puede elegir los módulos que desea monitorizar. Recomendamos activar la monitorización de todos los componentes.
- **Tareas** - Aquí encontrará enlaces a las tareas de seguridad más importantes: análisis del sistema, análisis en profundidad y actualización.

6.1. Componentes Monitorizados

Los componentes monitorizados se agrupan en varias categorías.

Categoría	Descripción
Seguridad Local	Aquí puede comprobar el estado de cada uno de los módulos de seguridad encargados de proteger los objetos almacenados en su equipo (archivos, registro, memoria, etc.).
Seguridad Online	Aquí puede comprobar el estado de cada uno de los módulos de seguridad encargados de proteger sus transacciones online y la actividad de su equipo mientras está conectado a Internet.
Análisis de Vulnerabilidad	Desde aquí puede comprobar si el software crucial de su PC está actualizado. También se comprueba si las cuentas de Windows cumplen los requisitos de seguridad.

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

6.1.1. Seguridad local

Sabemos que es importante estar informado cuando se produce algún problema que afecte a la seguridad de su equipo. Al monitorizar los módulos de seguridad, BitDefender Internet Security 2009 le hará saber si la configuración aplicada puede afectar a la seguridad del equipo, o le avisará cuando olvide realizar alguna tarea de seguridad importante.

Las incidencias relativas a la seguridad local están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Protección de archivos en tiempo real activada	Asegura el análisis de todos los archivos a los que accede o bien utilizan las aplicaciones que se ejecutan en el sistema.
Nunca ha analizado su equipo en busca de malware	Recomendamos encarecidamente iniciar una tarea de análisis bajo demanda cuanto antes, para asegurarse que los archivos almacenados en su equipo están libres de malware.
Actualización automática activada	Mantenga activada la actualización automática para asegurarse que las firmas de malware de su producto BitDefender se actualizan regularmente.

Incidencia	Descripción
Actualizando	Se está realizando una actualización del producto y firmas de malware.
Cortafuego activado	Protege su equipo frente a hackers y ataques externos.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

6.1.2. Seguridad online

Las incidencias relativas a la seguridad online están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Antispam activado	Le asegura que sus e-mails son analizados en busca de malware y filtrados en busca de spam.
Control de Identidad activado	Le ayuda a mantener a salvo su información confidencial, al analizar todo el tráfico web y el correo en busca de determinadas cadenas de texto. Recomendamos activar el Control de Identidad para mantener a salvo sus datos confidenciales (dirección de correo, IDs de usuario, contraseñas, números de tarjetas de crédito, etc) y impedir su robo.
Antiphishing activado para Mozilla Firefox	BitDefender le protege contra los intentos de phishing mientras navega por Internet.

Incidencia	Descripción
Antiphishing activado para Internet Explorer	BitDefender le protege contra los intentos de phishing mientras navega por Internet.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

6.1.3. Análisis de Vulnerabilidad

Las incidencias relativas a las vulnerabilidades están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Comprobación de Vulnerabilidades activada	Monitoriza las Actualizaciones de Microsoft Windows y Microsoft Office, así como las contraseñas de las cuentas de Windows, para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.
Actualizaciones Críticas de Microsoft	Instala las actualizaciones críticas de Microsoft disponibles.
Otras actualizaciones de Microsoft	Instala las actualizaciones no-críticas de Microsoft disponibles.
Actualizaciones Automáticas de Windows activadas	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.

Incidencia	Descripción
Admin (Contraseña Segura)	Indica la fortaleza de la contraseña de determinados usuarios.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

6.2. Tareas

Tareas - Le muestra enlaces a las tareas de seguridad más importantes: análisis del sistema, análisis en profundidad y actualización.

Dispone de los siguientes botones:

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

6.2.1. 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
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
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 personalizado	Use esta tarea para analizar archivos y carpetas concretos.

Nota
A través de las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso requerirá bastante 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 el Analizador de BitDefender.

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

Análisis personalizado

Al hacer clic en el botón **Análisis personalizado** y siguiendo los pasos del asistente, podrá crear una tareas de análisis personalizadas y, opcionalmente, guardarlas como tareas rápidas.

Paso 1/4 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

Ventana de Bienvenida

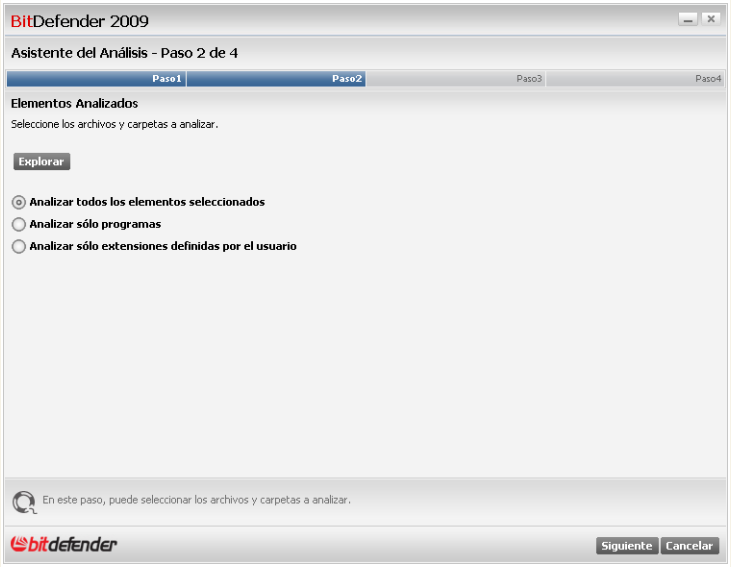
Este asistente le ayudará a analizar su equipo en busca de cualquier amenaza que pueda afectarle. Podrá elegir las carpetas y/o archivos a analizar, así como definir las acciones que se aplicarán a los archivos infectados. También recibirá un informe del análisis que le ayudará a evaluar el nivel de seguridad de su sistema. Por favor, siga todos los pasos del asistente y configure el proceso de análisis acorde con sus necesidades.

Nota
Para omitir este paso en futuros análisis, marque la casilla correspondiente.

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 2/4 - Seleccione los Elementos a Analizar

En este paso, puede elegir los archivos y carpetas que se analizarán.



Selección de los Elementos a Analizar

Haga clic en Explorar para seleccionar determinados archivos y/o carpetas de su equipo.

Dispone de las siguientes opciones:

Opción	Descripción
Analizar todos los elementos seleccionados	Seleccione esta opción para analizar sólo los elementos seleccionados anteriormente.
Analizar sólo programas	Seleccione esta opción para analizar únicamente archivos de programas y aplicaciones.
Analizar sólo extensiones definidas por el usuario	Seleccione esta opción para analizar sólo los archivos con determinadas extensiones. Aparecerá un cuadro de texto en el que podrá indicar estas extensiones. ***Nota*** Debe separar las extensiones con punto y coma ";" (Ej: exe;com;ivd;)

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 3/4 - Seleccione la Acción a Realizar

En este paso, puede elegir las acciones que deben aplicarse a las amenazas encontradas y seleccionar las opciones de análisis usando el control deslizante.

Selección de la Acción a Realizar

Puede seleccionar la acción a realizar en el menú correspondiente:

- **Al encontrar un archivo infectado**
- **Al encontrar un archivo sospechoso**
- **Al encontrar un archivo oculto**

Al mismo tiempo, puede configurar el nivel de protección del análisis. 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 de protección adecuado.

Hay 4 niveles de protección:

Nivel de Protección	Descripción
Alto	Ofrece un alto nivel de seguridad. El nivel de consumo de recursos es alto. ■ analiza todos los archivos y comprimidos ■ analiza en busca de virus y spyware ■ analiza en busca de procesos ocultos
Mediana	Ofrece un nivel de seguridad medio. El nivel de consumo de recursos es moderado. ■ analiza todos los archivos ■ analiza en busca de virus y spyware
Bajo	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. ■ analiza sólo archivos de programas ■ analiza en busca de virus
Personalizado	Desde aquí puede seleccionar sus propias opciones de análisis. Haga clic en Personalizar y establezca el nivel de análisis deseado. Seleccione las casillas correspondientes al tipo de malware que desea buscar en su equipo durante el proceso de análisis.

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 4/4 - Establezca las Opciones Adicionales

En este paso, puede ajustar algunas opciones adicionales antes de iniciar el proceso de análisis.

Configuración de las Opciones Adicionales

Para guardar la configuración de esta tarea de análisis y poder utilizarla en el futuro, seleccione la casilla correspondiente e introduzca un nombre apropiado en el cuadro de texto.

Nota
Aparecerá un nuevo botón con el nombre introducido anteriormente debajo del menú de tareas.

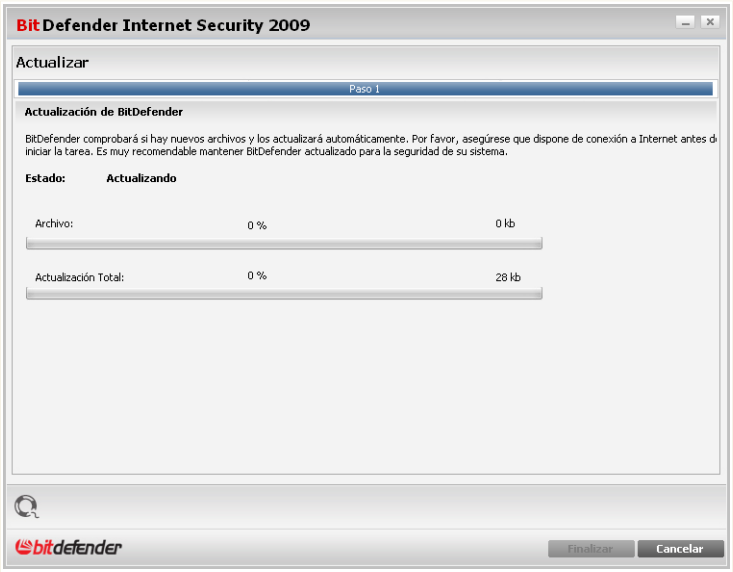
Si desea apagar el equipo una vez finalice el proceso de análisis, seleccione la casilla correspondiente.

Haga clic en **Iniciar Análisis** y siga el asistente guiado de tres pasos para completar el proceso de análisis.

6.2.2. 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 equipo y **cada hora** a partir de ese momento. 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 **Cancelar**. 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.

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.

6.2.3. Buscando Vulnerabilidades

El Análisis de Vulnerabilidad comprueba las Actualizaciones de Microsoft Windows y Microsoft Office, así como las contraseñas de las cuentas de Windows, para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.

Para comprobar las vulnerabilidades de su equipo, haga clic en **Análisis de Vulnerabilidad** y siga los pasos del Asistente.

Comprobando Vulnerabilidades

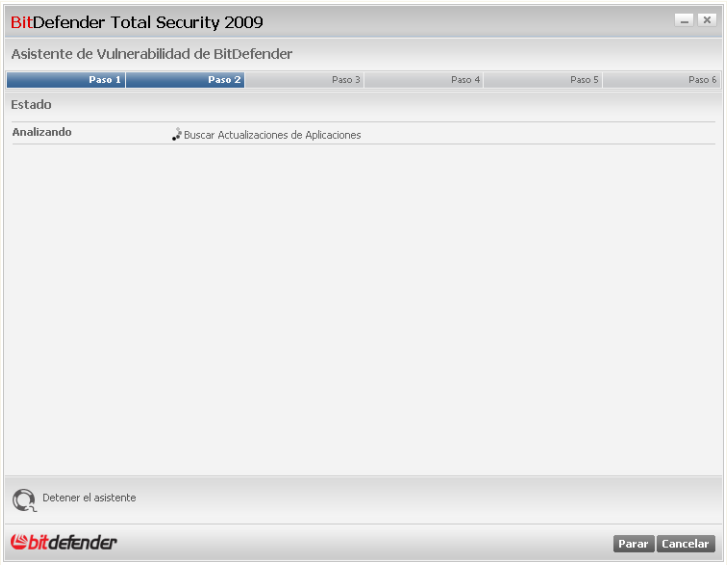
Para comprobar las vulnerabilidades de su equipo, haga clic en **Comprobar** y siga los pasos del Asistente.

Paso 1/6 – Seleccione las Vulnerabilidades a Comprobar

Vulnerabilidades

Haga clic en **Siguiente** para analizar su sistema en busca de las vulnerabilidades seleccionadas.

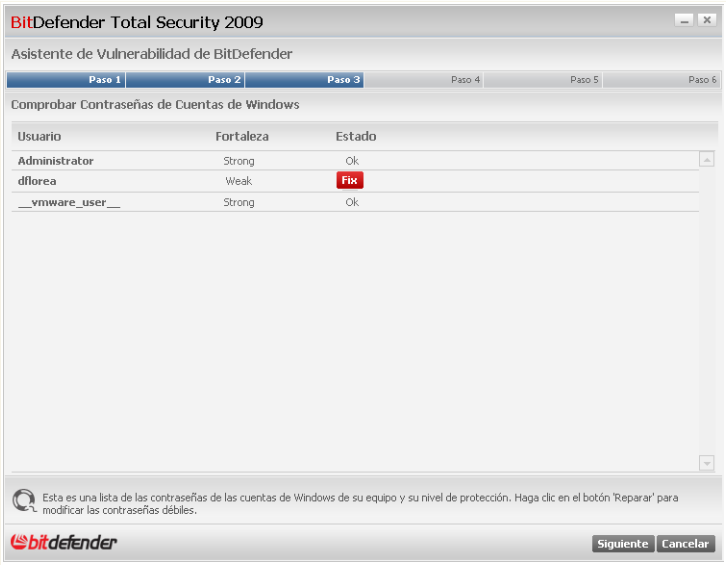
Paso 2/6 - Comprobando Vulnerabilidades



Comprobación de Vulnerabilidades

Espere hasta que BitDefender finalice la comprobación de vulnerabilidades.

Paso 3/6 - Cambie las Contraseñas Inseguras



Contraseñas de los Usuarios

Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo y el nivel de protección de sus contraseñas.

Haga clic en **Reparar** para modificar las contraseñas inseguras. Aparecerá una nueva ventana.

Cambiar Contraseña

Seleccione el método de reparación de esta incidencia:

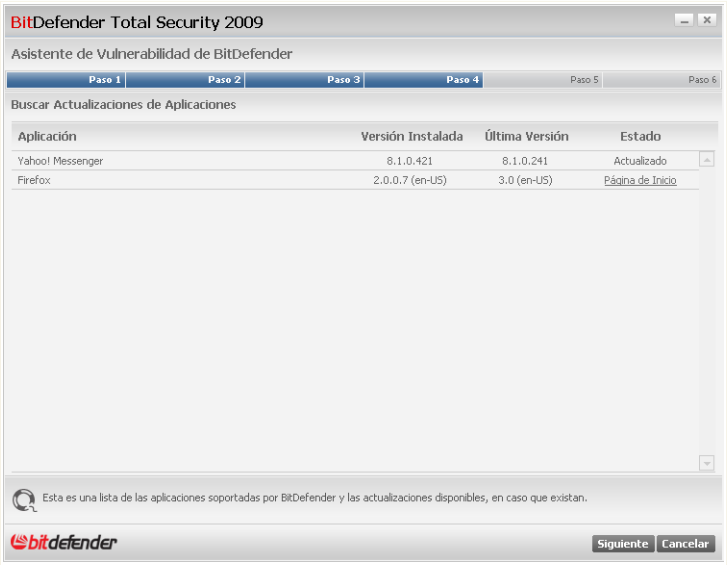
- **Forzar al usuario a cambiar la contraseña la próxima vez que inicie sesión.** BitDefender solicitará al usuario que cambie su contraseña la próxima vez que este usuario inicie sesión en Windows.
- **Cambiar contraseña del usuario.** Debe introducir la nueva contraseña en los campos de texto.

Nota
Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Haga clic en **Aceptar** para cambiar la contraseña.

Haga clic en **Siguiente**.

Paso 4/6 – Actualizar Aplicaciones



Aplicaciones

Puede ver la lista de todas las aplicaciones comprobadas por BitDefender y su estado de actualización. Si una aplicación no está actualizada, haga clic en el enlace indicado para descargar la nueva versión.

Haga clic en **Siguiente**.

Paso 4/6 – Actualizar Windows

Actualizaciones de Windows

Puede ver la lista de las actualizaciones críticas y no-críticas que actualmente no están instaladas en su equipo. Haga clic en **Instalar Todas las Actualizaciones del Sistema** para instalar todas las actualizaciones disponibles.

Haga clic en **Siguiente**.

Paso 6/6 – Ver Resultados

Resultados

Haga clic en **Cerrar**.

7. Parental

BitDefender incluye un módulo Parental que le permite bloquear el acceso a páginas web con contenido no apto o a Internet durante determinados periodos de tiempo, así como filtrar el tráfico de correo, IM y web a partir de determinadas palabras.

Para acceder al módulo Parental, haga clic en la pestaña **Parental**.

Parental

El módulo Parental consta de dos apartados:

- **Componentes Monitorizados** - Le permite ver la lista completa de todos los componentes monitorizados de cada módulo de seguridad. Puede elegir los módulos que desea monitorizar. Recomendamos activar la monitorización de todos los componentes.
- **Tareas** - Aquí encontrará enlaces a las tareas de seguridad más importantes: análisis del sistema, análisis en profundidad y actualización.

7.1. Componentes Monitorizados

El componente monitorizado es el siguiente:

Categoría	Descripción
Control de Contenido	Desde aquí puede comprobar el estado del Control de Contenido, que le permite bloquear el acceso a Internet y a determinadas aplicaciones a sus hijos.

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

7.1.1. Control de Contenido

El Control de Contenido monitoriza el estado de los módulos que le permiten bloquear a sus hijos el acceso a Internet y a determinadas aplicaciones.

Las incidencias relativas al Control de Contenido están descritas a través de frases muy explícitas. En caso que exista algún riesgo que pueda afectar a sus hijos, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Control de Parental no configurado	El módulo Control de Contenido puede bloquear el acceso a las páginas web que considere inapropiadas, bloquear el acceso a Internet en determinados periodos de tiempo, y filtrar el tráfico web, de correo y mensajería instantánea en busca de determinadas palabras.

Cuando los botones de estado están en verde, sus hijos pueden navegar por Internet de forma segura. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

7.2. Tareas

Tareas - Le muestra enlaces a las tareas de seguridad más importantes: análisis del sistema, análisis en profundidad y actualización.

Dispone de los siguientes botones:

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

7.2.1. 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
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
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.
Asistente del Análisis	Use esta tarea para analizar archivos y carpetas concretos.

Nota

A través de las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso requerirá bastante 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 el Analizador de BitDefender.

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

Asistente del Análisis

Al hacer clic en el botón **Asistente del Análisis** y siguiendo los pasos del asistente, podrá crear una tareas de análisis personalizadas y, opcionalmente, guardarlas como tareas rápidas.

Paso 1/4 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

Ventana de Bienvenida

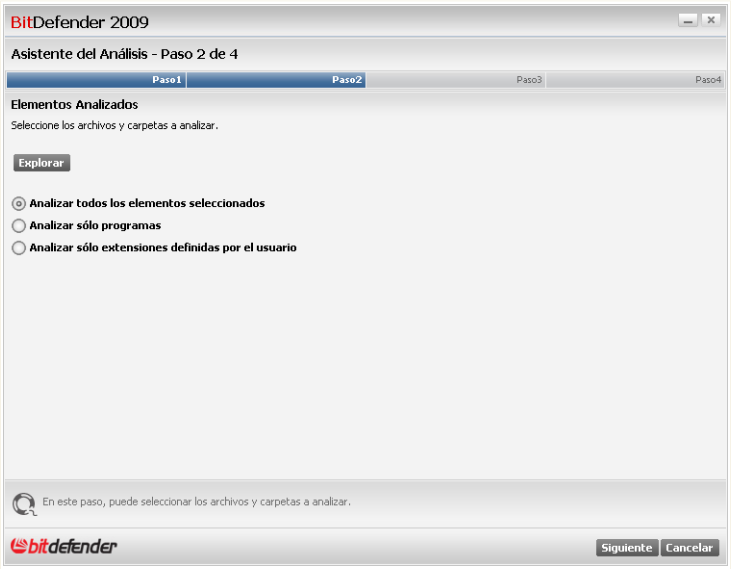
Este asistente le ayudará a analizar su equipo en busca de cualquier amenaza que pueda afectarle. Podrá elegir las carpetas y/o archivos a analizar, así como definir las acciones que se aplicarán a los archivos infectados. También recibirá un informe del análisis que le ayudará a evaluar el nivel de seguridad de su sistema. Por favor, siga todos los pasos del asistente y configure el proceso de análisis acorde con sus necesidades.

Nota
Para omitir este paso en futuros análisis, marque la casilla correspondiente.

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 2/4 - Seleccione los Elementos a Analizar

En este paso, puede elegir los archivos y carpetas que se analizarán.



Selección de los Elementos a Analizar

Haga clic en Explorar para seleccionar determinados archivos y/o carpetas de su equipo.

Dispone de las siguientes opciones:

Opción	Descripción
Analizar todos los elementos seleccionados	Seleccione esta opción para analizar sólo los elementos seleccionados anteriormente.
Analizar sólo programas	Seleccione esta opción para analizar únicamente archivos de programas y aplicaciones.
Analizar sólo extensiones definidas por el usuario	Seleccione esta opción para analizar sólo los archivos con determinadas extensiones. Aparecerá un cuadro de texto en el que podrá indicar estas extensiones. ***Nota*** Debe separar las extensiones con punto y coma ";" (Ej: exe;com;ivd;)

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 3/4 - Seleccione la Acción a Realizar

En este paso, puede elegir las acciones que deben aplicarse a las amenazas encontradas y seleccionar las opciones de análisis usando el control deslizante.

Selección de la Acción a Realizar

Puede seleccionar la acción a realizar en el menú correspondiente:

- **Al encontrar un archivo infectado**
- **Al encontrar un archivo sospechoso**
- **Al encontrar un archivo oculto**

Al mismo tiempo, puede configurar el nivel de protección del análisis. 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 de protección adecuado.

Hay 4 niveles de protección:

Nivel de Protección	*Descripción*
Alto	Ofrece un alto nivel de seguridad. El nivel de consumo de recursos es alto.

Nivel de Protección	Descripción
	■ analiza todos los archivos y comprimidos ■ analiza en busca de virus y spyware ■ analiza en busca de procesos ocultos
Mediana	Ofrece un nivel de seguridad medio. El nivel de consumo de recursos es moderado. ■ analiza todos los archivos ■ analiza en busca de virus y spyware
Bajo	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. ■ analiza sólo archivos de programas ■ analiza en busca de virus
Personalizado	Desde aquí puede seleccionar sus propias opciones de análisis. Haga clic en Personalizar y establezca el nivel de análisis deseado. Seleccione las casillas correspondientes al tipo de malware que desea buscar en su equipo durante el proceso de análisis.

Haga clic en **Siguiente** para continuar o haga clic en **Cancelar** si quiere salir del asistente.

Paso 4/4 - Establezca las Opciones Adicionales

En este paso, puede ajustar algunas opciones adicionales antes de iniciar el proceso de análisis.

Configuración de las Opciones Adicionales

Para guardar la configuración de esta tarea de análisis y poder utilizarla en el futuro, seleccione la casilla correspondiente e introduzca un nombre apropiado en el cuadro de texto.

Nota
Aparecerá un nuevo botón con el nombre introducido anteriormente debajo del menú de tareas.

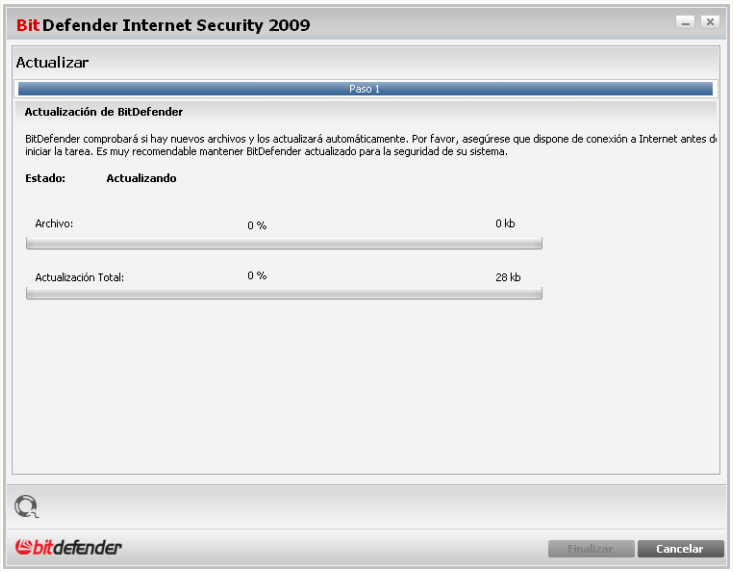
Si desea apagar el equipo una vez finalice el proceso de análisis, seleccione la casilla correspondiente.

Haga clic en **Iniciar Análisis** y siga el asistente guiado de tres pasos para completar el proceso de análisis.

7.2.2. 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 equipo y **cada hora** a partir de ese momento. 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 **Cancelar**. 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.

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.

8. Blindaje de Archivos

BitDefender incluye un módulo de Blindaje de Archivos que no sólo le ayuda a mantener sus datos a salvo, sino también a mantener su confidencialidad. Para conseguirlo, use el blindaje de archivos.

Blindaje de Archivos. Seguramente querrá mantener sus datos críticos lejos de los fisgones. Aquí es donde el Blindaje de Archivos del Administrador de Archivos puede resultarle muy útil.

- El Blindaje de Archivos es un área de almacenamiento protegida, situada dentro de su equipo, en la que puede guardar información personal o archivos confidenciales.
- El Blindaje de Archivos se basa en un archivo cifrado en su equipo, cuya extensión es `bvd`.
- Al estar cifrado, los datos que contiene este archivo no son vulnerables a robos o agujeros de seguridad.
- Cuando monte este archivo `bvd`, aparecerá una nueva partición lógica (una unidad nueva). Puede entender fácilmente este proceso si imagina que funciona de forma similar al montaje de una imagen ISO en una unidad de CD virtual.

Abra Mi PC y verá una nueva unidad basada en el archivo de blindaje, desde la que podrá realizar operaciones con los archivos (copiar, eliminar, modificar, etc.). Los archivos estarán protegidos mientras residan en esta unidad (ya que para la operación de montaje es necesario introducir una contraseña). Al finalizar, bloquee (desmonte) su blindaje para empezar a proteger su contenido.

Para acceder al módulo Administrador de Archivos, haga clic en la pestaña **Blindaje**.

Blindaje de Archivos

- **Componentes Monitorizados** - Le permite ver la lista completa de todos los componentes monitorizados por cada módulo de seguridad. Puede elegir los módulos que desea monitorizar. Recomendamos activar la monitorización de todos los componentes.

8.1. Componentes Monitorizados

El componente monitorizado es el siguiente:

Categoría	Descripción
Blindaje de archivos	Es un área de almacenamiento protegida, situada dentro de su equipo, en la que puede guardar información personal o archivos confidenciales. Al estar cifrada, los documentos que contenga no serán vulnerables a tentativas de robo o agujeros de seguridad.

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

8.1.1. Blindaje de archivos

Las incidencias relativas al blindaje de archivos están descritas a través de frases muy explícitas. En caso que exista algún riesgo para la privacidad de sus datos, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	*Descripción*
Blindaje de Archivos activado	El Blindaje de Archivos cifra sus documentos confidenciales en unidades blindadas especiales.

Cuando los botones de estado son verdes, los riesgos de seguridad de sus datos son mínimos. Para que los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

8.2. Tareas

Dispone de los siguientes botones:

- **Blindar Archivo** - inicia un asistente que le permite almacenar sus archivos / documentos de forma privada cifrándolos en unidades especiales blindadas.
- **Desblindar Archivos** - inicia un asistente que le permite eliminar sus datos del blindaje.
- **Ver Blindaje** - inicia un asistente que le permite ver el contenido de sus blindajes.
- **Bloquear Blindaje** - inicia un asistente que le permite bloquear su blindaje y proteger su contenido.

8.2.1. Añadiendo Archivos al Blindaje

El Blindaje de Archivos es un área especial que puede usar para almacenar sus archivos y documentos más importantes de forma segura. Los datos incluidos en un blindaje están cifrados.

Al hacer clic en **Blindar Archivos**, se iniciará un asistente que le guiará a través del proceso de creación del blindaje y le permitirá añadir documentos en el mismo.

Paso 1/6 - Seleccione el Objetivo

Aquí puede especificar los archivos y carpetas que se añadirán al blindaje.

Objetivo

Haga clic en **Ruta**, seleccione el archivo o carpeta que desea añadir y haga clic en **Aceptar**. La rutas de los elementos seleccionados aparecerá en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento.

Nota
Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiente**.

Paso 2/6 - Seleccione el Blindaje

Desde aquí puede crear un nuevo blindaje o seleccionar un blindaje existente.

Selección del Blindaje

Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 5 si el blindaje seleccionado está abierto (montado) o al paso 4 si el blindaje está bloqueado (desmontado).

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 5 si el blindaje seleccionado está abierto (montado) o al paso 4 si el blindaje está bloqueado (desmontado).

Seleccione **Crear Nuevo Blindaje de Archivos** si ninguno de los blindajes existentes se ajusta a sus necesidades. Se le dirigirá al paso 3.

Haga clic en **Siguiente**.

Paso 3/6 – Crear un Blindaje

Aquí puede especificar la información del nuevo Blindaje.

Creación del Blindaje

Para completar la información relacionada con el blindaje, siga estos pasos:

1. Haga clic en **Explorar** e indique la ubicación del archivo `bvd`.

   Nota
   Recuerde que el archivo de blindaje es un archivo cifrado ubicado en si equipo con extensión `bvd`.

2. Seleccione la letra de la unidad del nuevo blindaje en el correspondiente menú desplegable.

   Nota
   Recuerde que cuando monta un archivo `bvd`, aparecerá una nueva partición lógica (una nueva unidad).

3. Introduzca una contraseña para el blindaje en el campo correspondiente.

Nota
La contraseña debe contener 8 caracteres como mínimo.

4. Vuelva a introducir la contraseña.
5. Defina el tamaño del blindaje (en MB) introduciendo un número en el campo correspondiente.

Nota
El tamaño sólo debe contener dígitos.

Haga clic en **Siguiente**.

Se le dirigirá al paso 5.

Paso 4/6 - Contraseña

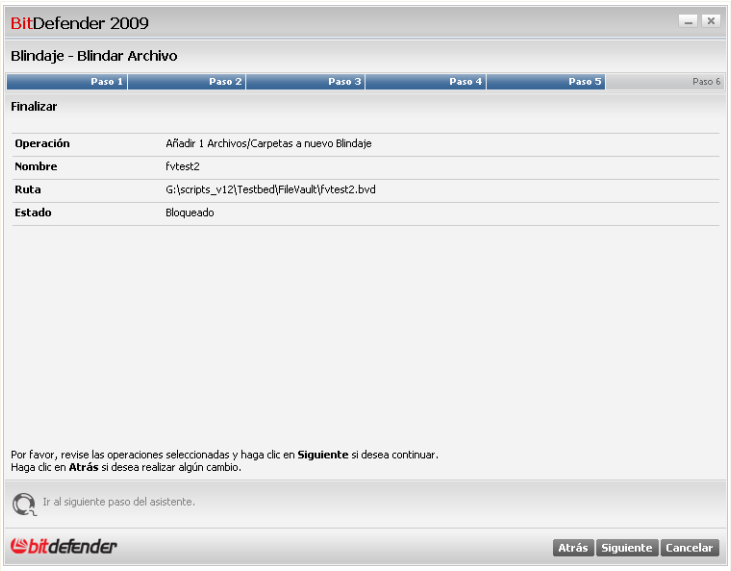
Aquí es donde debe introducir la contraseña del blindaje seleccionado.

Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 5/6 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.



Resumen

Haga clic en **Siguiente**.

Paso 6/6 – Resultados

Aquí puede ver el contenido del blindaje.

Resultados

Haga clic en **Finalizar**.

8.2.2. Eliminando Archivos del Blindaje

Al hacer clic en **Desblindar Archivos** se iniciará un asistente que le guiará a través de los pasos necesarios para eliminar archivos de un blindaje determinado.

Paso 1/5 - Seleccione un Blindaje

Aquí puede indicar el blindaje del que desea quitar los archivos.

Selección del Blindaje

Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Haga clic en **Siguiente**.

Paso 2/5 - Contraseña

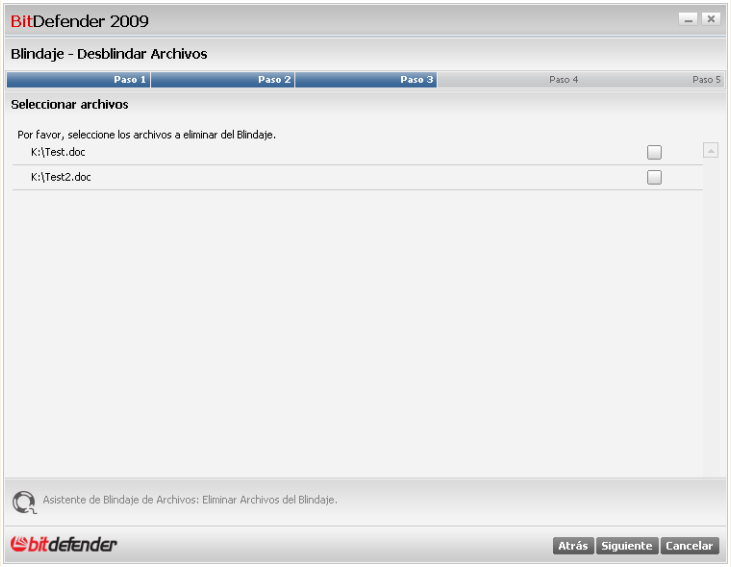
Aquí es donde debe introducir la contraseña del blindaje seleccionado.

Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 3/5 – Seleccione los Archivos

Aquí puede ver la lista de archivos que contiene el blindaje previamente seleccionado.



Selección de los archivos

Seleccione los archivos a eliminar y haga clic en **Siguiente**.

Paso 4/5 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.

Resumen

Haga clic en **Siguiente**.

Paso 5/5 – Resultados

Aquí puede ver los resultados de la operación.

Resultados

Haga clic en **Finalizar**.

8.2.3. Visualizando los Archivos del Blindaje

Al hacer clic en **Ver Blindaje**, se iniciará un asistente que le permitirá ver el contenido de un blindaje determinado.

Paso 1/4 - Seleccione el Blindaje

Aquí puede especificar el blindaje cuyo contenido desea visualizar.

Selección del Blindaje

Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Haga clic en **Siguiente**.

Paso 2/4 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.

Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 3/4 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.

Resumen

Haga clic en **Siguiente**.

Paso 4/4 – Resultados

Desde aquí puede ver los archivos que contiene el blindaje.

Resultados

Haga clic en **Finalizar**.

8.2.4. Bloqueando un Blindaje

El blindaje de archivos se basa en un archivo (archivo de blindaje) almacenado en su equipo con extensión `bvd`. Este archivo puede abrirse (montar unidad) o bloquearse (desmontar unidad).

Para comprender este proceso, imagine que se trata de la caja fuerte de un banco, cuya puerta puede estar abierta o bloqueada. El contenido de la caja fuerte sólo está protegido cuando la puerta está bloqueada, del mismo modo que sólo puede acceder a su contenido cuando la puerta está abierta.

Al hacer clic en **Bloquear Blindaje** se iniciará un asistente que le guiará a través del proceso de bloqueo (desmontaje) de un blindaje determinado.

Paso 1/3 - Seleccione el Blindaje

Aquí puede indicar el blindaje que desea bloquear.

Selección del Blindaje

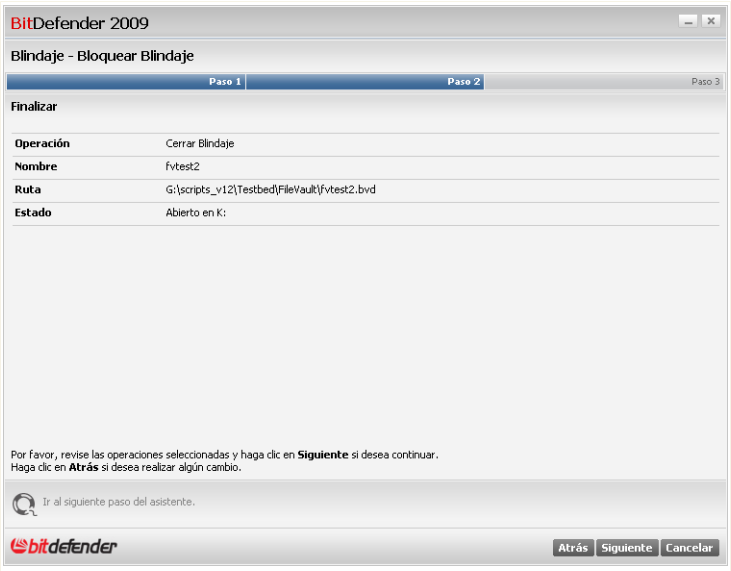
Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje.

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista.

Haga clic en **Siguiente**.

Paso 2/3 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.

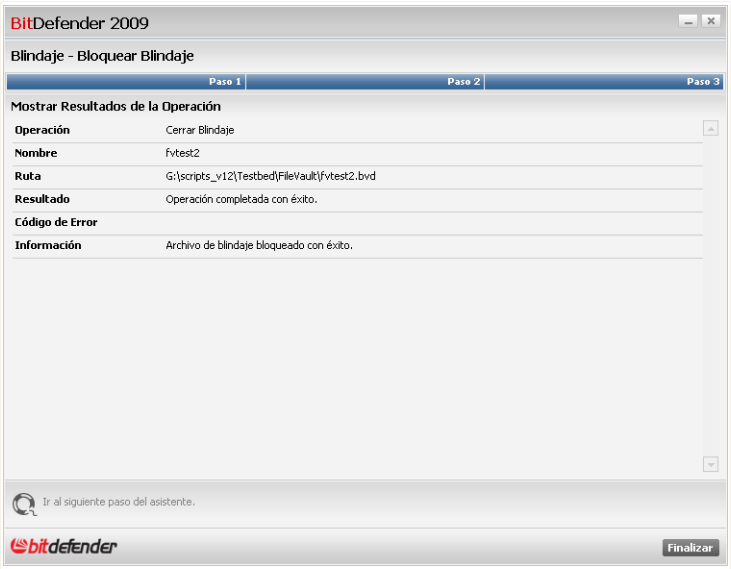


Resumen

Haga clic en **Siguiente**.

Paso 3/3 – Resultados

Aquí puede ver los resultados de la operación.



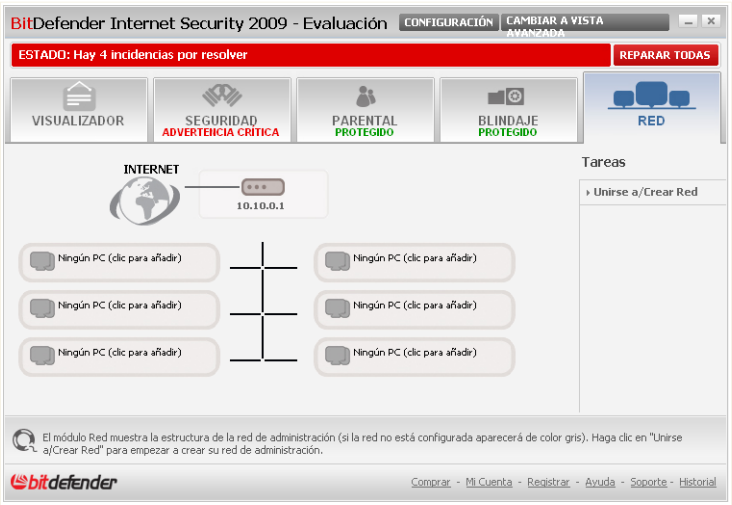
Resultados

Haga clic en **Finalizar**.

9. Red

El módulo Red le permite administrar los productos BitDefender instalados en los equipos de una pequeña red desde un único equipo.

Para acceder al módulo Red, haga clic en la pestaña **Red**.



Red

Para poder administrar los productos BitDefender de los otros equipos de la pequeña red, debe seguir estos pasos:

1. Únase a la red de administración de BitDefender desde su equipo. Unirse a una red consiste en establecer una contraseña de administración para gestionar la red de administración.
2. Diríjase a cada unos de los equipos que desee administrar remotamente y únalos a la red (defina una contraseña).
3. Vuelva a su equipo y añada los equipos que desee administrar.

9.1. Tareas

Inicialmente, sólo habrá un botón disponible.

- **Unirse a/Crear Red** - le permite definir la contraseña de la red, así como acceder a la red.

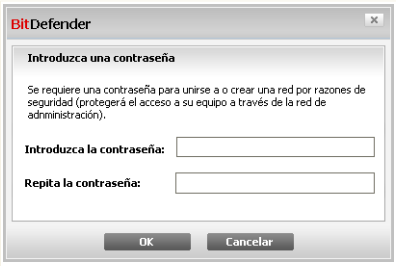
Una vez se haya unido a la red, aparecerán varios botones.

- **Abandonar Red** - le permite salir de la red.
- **Administración de Red** - le permite añadir un equipo a su red.
- **Analizar Todos** - le permite analizar todos los equipos administrados a la vez.
- **Actualizar Todos** - le permite actualizar todos los equipos administrados a la vez.
- **Registrar Todos** - le permite registrar todos los equipos administrados a la vez.

9.1.1. Unirse a la Red de BitDefender

Para unirse a la red de administración de BitDefender, siga estos pasos:

1. Haga clic en **Unirse a/Crear Red**. Se le solicitará configurar la contraseña de administración de red.



Configurar Contraseña

2. Introduzca la misma contraseña en cada uno de los campos de texto.
3. Haga clic en **Aceptar**.

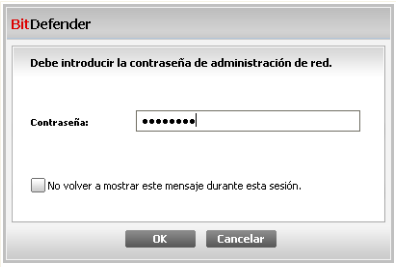
Podrá ver como el nombre del equipo aparece en el mapa de la red.

9.1.2. Añadiendo Equipos a la Red de BitDefender

Antes de añadir un equipo a la red de administración de BitDefender, debe configurar la contraseña de administración de red en el equipo correspondiente.

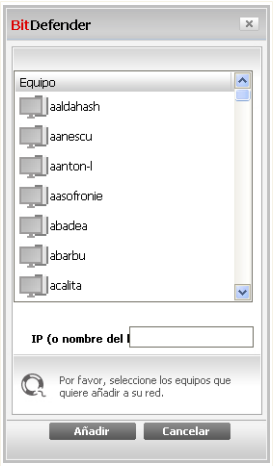
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

1. Haga clic en **Administración de Red**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**. Aparecerá una nueva ventana.

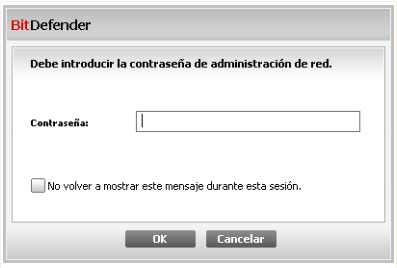


Añadir Equipo

Podrá ver la lista de los equipos de la red. A continuación se explica el significado de los iconos:

- Indica un equipo conectado con ningún producto BitDefender instalado.
- Indica un equipo conectado con BitDefender instalado.
- Indica un equipo desconectado con BitDefender instalado.

3. Realice una de estas acciones:
   - Seleccione un equipo de la lista para añadirlo.
   - Introduzca la dirección IP o el nombre del equipo a añadir en el campo editable correspondiente.
4. Haga clic en **Añadir**. Se le solicitará la contraseña de administración de red del equipo correspondiente.



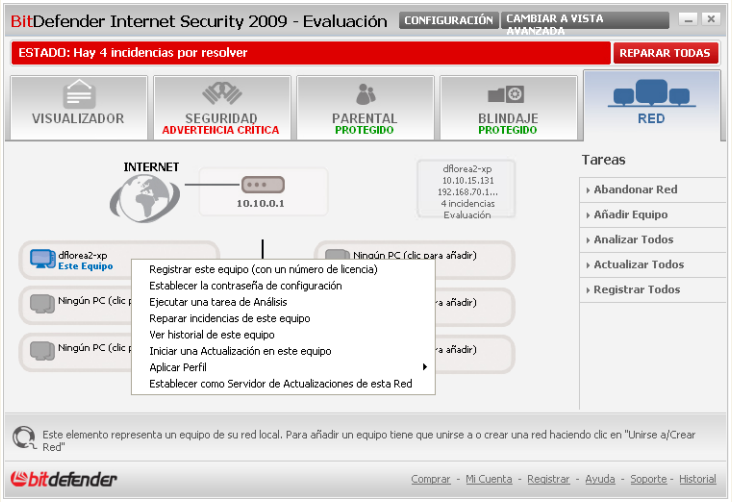
Autentificar

5. Introduzca la contraseña de administración de red configurada en el equipo correspondiente.
6. Haga clic en **Aceptar**. Si ha introducido la contraseña correcta, el nombre del equipo seleccionado aparecerá en el mapa de la red.

Nota
Puede añadir hasta cinco equipos en el mapa de la red.

9.1.3. Administrando la Red de BitDefender

Una vez haya creado con éxito una red de administración de BitDefender, podrá gestionar todos los productos BitDefender desde un único equipo.



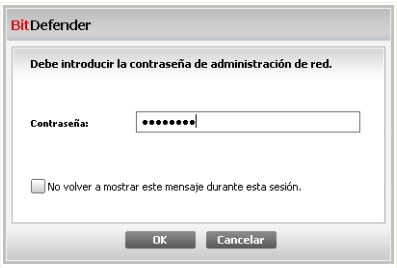
Mapa de la Red

Si sitúa el cursor del ratón encima de un equipo del mapa de la red, podrá ver información sobre el equipo (nombre, dirección IP, número de incidencias que afectan a la seguridad del sistema y estado de registro de BitDefender).

Si hace clic derecho en el nombre de un equipo del mapa de la red, podrá ver todas las tareas de administración que puede ejecutar remotamente.

- **Registrar este equipo**
- **Establecer contraseña de configuración**
- **Ejecutar una tarea de Análisis**
- **Reparar incidencias de este equipo**
- **Ver historial de este equipo**
- **Iniciar una Actualización en este equipo**
- **Aplicar Perfil**
- **Iniciar una tarea de Optimizador en este equipo**
- **Establecer como Servidor de Actualizaciones de esta Red**

Antes de ejecutar una tarea en un equipo determinado, se le solicitará la contraseña de administración de red local.



Introducir Contraseña

Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**.

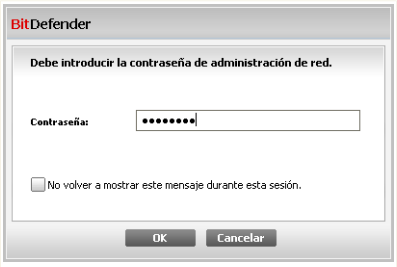
Nota

Si tiene previsto ejecutar varias tareas, puede interesarle la opción **No volver a mostrar este mensaje durante esta sesión**. Al seleccionar esta opción, no se le volverá a solicitar esta contraseña durante la actual sesión.

9.1.4. Analizando Todos los Equipos

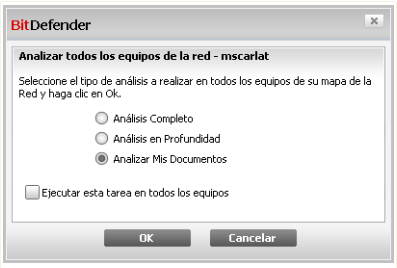
Para analizar todos los equipos administrados, siga estos pasos:

1. Haga clic en **Analizar Todos**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Seleccione un tipo de análisis.
   - **Análisis Completo** - inicia un análisis completo de su equipo (archivos comprimidos excluidos).
   - **Análisis en Profundidad** - inicia un análisis completo de su equipo (archivos comprimidos incluidos).
   - **Analizar Mis Documentos** - inicia un análisis rápido de sus documentos.



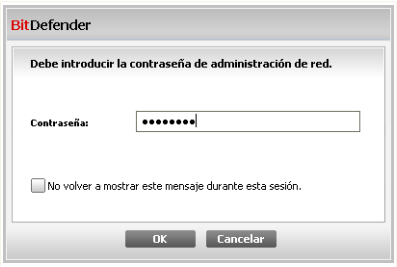
Selección del Tipo de Análisis

3. Haga clic en **Aceptar**.

9.1.5. Actualizando Todos los Equipos

Para actualizar todos los equipos administrados, siga estos pasos:

1. Haga clic en **Actualizar Todos**. Se le solicitará introducir la contraseña de administración de red local.



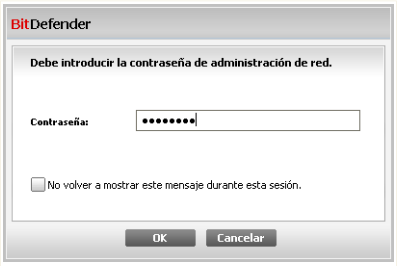
Introducir Contraseña

2. Haga clic en **Aceptar**.

9.1.6. Registrando Todos los Equipos

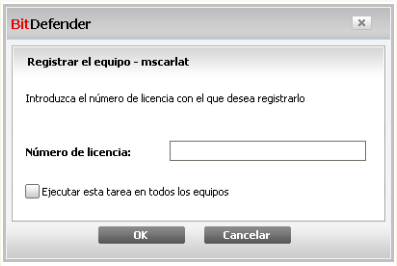
Para registrar todos los equipos administrados, siga estos pasos:

1. Haga clic en **Registrar Todos**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Introduzca el número de licencia con el que quiere registrar los equipos.



Registrar Todos

3. Haga clic en **Aceptar**.

10. Configuración Básica

En el módulo Configuración Básica podrá activar o desactivar fácilmente los módulos de seguridad más importantes.

Para acceder al módulo Configuración Básica, haga clic en la pestaña **Configuración Básica** situado en la parte superior de la Vista Básica.

Configuración Básica

Los módulos de seguridad disponibles están agrupados en varias categorías.

Categoría	*Descripción*
Seguridad Local	Desde aquí puede activar / desactivar la protección de archivos en tiempo real o la actualización automática.
Seguridad Online	Desde aquí puede activar / desactivar la protección en tiempo real del correo y web.
Configuración del Control de Contenido	Desde aquí puede activar / desactivar el Control de Contenido.
Seguridad de la red	Desde aquí puede activar / desactivar el Cortafuego.

Categoría	Descripción
Configuración General	Desde aquí puede activar / desactivar el Modo Trabajo, portátil, contraseñas, barra de actividad del análisis y otras opciones.

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

10.1. Seguridad local

Puede activar / desactivar los módulos de seguridad con un simple clic.

Módulo de seguridad	Descripción
Protección Antivirus y Antispyware de Archivos en Tiempo Real	La protección de archivos en tiempo real le asegura el análisis de los archivos a los que accede y los que usan las aplicaciones que se ejecutan en este sistema.
Actualización Automática	La Actualización Automática asegura que los archivos y firmas de virus más recientes de BitDefender se descarguen e instalen automáticamente de forma regular.
Comprobación Automática de Vulnerabilidades	La Comprobación Automática de Vulnerabilidades comprueba si el software crucial de su PC está actualizado.

10.2. Seguridad online

Puede activar / desactivar los módulos de seguridad con un simple clic.

Módulo de seguridad	Descripción
Protección Antivirus, Antispam y Antiphishing del	La protección en tiempo real del correo se encarga de filtrar su correo electrónico en busca de spam y tentativas de phishing.

Módulo de seguridad	Descripción
Correo en Tiempo Real	
Protección Antivirus y Antispyware Web en Tiempo Real	La protección web en tiempo real analiza todos los archivos descargados vía HTTP en busca de virus y spyware.
Protección Antiphishing Web en Tiempo Real	La Protección Antiphishing Web en Tiempo Real analiza todos los archivos descargados vía HTTP en busca de tentativas de phishing.
Control de Identidad	El Control de Identidad le ayuda a mantener a salvo su información confidencial, al analizar todo el tráfico web y el correo en busca de determinadas cadenas de texto.
Cifrado de IM	Si sus contactos de Mensajería Instantánea (IM) tienen BitDefender 2009 instalado, se cifrarán todas sus conversaciones a través de Yahoo! Messenger y Windows Live Messenger.

10.3. Configuración del Control de Contenido

Puede activar / desactivar el módulo Control de Contenido con un sólo clic.

El Control de Contenido puede bloquear el acceso a las páginas web que considere inapropiadas, bloquear el acceso a Internet durante determinados periodos de tiempo, y filtrar el tráfico web, de correo y mensajería instantánea en busca de determinadas palabras.

10.4. Configuración de la Red

Puede activar / desactivar el módulo Cortafuego con un sólo clic.

El Cortafuego protege su equipo frente a hackers y ataques externos.

10.5. Configuración del Blindaje de Archivos

Puede activar / desactivar el módulo Blindaje de Archivos con un sólo clic.

El Blindaje de Archivos cifra sus documentos confidenciales en unidades blindadas especiales.

10.6. Configuración General

Puede activar / desactivar elementos relacionados con la seguridad con un simple clic.

Elemento	Descripción
Modo Trabajo	El Modo Trabajo modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
Modo Portátil	El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.
Contraseña de la Configuración	Al activar esta opción, protegerá la configuración de BitDefender de modo que sólo pueda modificarla la persona que conozca la contraseña.
Contraseña del Control de Contenido	Al activar esta opción, puede restringir la configuración del Control de Contenido, de modo que sólo pueda cambiar la configuración la persona que conozca la contraseña.
BitDefender News	Active esta opción si desea recibir noticias importantes sobre BitDefender, las actualizaciones del producto y las nuevas amenazas de seguridad.
Alertas de Notificación del Producto	Al activar esta opción, recibirá alertas de información sobre la actividad del producto.
Barra de Actividad del Análisis	La Barra de Actividad del Análisis le muestra el progreso de la actividad del análisis de BitDefender. La barra gris representa la actividad de análisis de su equipo, la barra naranja representa la actividad de su equipo en Internet.
Cargar BitDefender al iniciar Windows	Al activar esta opción, la interfaz de BitDefender se cargará al iniciar el sistema. Esta opción no afecta al nivel de protección.
Enviar Informes de Virus	Al activar esta opción, enviará informes de análisis virus a los Laboratorios BitDefender para su análisis. Los informes no

Elemento	Descripción
	contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.
Detección de Epidemias	Al activar esta opción, enviará informes sobre amenazas potenciales a los Laboratorios BitDefender para su análisis. Los informes no contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.

11. Barra de Estado

Como observará, en la parte superior de la ventana de BitDefender Internet Security 2009 hay una barra de estado que muestra el número de incidencias por resolver. Haga clic en el botón **Reparar Todas** para eliminar cualquier amenaza para la seguridad de su equipo. Aparecerá una ventana de estado de seguridad.

El estado de seguridad muestra una lista organizada sistemáticamente y muy manejable sobre las vulnerabilidades de seguridad detectadas en su ordenador. BitDefender Internet Security 2009 le avisará siempre que detecte un problema que pueda afectar a la seguridad de su equipo.

Barra de Estado

11.1. Seguridad local

Sabemos que es importante estar informado cuando se produce algún problema que afecte a la seguridad de su equipo. Al monitorizar los módulos de seguridad, BitDefender Internet Security 2009 le hará saber si la configuración aplicada puede afectar a la seguridad del equipo, o le avisará cuando olvide realizar alguna tarea de seguridad importante.

Las incidencias relativas a la seguridad local están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	*Descripción*
Protección de archivos en tiempo real activada	Asegura el análisis de todos los archivos a los que accede o bien utilizan las aplicaciones que se ejecutan en el sistema.
Nunca ha analizado su equipo en busca de malware	Recomendamos encarecidamente iniciar una tarea de análisis bajo demanda cuanto antes, para asegurarse que los archivos almacenados en su equipo están libres de malware.
Actualización automática activada	Mantenga activada la actualización automática para asegurarse que las firmas de malware de su producto BitDefender se actualizan regularmente.
Actualizando	Se está realizando una actualización del producto y firmas de malware.
Cortafuego activado	Protege su equipo frente a hackers y ataques externos.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

11.2. Seguridad online

Las incidencias relativas a la seguridad online están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Antispam activado	Le asegura que sus e-mails son analizados en busca de malware y filtrados en busca de spam.
Control de Identidad activado	Le ayuda a mantener a salvo su información confidencial, al analizar todo el tráfico web y el correo en busca de determinadas cadenas de texto. Recomendamos activar el Control de Identidad para mantener a salvo sus datos confidenciales (dirección de correo, IDs de usuario, contraseñas, números de tarjetas de crédito, etc) y impedir su robo.
Antiphishing activado para Mozilla Firefox	BitDefender le protege contra los intentos de phishing mientras navega por Internet.
Antiphishing activado para Internet Explorer	BitDefender le protege contra los intentos de phishing mientras navega por Internet.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

11.3. Blindaje de archivos

Las incidencias relativas al blindaje de archivos están descritas a través de frases muy explícitas. En caso que exista algún riesgo para la privacidad de sus datos, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Blindaje de Archivos activado	El Blindaje de Archivos cifra sus documentos confidenciales en unidades blindadas especiales.

Cuando los botones de estado son verdes, los riesgos de seguridad de sus datos son mínimos. Para que los botones se vuelvan verdes, siga estos pasos:

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

11.4. Análisis de Vulnerabilidad

Las incidencias relativas a las vulnerabilidades están descritas a través de frases muy explícitas. En caso que exista algún riesgo de seguridad, encontrará un botón de estado rojo llamado **Reparar** junto a cada frase. En caso contrario, aparecerá un botón de estado verde llamado **Correcto**.

Incidencia	Descripción
Comprobación de Vulnerabilidades activada	Monitoriza las Actualizaciones de Microsoft Windows y Microsoft Office, así como las contraseñas de las cuentas de Windows, para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.
Actualizaciones Críticas de Microsoft	Instala las actualizaciones críticas de Microsoft disponibles.
Otras actualizaciones de Microsoft	Instala las actualizaciones no-críticas de Microsoft disponibles.
Actualizaciones Automáticas de Windows activadas	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.

Incidencia	Descripción
Admin (Contraseña Segura)	Indica la fortaleza de la contraseña de determinados usuarios.

Cuando los botones de estado son verdes, los riesgos de seguridad de su sistema son mínimos. Para que todos los botones se vuelvan verdes, siga estos pasos:

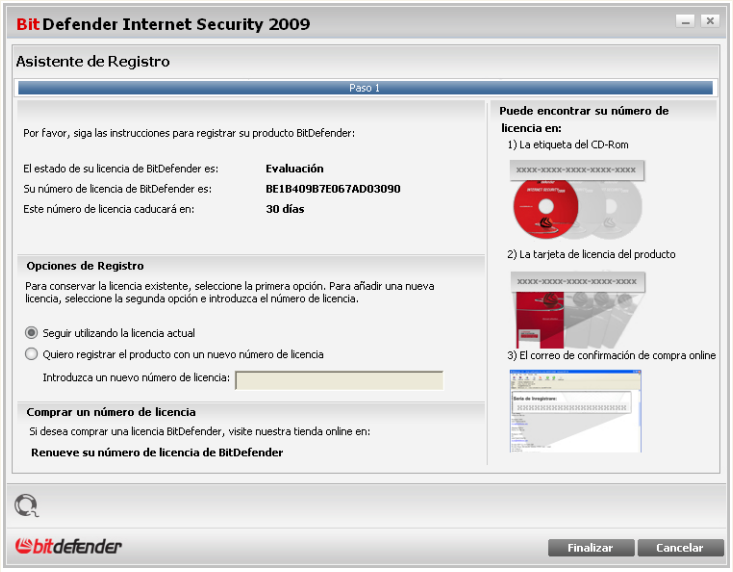
1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.
2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

Si desea excluir la monitorización de una incidencia, desmarque la casilla **monitorizar este componente**.

12. Registro

BitDefender Internet Security 2009 incluye un periodo de evaluación de 30 días. Si desea registrar BitDefender Internet Security 2009, cambiar el número de licencia o crear una cuenta de BitDefender, haga clic en enlace **Registrar**, ubicado en la parte inferior de la ventana de BitDefender. Aparecerá el Asistente de Registro.

12.1. Paso 1/1 - Registrar BitDefender Internet Security 2009



Registro

Puede ver el estado del registro de BitDefender, el número de licencia actual y los días restantes hasta la fecha de caducidad de la licencia.

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

Para registrar BitDefender Internet Security 2009:

1. Seleccione la opción **Quiero registrar el producto con un nuevo número de licencia**.
2. Introduzca el número de licencia en el campo editable.

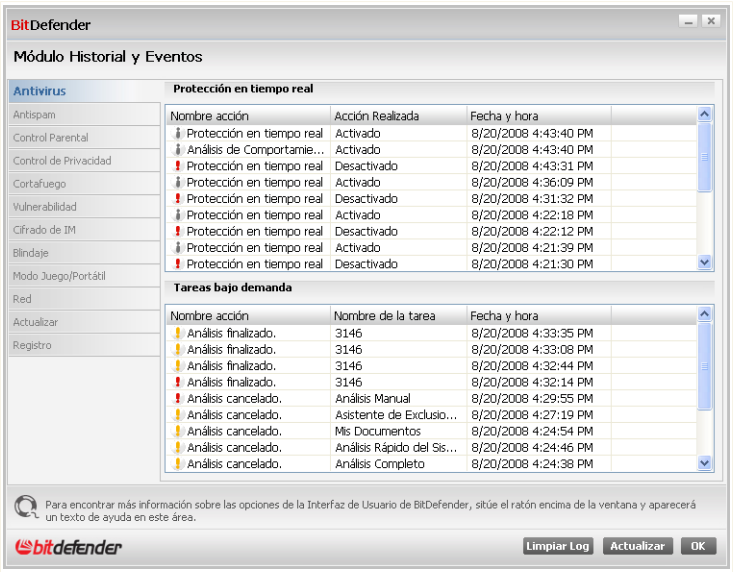
Nota
Puede encontrar su número de licencia en:
- la etiqueta del CD.
- la tarjeta de licencia del producto.
- el mensaje de confirmación de compra online.

Si no dispone de ningún número de licencia de BitDefender, haga clic en el enlace indicado para dirigirse a la tienda online de BitDefender y adquirir una.

Haga clic en **Finalizar**.

13. Historial

El enlace del **Historial** situado en la parte inferior de la interfaz 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, etc.



Eventos

Para ayudarle a filtrar el historial y eventos de BitDefender, se muestran las siguientes categorías en la parte izquierda:

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

- **Red**
- **Blindaje de Archivos**

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 Log** si desea eliminar los registros antiguos, o en **Actualizar** para asegurarse que se visualizan los últimos registros.

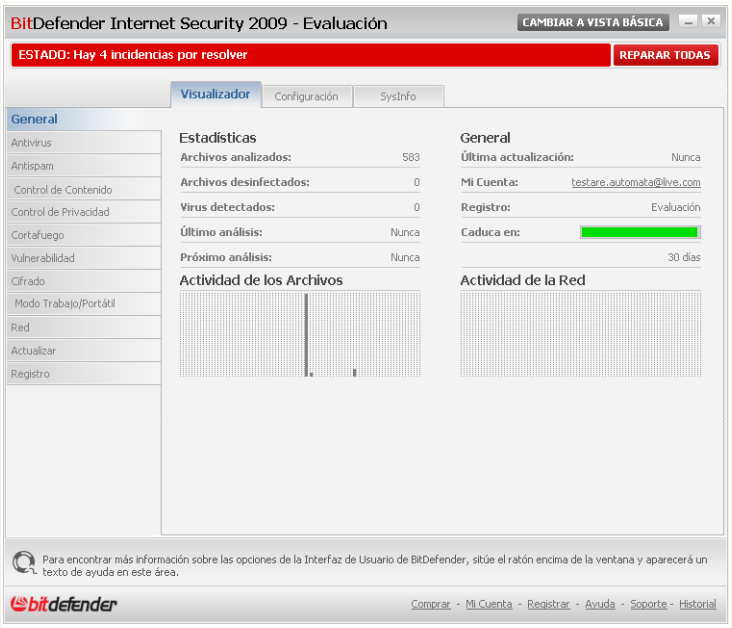
Administración Avanzada

14. General

El módulo General le ofrece información sobre la actividad de BitDefender y su sistema. Desde aquí también puede cambiar algunos aspectos del comportamiento general de BitDefender.

14.1. Visualizador

Para ver estadísticas sobre la actividad del producto y su estado de registro, diríjase al apartado **General > Visualizador** en la Vista Avanzada



Visualizador

El Visualizador consta de varios apartados:

- **Estadísticas** - Muestra información importante sobre la actividad de BitDefender.

- **General** - Muestra el estado de la actualización, el estado de su cuenta, registro e información de la licencia.
- **Archivos** - Indica la evolución del número de objetos analizados por BitDefender Antimalware durante el último periodo. La altura de la barra indica la intensidad del tráfico durante ese intervalo de tiempo.
- **Internet** - Indica la evolución del tráfico de la red filtrado por el Cortafuego de BitDefender durante el último periodo. La altura de la barra indica la intensidad del tráfico durante ese intervalo de tiempo.

14.1.1. Estadísticas

Si desea controlar la actividad de BitDefender, puede empezar por el apartado Estadísticas. Puede ver los siguientes elementos:

Elemento	Descripción
Archivos analizados	Indica el número de archivos que han sido analizados en busca de malware durante el último análisis.
Archivos desinfectados	Indica el número de archivos han sido desinfectados por BitDefender durante el último análisis.
Virus detectados	Indica el número de virus detectados en su sistema durante el último análisis.
Análisis de puertos bloqueados	Indica el número de análisis de puertos bloqueados por el Cortafuego de BitDefender. Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers que buscan puertos abiertos en su equipo para intentar aprovecharse de ellos. Mantenga activados el Cortafuego y el Modo Oculto en todo momento para estar protegido frente a los análisis de puertos.

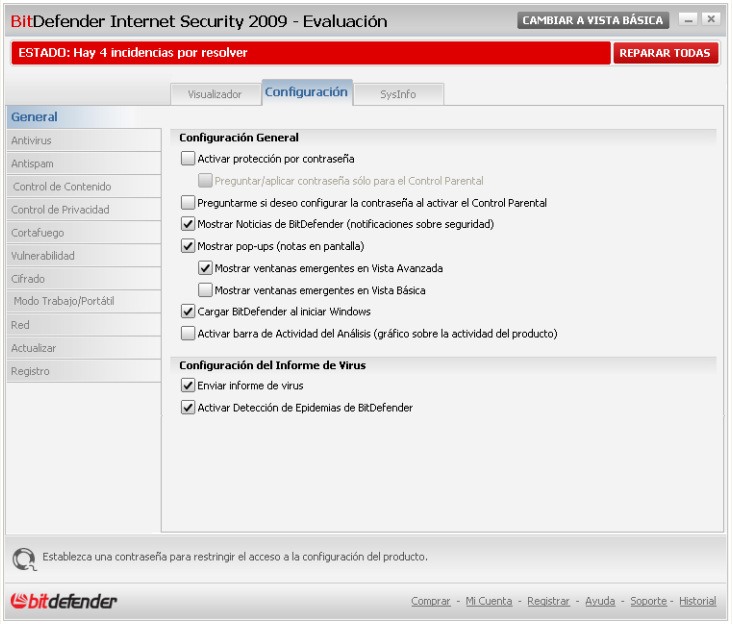
14.1.2. General

Aquí puede ver un resumen de las estadísticas relacionadas con el estado de la actualización, el estado de su cuenta e información sobre el registro y la licencia.

Elemento	Descripción
Última actualización	Indica la fecha en la que el producto BitDefender se actualizó por última vez. Por favor, realice actualizaciones regularmente para estar completamente protegido.
Mi Cuenta	Indica la dirección de correo que puede utilizar para acceder a su cuenta de copia online, para recuperar su licencia o para beneficiarse del soporte de BitDefender u otros servicios.
Registro	Le indica el tipo de licencia utilizada y su estado. Para mantener su equipo protegido, debería renovar o actualizar su licencia de BitDefender una vez haya caducado.
Caduca en	Indica el número de días restantes hasta que caduque la licencia.

14.2. Configuración

Para configurar las opciones generales de BitDefender, diríjase al apartado **General > Configuración** en la Vista Avanzada.



Configuración General

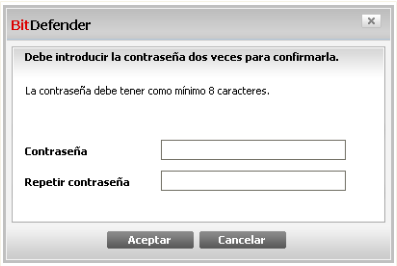
En este apartado puede configurar el comportamiento general de BitDefender. Por defecto, BitDefender se carga al inicio de Windows y sigue funcionando minimizado en la barra del sistema.

14.2.1. 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 cambie la configuración del Control de Contenido, marque la opción **Preguntar/aplicar contraseña sólo para el 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.

- **Preguntarme si deseo configurar la contraseña al activar el Control de Contenido** - se le pedirá que configure una contraseña cuando active el Control de Contenido y no haya ninguna contraseña definida. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control de Contenido que ha configurado exclusivamente para un usuario.
- **Mostrar Noticias de BitDefender (noticias relacionadas con la seguridad)** - ocasionalmente muestra 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.

14.2.2. 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.

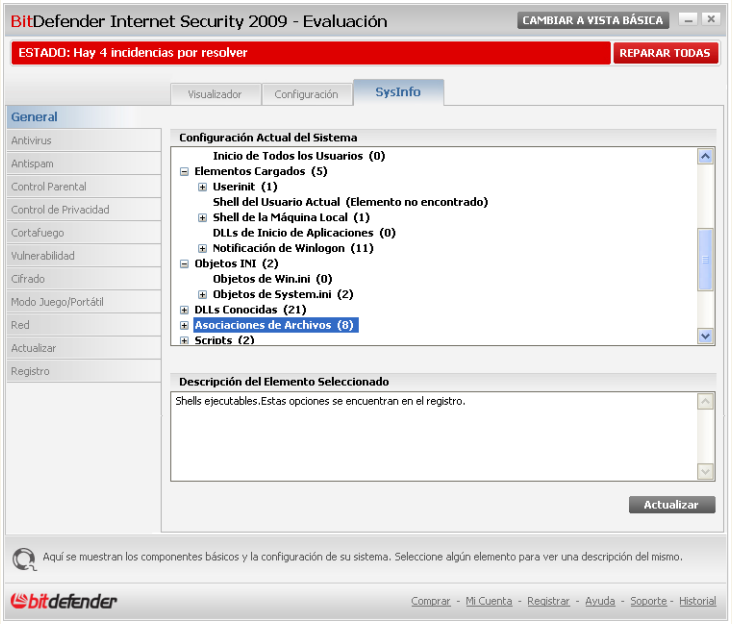
- **Activar la Detección de Epidemias** - envía informes acerca de las posibles epidemias de virus a los Laboratorios de BitDefender.

  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.

14.3. 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, diríjase al apartado **General > Sistema** en la Vista Avanzada.



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:

- **Restaurar** - restaura la asociación actual del archivo a la asociación predeterminada. ¡Sólo disponible en la opción **Asociaciones de Archivos**!
- **Ir a** - abre una ventana para mostrar la ubicación del objeto seleccionado (el **Registro** por ejemplo).

> ***Nota***
> En función del elemento seleccionado, puede que el botón **Ir a** no aparezca.

- **Actualizar** - actualiza el contenido del apartado **Sistema**.

15. Antivirus

BitDefender protege a su equipo frente a todo tipo de malware (virus, troyanos, spyware, rootkits y otros). La protección que ofrece BitDefender está dividida en dos apartados:

- Protección en tiempo real - impide que las nuevas amenazas de malware entren en su sistema. Por ejemplo, BitDefender analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.

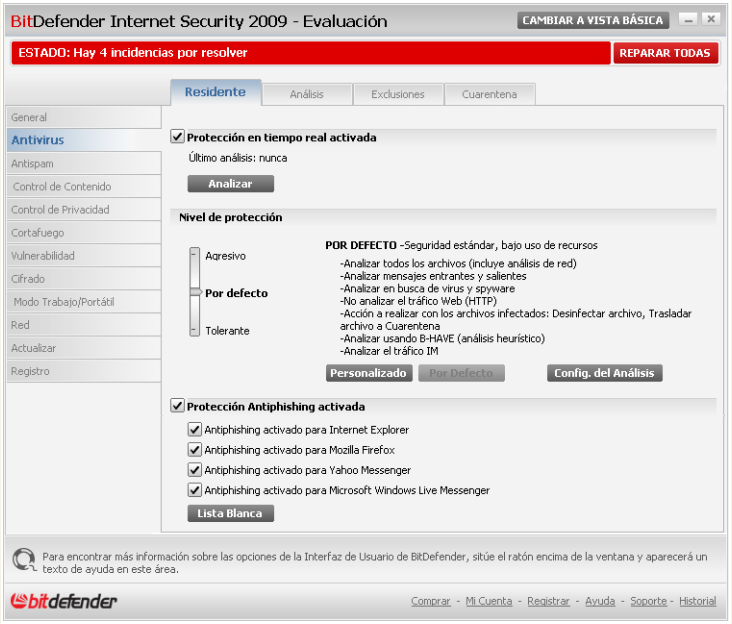
  Nota
  La protección en tiempo real también se denomina análisis al acceder, y se encarga de analizar los archivos a medida que los usuarios acceden a los mismos.

- Análisis bajo demanda - permite detectar y eliminar el malware que ya reside en el 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.

15.1. Protección en Tiempo Real

BitDefender le ofrece una protección ininterrumpida (Protección en Tiempo Real) frente a todo tipo de amenazas de malware, al analizar todos los archivos a los que accede, los mensajes y las comunicaciones a través de aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). El Antiphishing de BitDefender le impide revelar información personal mientras navega por Internet, al avisarle cada vez que detecte una página web de phishing en potencia.

Para configurar y monitorizar la Protección en Tiempo Real y el Antiphishing de BitDefender, haga clic en **Antivirus > Residente** en la Vista Avanzada.



Protección en Tiempo Real

Puede ver si la Protección en Tiempo Real está activada o desactivada. Si desea cambiar el estado de la Protección en Tiempo Real, desmarque o marque la casilla correspondiente.

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

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

15.1.1. 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 de protección adecuado.

Hay 3 niveles de seguridad:

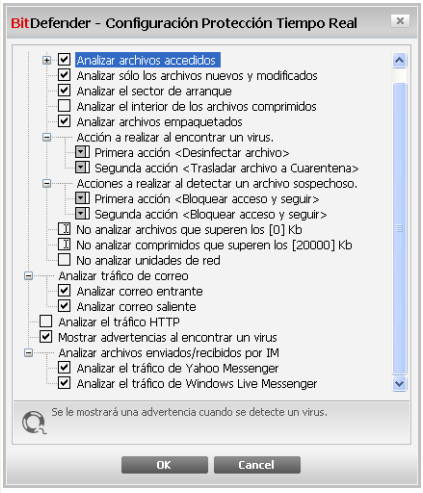
Nivel de Protección	Descripción
Tolerante	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. Los programas y mensajes entrantes se analizan sólo en busca de virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se 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**.

15.1.2. Personalizando el Nivel de Protección

Los usuarios avanzados querrán aprovechar las opciones de análisis que BitDefender ofrece. El análisis puede configurarse para que sólo se analicen 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:



Configuración de la Protección en Tiempo Real

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 pueden desplegarse. 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 archivos a los que accede y las comunicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). Más adelante podrá seleccionar el tipo de archivos 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;`

Opción		Descripción
		.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 el sector 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.
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 archivo infectado, se bloqueará el acceso al mismo.
	Desinfectar archivo	Desinfecta los archivos infectados.

Opción		Descripción
	Eliminar archivo	Elimina los archivos 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 archivo infectado, se bloqueará el acceso al mismo.
	Eliminar archivo	Elimina los archivos 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 comprimidos que superen los [20000] Kb		Introduzca el tamaño máximo de los archivos comprimidos a analizar, en kilobytes (KB). Si desea analizar todos los archivos comprimidos, independientemente de su tamaño, introduzca el valor 0.
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 archivo 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.

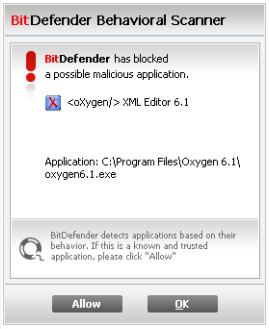
  Si el programa detecta archivos sospechosos, puede iniciar el asistente desde la ventana de alertas para enviar el archivo al Laboratorio BitDefender. Una vez analizado, puede recibir información a través de la dirección de e-mail introducida en el asistente.
- **Analizar archivos enviados/recibidos por IM.** Para analizar los archivos que reciba o envíe a través de Yahoo Messenger o Windows Live Messenger, seleccione la casilla correspondiente.

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

15.1.3. Configurando el Análisis de Comportamiento

El Análisis de Comportamiento le ofrece una capa de protección frente a las nuevas amenazas para las cuales todavía no existe una firma de malware. Monitoriza y analiza constantemente el comportamiento de las aplicaciones que se ejecutan en su equipo y le avisa si alguna aplicación tiene un comportamiento sospechoso.

El Análisis de Comportamiento le alertará cuando una aplicación intente realizar una acción potencialmente maliciosa y le preguntará qué acción aplicar.

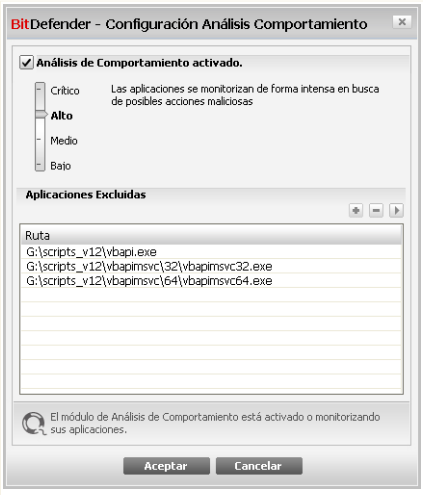


Alerta del Análisis de Comportamiento

Si conoce y confía en la aplicación detectada, haga clic en **Permitir**. El Análisis de Comportamiento dejará de analizar la aplicación en busca de comportamiento potencialmente malicioso.

Si desea cerrar la aplicación de inmediato, haga clic en **Aceptar**.

Para configurar el Análisis de Comportamiento, haga clic en **Config. del Análisis**.



Configuración del Análisis de Comportamiento

Si desea desactivar el Análisis de Comportamiento, desmarque la casilla **Análisis de Comportamiento activado**.

Importante
Mantenga el Análisis de Comportamiento activado para estar protegido frente a los virus desconocidos.

Configurando el Nivel de Protección

El nivel de protección del Análisis de Comportamiento cambia cuando establece un nuevo nivel de protección en tiempo real. Si no está satisfecho con el nivel de protección predeterminado, puede configurar manualmente el nivel de protección.

Nota
Recuerde que si cambia el nivel de protección en tiempo real, el nivel del Análisis de Comportamiento cambiará en consecuencia.

Mueva el control deslizante hasta el nivel de protección que mejor se ajuste a sus necesidades.

Nivel de Protección	*Descripción*
Crítico	Las aplicaciones se monitorizan de forma muy estricta en busca de posibles acciones maliciosas.
Alto	Las aplicaciones se monitorizan de forma intensa en busca de posibles acciones maliciosas.
Mediana	Las aplicaciones se monitorizan de forma moderada en busca de posibles acciones maliciosas.
Bajo	Las aplicaciones se monitorizan en busca de posibles acciones maliciosas.

Administrando las Aplicaciones Excluidas

Puede configurar el Análisis de Comportamiento para que no analice determinadas aplicaciones. Las aplicaciones que actualmente no están siendo controladas por el Análisis de Comportamiento se listan en la tabla **Aplicaciones Excluidas**.

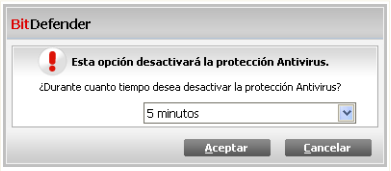
Para administrar las aplicaciones excluidas, puede utilizar los botones situados en la parte superior de la tabla:

- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.

- **Edit** - edit an application path.

15.1.4. 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.

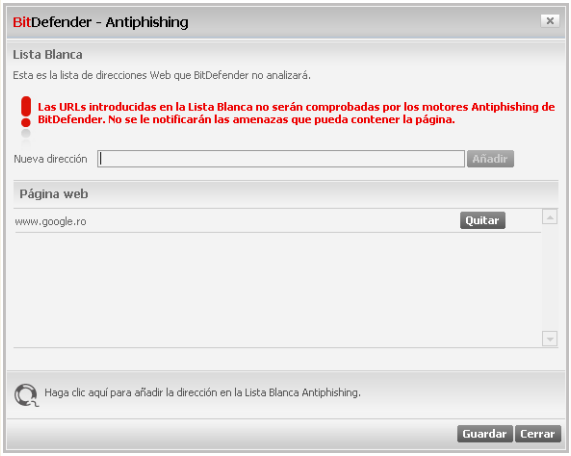
15.1.5. Configurando la Protección Antiphishing

BitDefender ofrece protección antiphishing en tiempo real para:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Puede elegir entre desactivar la protección antiphishing por completo, o sólo para alguna de estas aplicaciones.

Haga clic en **Lista Blanca** para configurar y administrar la lista de páginas web que no deben analizarse con los motores Antiphishing de BitDefender.



Lista Blanca Antiphishing

Puede ver las páginas web que no están siendo analizadas por BitDefender en busca de phishing.

Para añadir una página a la Lista Blanca, introduzca la dirección en el campo **Nueva dirección** y haga clic en **Añadir**. La Lista Blanca sólo debería contener páginas web en las que confíe plenamente. Por ejemplo, añada las páginas web en las que realice compras online.

Nota

Puede añadir páginas web la Lista Blanca fácilmente desde la barra de herramientas de BitDefender Antiphishing integrada en su navegador web.

Si desea quitar una página web de la Lista Blanca, haga clic en el botón **Quitar** correspondiente.

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

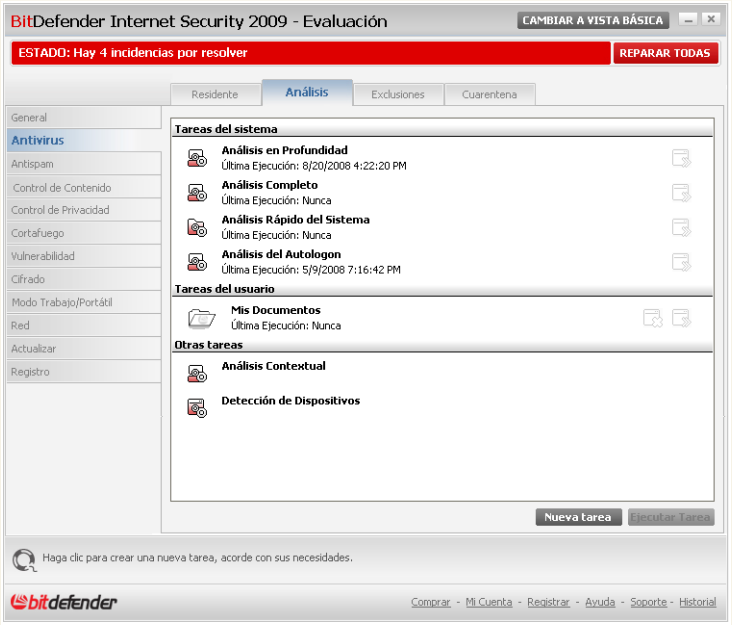
15.2. Análisis Bajo Demanda

El objetivo principal de BitDefender es mantener su ordenador libre de virus. Los dos primeros pasos para lograr esta meta consisten en impedir el acceso de nuevos virus

a su sistema; y en analizar sus mensajes de correo o cualquier archivo 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, diríjase al apartado **Antivirus > Análisis** en la Vista Avanzada.



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.

15.2.1. 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. 158).

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 predeterminada, BitDefender 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 predeterminada, BitDefender 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 predeterminada, BitDefender analiza en busca de cualquier tipo de malware, excepto rootkits, pero no analiza la memoria, el registro ni las cookies.
Análisis del Autologon	Analiza los elementos que se ejecutan cuando un usuario inicia sesión en Windows. El Análisis del Autologon se inicia 3 minutos después que el usuario inicio sesión.

Nota
A través de las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso requerirá bastante 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.

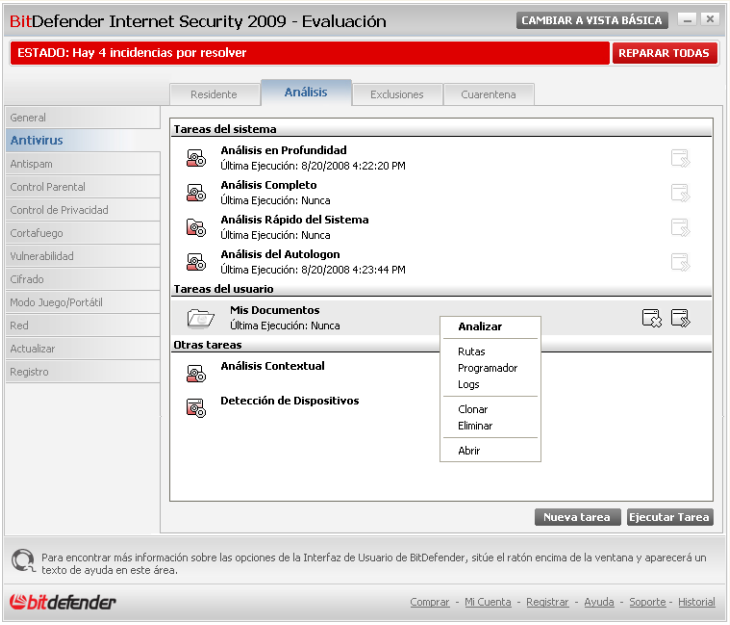
  Nota
  No disponible para tareas de sistema. No se puede eliminar una tarea de sistema.

- **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.

15.2.2. Utilizando el Menú Contextual

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



Menú Contextual

seleccionada para abrirlo.

El menú contextual 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.

> ***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**.

15.2.3. 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.

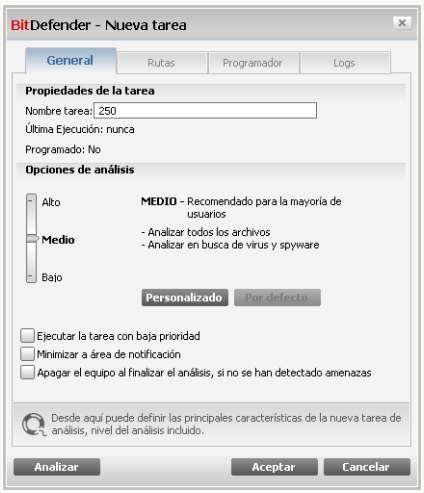
15.2.4. Configurando una Tarea de Análisis

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. 177).

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.

Nivel de Protección	Descripción
	Sólo los programas se analizan en busca de virus. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.
Mediana	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:

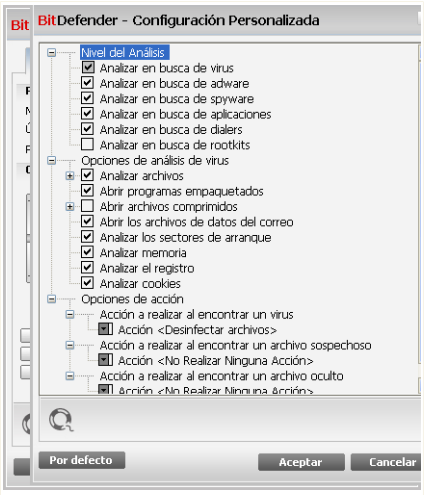
- **Ejecutar el análisis con prioridad baja.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
- **Minimizar ventana de análisis a la barra de tareas.** Minimiza la ventana de análisis a la barra de tareas. Para visualizar la ventana haga doble clic en el icono.
- **Apagar el equipo al finalizar el análisis, si no se han detectado amenazas**

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 que sólo se analicen 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 3 categorías:

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

Opción	*Descripción*
Analizar en busca de virus	Analizar en busca de virus conocidos. 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 archivos se tratarán como si fuesen archivos infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada.

Opción	Descripción
Analizar en busca de spyware	Analiza en busca de spyware. Estos archivos se tratarán como si fuesen archivos infectados.
Analizar en busca de aplicaciones	Analiza en busca de aplicaciones legítimas que pueden utilizarse como herramientas de espionaje, para ocultar aplicaciones maliciosas u otros fines maliciosos.
Analizar en busca de dialers	Analiza en busca de dialers de números de alta tarificación. Estos archivos se tratarán como si fuesen archivos 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 (archivos y procesos), generalmente denominados rootkits.

- **Opciones de análisis de virus.** Indique el tipo de objetos a analizar (tipos de archivo, comprimidos y otros) seleccionado las opciones adecuadas en la categoría **Opciones de análisis de virus**.

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`; `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.

Opción	Descripción
Abrir archivos comprimidos	Para analizar el contenido de los archivos comprimidos. El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema. Haga clic en el campo **Límite de tamaño de comprimidos** e introduzca el tamaño máximo de los archivos comprimidos a analizar, en kilobytes (KB).
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 registro	Analiza las entradas del registro.
Analizar cookies	Analiza los archivos de las cookies.

- **Opciones de acción.** Indique la acción a realizar en cada una de las categorías de archivos detectados, usando las opciones de la categoría **Opciones de acción**.

Nota
Para establecer la nueva acción, haga clic en la acción establecida y seleccione la opción deseada en el menú que aparecerá.

  - 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 archivos infectados. Estos archivos aparecerán en el informe de análisis.
Desinfectar archivos	Elimina el código de malware de los archivos infectados detectados.

Acción	Descripción
Eliminar archivos	Elimina los archivos infectados inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Para trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

- 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 archivos sospechosos. Estos archivos aparecerán en el informe de análisis.
Eliminar archivos	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

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 archivos ocultos. Estos archivos aparecerán en el informe de análisis.
Mover a la Cuarentena	Trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse

Acción	Descripción
	ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.
Hacer visible	Muestra los archivos ocultos para que pueda verlos.

- **Opciones de acción para los archivos comprimidos.** El análisis y tratamiento de los archivos almacenados dentro de los comprimidos están sujetos a algunas restricciones. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Según el formato del archivo comprimido (tipo), es posible que BitDefender no pueda desinfectar, aislar o eliminar los objetos infectados que contenga. Configure las acciones a realizar con los comprimidos detectados a través de las opciones de la categoría **Opciones de acción para los archivos comprimidos**.
  - Seleccione la acción a realizar cuando se detecte un archivo infectado. Dispone de las siguientes opciones:

Acción	Descripción
No Realizar Ninguna Acción	Sólo registra los archivos comprimidos infectados en el informe del análisis. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Desinfectar archivos	Elimina el código de malware de los archivos infectados detectados. La desinfección puede fallar en algunos casos, por ejemplo, cuando el archivo infectado se encuentra dentro de un archivo de datos del correo.
Eliminar archivos	Elimina de forma inmediata los archivos infectados, sin mostrar advertencia alguna.
Mover a la Cuarentena	Traslada los archivos infectados de su ubicación original a la carpeta de la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

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

Acción	Descripción
No Realizar Ninguna Acción	Sólo registra los archivos comprimidos sospechosos en el informe del análisis. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Eliminar archivos	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

- Seleccione la acción a realizar al detectar archivos protegidos con contraseña. Dispone de las siguientes opciones:

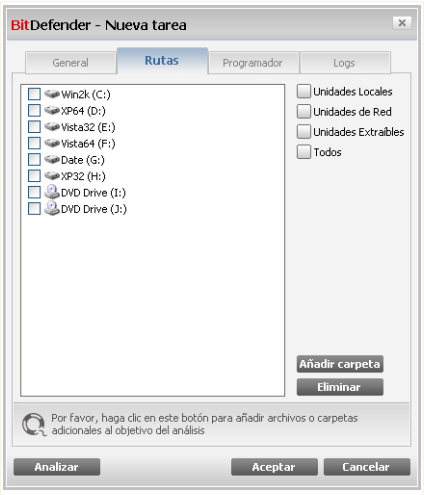
Acción	Descripción
Registrar como no analizado	Sólo registra los archivos comprimidos protegidos con contraseña en el informe del análisis. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Solicitar contraseña	Al detectar un archivo comprimido protegido con contraseña, solicitará la contraseña al usuario para poder analizar el contenido del archivo.

Nota
Si decide ignorar los archivos infectados o la acción elegida falla, debería elegir una nueva acción en el Asistente de Análisis.

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

Estableciendo 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 archivos 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 archivos y carpetas para añadirlos a la lista.

- **Eliminar** - elimina el archivo o carpeta seleccionado de la lista de objetos a analizar.

  Nota
  Sólo podrá eliminar los archivos y carpetas que haya añadido, pero no aquellos detectados 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 de que sean locales, de red o extraíbles.

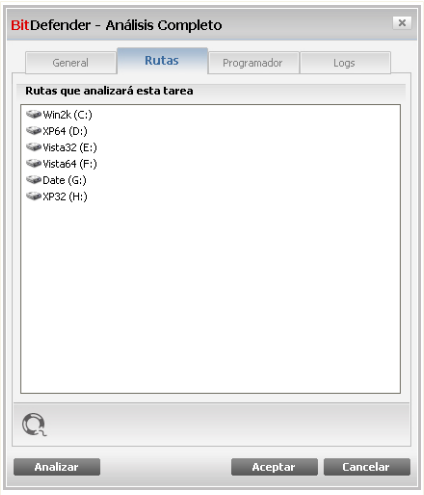
Nota
Si desea analizar todo el sistema en busca de virus, seleccione la casilla correspondiente a **Todas las unidades**.

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

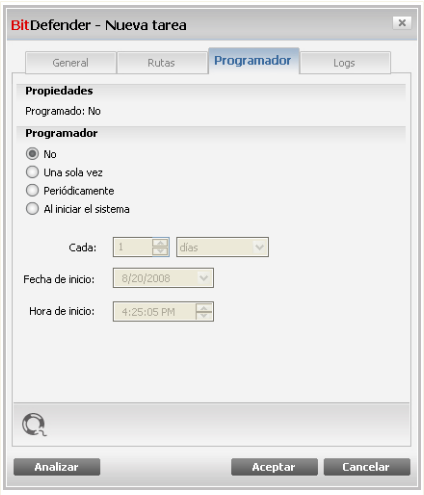
Las tareas **Análisis Completo** y **Análisis en Profundidad** analizarán todas las unidades locales, mientras que la tarea **Análisis Rápido del Sistema** sólo analizará las carpetas `Windows` y `Archivos de Programa`.

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 requerirá bastante tiempo, y funcionará mejor si se cierran los otros programas que puedan estar abiertos. Por esta razón es aconsejable que programe este tipo de tareas con antelación, para que se inicien en aquellos momentos en los 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

Podrá ver la planificación de la tarea.

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** la frecuencia (número de minutos/horas/días/semanas/meses/años) con la que desea repetir el proceso. También puede indicar la fecha y hora de inicio en los campos **Fecha y hora de inicio**.
- **Al iniciar el sistema** - inicia un análisis cuando transcurran los minutos indicados después que el usuario inicie sesión en Windows.

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

15.2.5. 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 archivo o carpeta que desee analizar y seleccione la opción BitDefender Antivirus 2009.
- 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 el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado "*Analizador de BitDefender*" (p. 173).

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

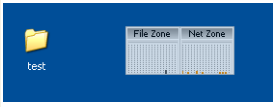
Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **BitDefender Antivirus 2009**.

Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado "*Analizador de BitDefender*" (p. 173).

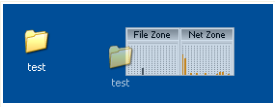
Puede modificar las opciones del análisis o ver los informes en la ventana **Propiedades** de la tarea **Análisis del Menú Contextual**.

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 Archivo



Soltar Archivo

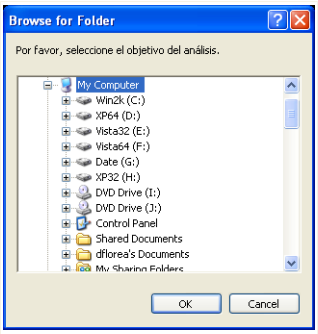
Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado "*Analizador de BitDefender*" (p. 173).

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 2009** → **Análisis Manual de BitDefender** . Aparecerá la siguiente pantalla:



Análisis Manual

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

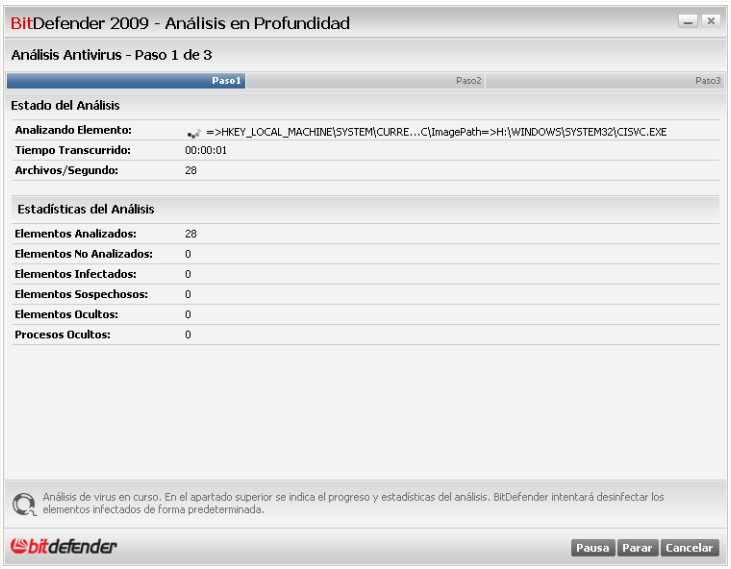
Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado "*Analizador de BitDefender*" (p. 173).

Analizador de BitDefender

Cuando inicie un proceso de análisis bajo demanda, aparecerá el Analizador de BitDefender. 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.

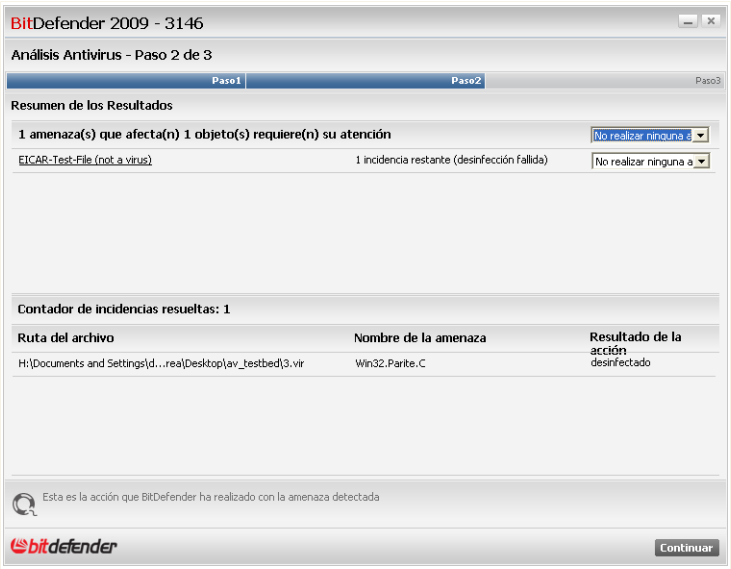
Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

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 donde podrá ver los resultados del análisis.



Acciones

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

Los objetos infectados se muestran agrupados a partir del malware que los ha 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 todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias.

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. Haga clic en **Mostrar Informe** para ver el informe del análisis.

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

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

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.

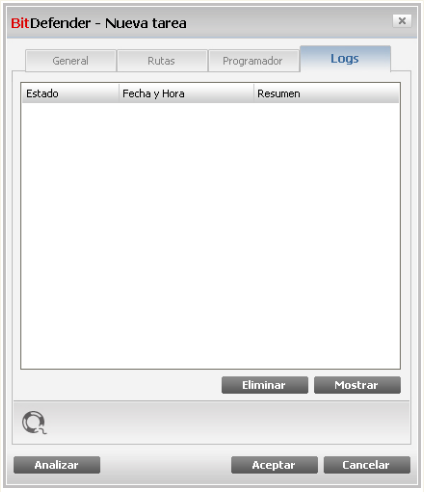
Objetos Sospechosos Detectados por BitDefender

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.

15.2.6. 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:

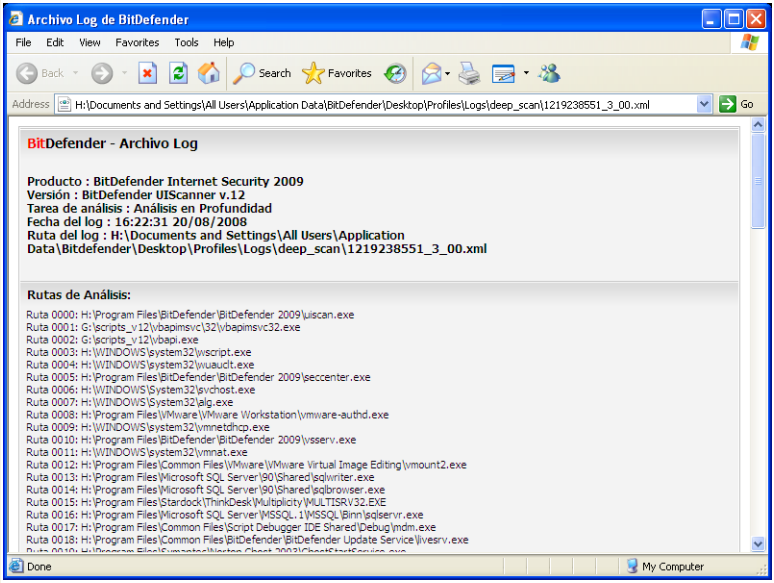
- **Eliminar** - para eliminar el informe del análisis seleccionado.
- **Mostrar** - para ver el informe del análisis seleccionado. El informe del análisis se abrirá en su navegador predeterminado.

Nota
Para ver o eliminar un archivo también puede hacer clic derecho encima del archivo, y seleccionar la opción correspondiente en el menú contextual.

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.

15.3. 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.

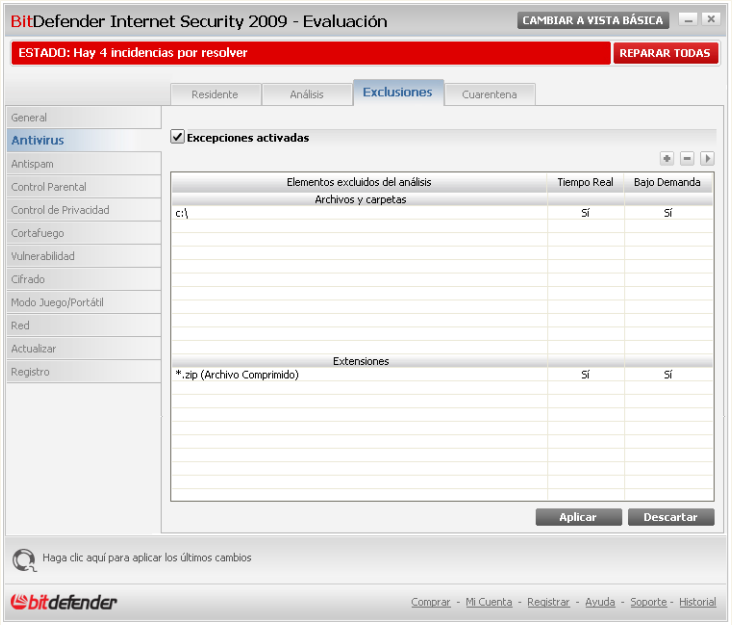
Pueden excluirse del análisis dos tipos de objetos:

- **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 o una aplicación acceden al mismo.

Para ver y administrar los objetos excluidos del análisis, diríjase al apartado **Antivirus > Excepciones** en la Vista Avanzada.



Excepciones

Aquí podrá ver todos los objetos (archivos, carpetas, extensiones) que han sido excluidos del análisis. En cada uno de los objetos podrá ver si ha sido 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 contextual para editarlo o eliminarlo.

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

15.3.1. 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.

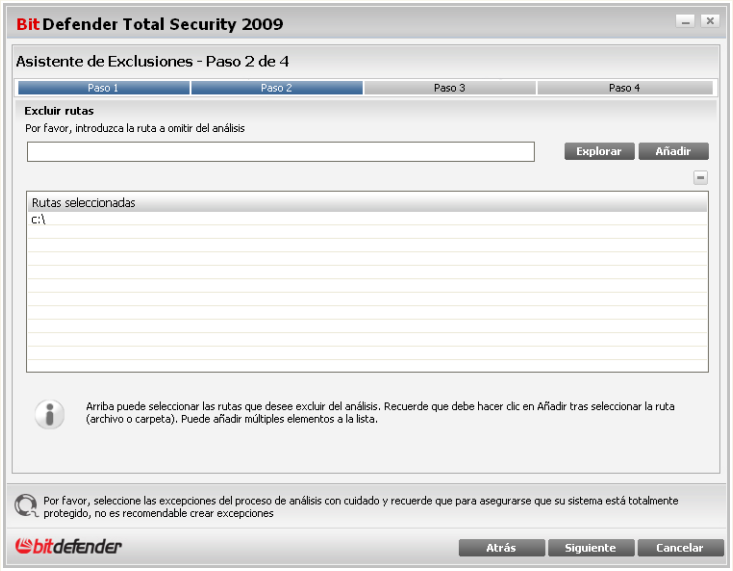
Paso 1/4 – Seleccione el Tipo de Objeto

Tipo de Objeto

Seleccione la opción de exclusión de ruta de análisis.

Haga clic en **Siguiente**.

Paso 2/4 – Indique las 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**.

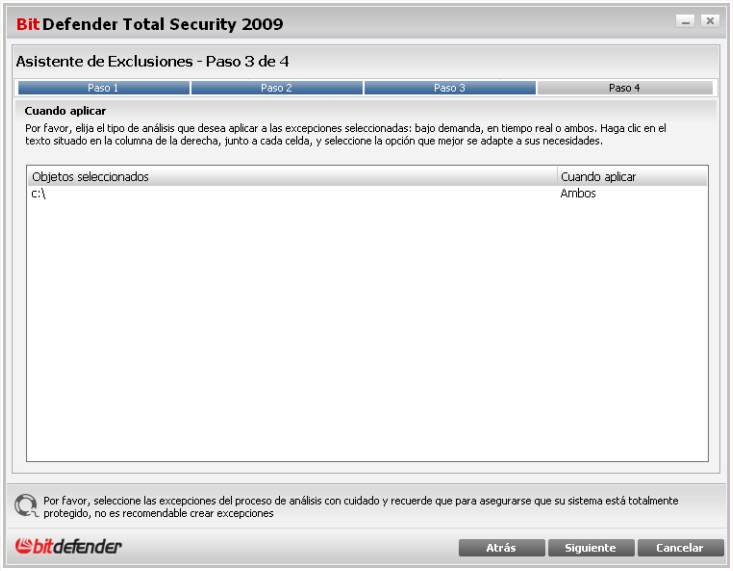
> ***Nota***
> Si la ruta seleccionada no existe, aparecerá un mensaje de error. Haga clic en **Aceptar** y compruebe la validez de ruta.

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 3/4 – Seleccione el Tipo de Análisis



Tipo de Análisis

Verá 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 **Siguiente**.

Paso 4/4 – Analice los Archivos Excluidos

Analice los Archivos Excluidos

Es muy recomendable analizar los archivos de las rutas excluidas para asegurarse que no están infectados. Seleccione la casilla para analizar estos archivos antes de excluirlos del análisis.

Haga clic en **Finalizar**.

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

15.3.2. 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.

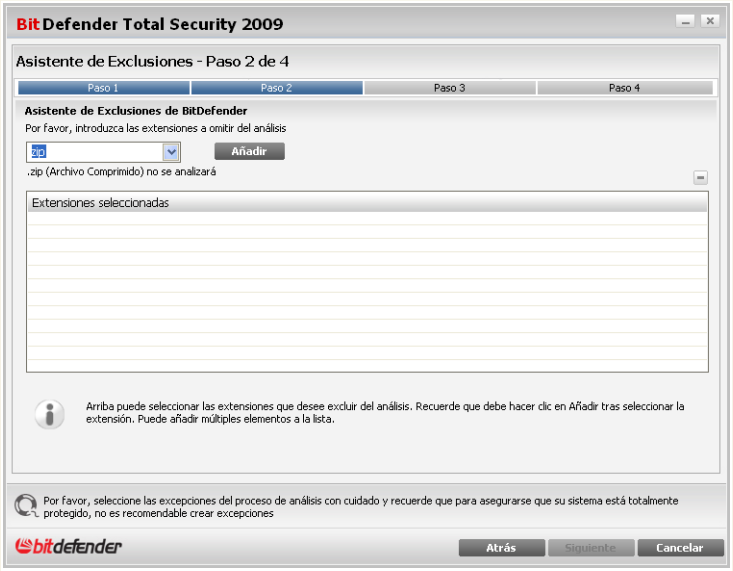
Paso 1/4 – Seleccione el Tipo de Objeto

Tipo de Objeto

Seleccione la opción de exclusión del análisis de una extensión.

Haga clic en **Siguiente**.

Paso 2/4 – Indique las Extensiones Excluidas



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).

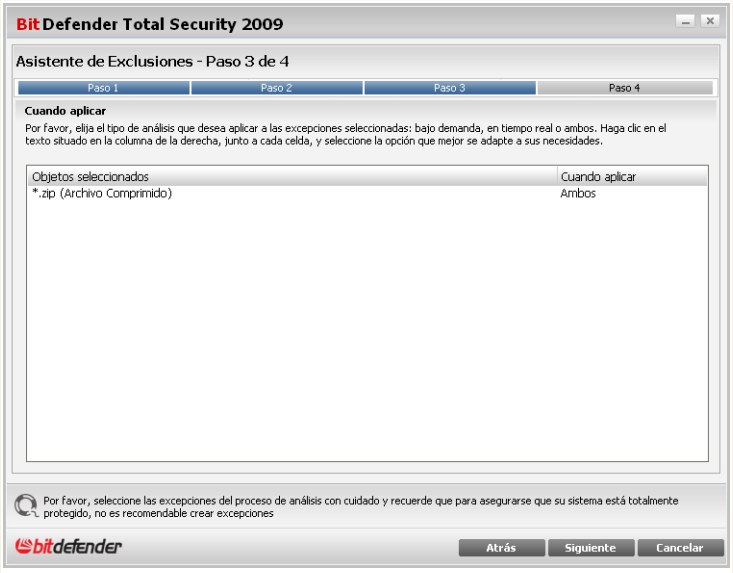
- Introduzca la extensión que desea excluir en el campo editable, y haga clic en **Añadir**.

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 3/4 – Seleccione el Tipo de Análisis



Tipo de Análisis

Verá una tabla que contiene las extensiones a excluir y el tipo de análisis del que han sido excluidas.

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 en la lista.

Haga clic en **Siguiente**.

Paso 4/4 – Seleccione el Tipo de Análisis

Tipo de Análisis

Es muy recomendable analizar los archivos que tienen las extensiones indicadas para asegurarse que no están infectados. Seleccione la casilla para analizar estos archivos antes de excluirlos del análisis.

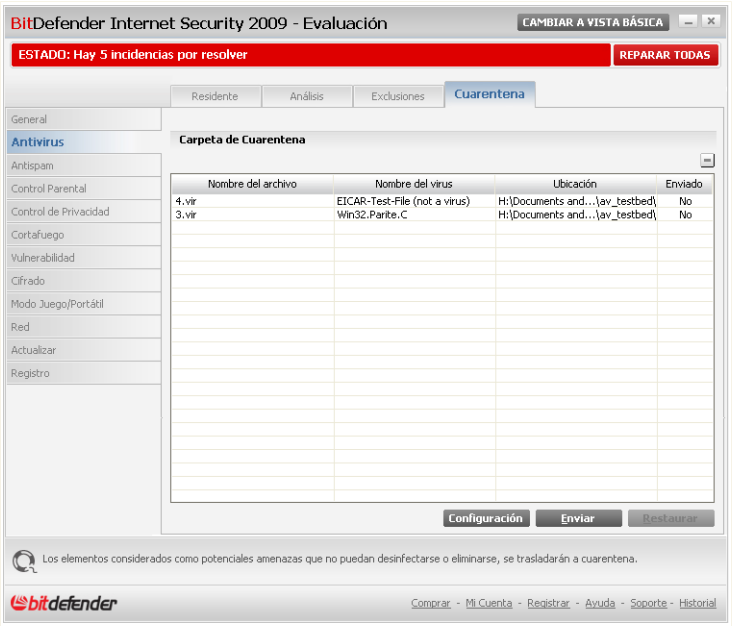
Haga clic en **Finalizar**.

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

15.4. Área de Cuarantena

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

Para ver y administrar los archivos en cuarentena y configurar sus opciones, diríjase al apartado **Antivirus > Cuarentena** en la Vista Avanzada.



Cuarentena

El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena. Podrá ver el nombre del archivo, nombre del virus detectado, ruta de su ubicación original y fecha de traslado a cuarentena de cada uno de los archivos en Cuarentena.

Nota

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

15.4.1. Administrando los Archivos en Cuarentena

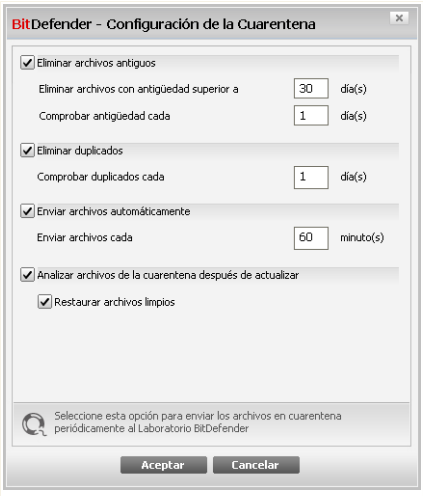
Para eliminar un archivo de la cuarentena haga clic en el botón **Eliminar**. Si quiere restaurar un archivo a su ubicación inicial haga clic en **Restaurar**.

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.

15.4.2. Configurando las Opciones de Cuarentena

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



Configuración de 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.

Analizar archivos de la cuarentena después de actualizar. Para analizar automáticamente los archivos de la cuarentena después de cada actualización, marque la casilla correspondiente. Puede restaurar los archivos desinfectados a su ubicación original, seleccionando la opción **Restaurar archivos limpios**.

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

16. 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.

16.1. 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.

16.1.1. Los Filtros Antispam

El motor BitDefender Antispam incorpora varios filtros 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 de Amigos y Lista de Spammers

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).

Puede gestionar la Lista de Amigos / Spammers desde la Vista Avanzada 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 ejemplo, 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 las decisiones del módulo Bayesiano utilizando los botones **Es Spam** y **No Spam** desde la Barra de Herramientas Antispam.

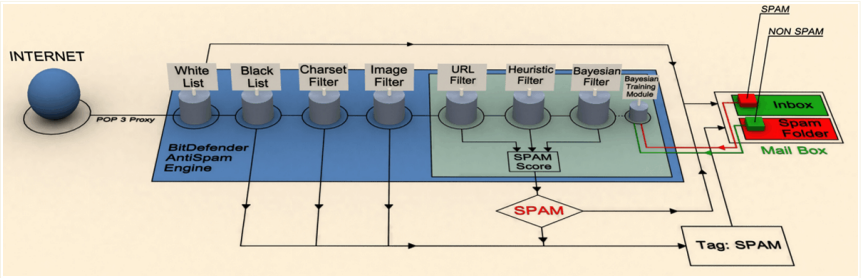
Nota
Cada vez que realiza una actualización:

- se añaden nuevas firmas 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 eficacia de los motores Antispam.
Para protegerle contra los spammers, BitDefender puede realizar actualizaciones automáticas. Mantenga activada la opción **Actualización automática**.

16.1.2. 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 que provenga de Internet pasará primero por los filtros Lista de Amigos/Lista de Spammers. 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.

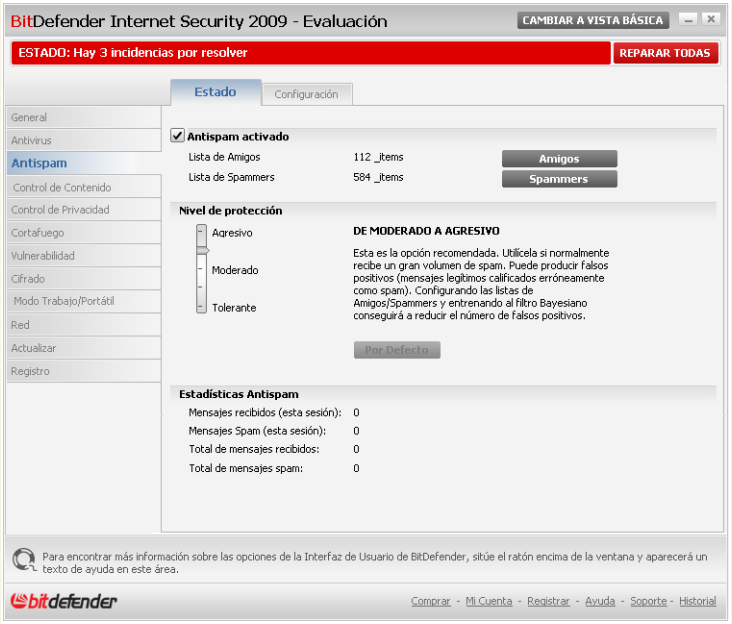
El Filtro Bayesiano clasifica los mensajes según datos estadísticos referentes a la índice de aparición de determinadas palabras en mensajes clasificados como SPAM en comparación con aquellos declarados como NO-SPAM (por el administrador o por el filtro heurístico). Se añadirá una puntuación de SPAM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

16.2. Estado

Para configurar la protección Antispam, diríjase al apartado **Antispam > Estado** en la Vista Avanzada.



Estado del Antispam

Podrá ver si la protección Antispam está activada o desactivada. Si desea cambiar el estado del Antispam, desmarque o marque la casilla correspondiente.

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).

16.2.1. Estableciendo 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 de protección adecuado.

Hay 5 niveles de protección:

Nivel de Protección	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 Permisivo 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). 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**.

16.2.2. Configurando la 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
Cualquier mensaje que provenga de una dirección incluida en la **Lista de Amigos** llegará directamente a su Bandeja de Entrada.

Para configurar la Lista de Amigos, haga clic en **Amigos** (o haga clic en el botón **Amigos** de 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 al cargar 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**.

16.2.3. Configurando la 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 configurar la Lista de Spammers, haga clic en **Spammers** (o haga clic en el botón **Spammers** de 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 al cargar 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 desea reinstalar BitDefender, recomendamos guardar las listas de **Amigos** / **Spammers** antes de iniciar el proceso, para así volver a cargarlas cuando finalice la reinstalación.

16.3. Configuración

Para modificar la configuración del antispam, diríjase al apartado **Antispam > Configuración** en la Vista Avanzada.

Configuración 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 "+" para abrir una categoría, o en la casilla "-" para cerrar una categoría.

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

Si desea aplicar la configuración predeterminada, haga clic en **Por Defecto**.

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

16.3.1. 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.

16.3.2. Filtros Antispam Básicos

- **Lista de Amigos / Spammers** - filtra los mensajes a partir de las listas 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** - cuando haga clic en el botón **No Spam** de la Barra de Herramientas Antispam, el remitente será añadido automáticamente a la Lista de Amigos.
  - **Añadir automáticamente a la Lista de Spammers** - cuando haga clic en el botón **Es Spam** de la Barra de Herramientas Antispam, el remitente será añadido automáticamente a la Lista de Spammers.

Nota
Los botones **No Spam** y **Es Spam** se utilizan para entrenar al 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.

16.3.3. 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 al Motor de Aprendizaje (bayesiano) con los correos salientes** - entrena el Motor de Aprendizaje (bayesiano) con los mensajes 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.

17. Control de Contenido

El Control de Contenido de BitDefender le permite controlar el acceso a Internet y a determinadas aplicaciones de cada una de las cuentas de usuario de Windows del sistema.

Puede configurar Control de Contenido para que bloquee:

- páginas web con contenido inadecuado.
- la conexión a Internet durante determinados periodos de tiempo (por ejemplo, en las horas de estudio).
- páginas web, mensajes de correo y conversaciones de mensajería instantánea que contengan determinadas palabras clave.
- aplicaciones como juegos, chat, aplicaciones de intercambio de archivos u otros.
- mensajes enviados por contactos de mensajería instantánea que no provengan de los contactos permitidos.

Importante

Sólo los usuarios con permisos de administrador (administradores del sistema) pueden acceder y configuar el Control de Contenido. Para asegurarse que nadie modifica la configuración del Control de Contenido de los usuarios, puede proteger la configuración con una contraseña. Se le pedirá configurar una contraseña cuando active el Control de Contenido de un usuario determinado.

Para configurar correctamente el Control de Contenido y restringir las actividades online y en el equipo de sus hijos, debe completar estas tareas:

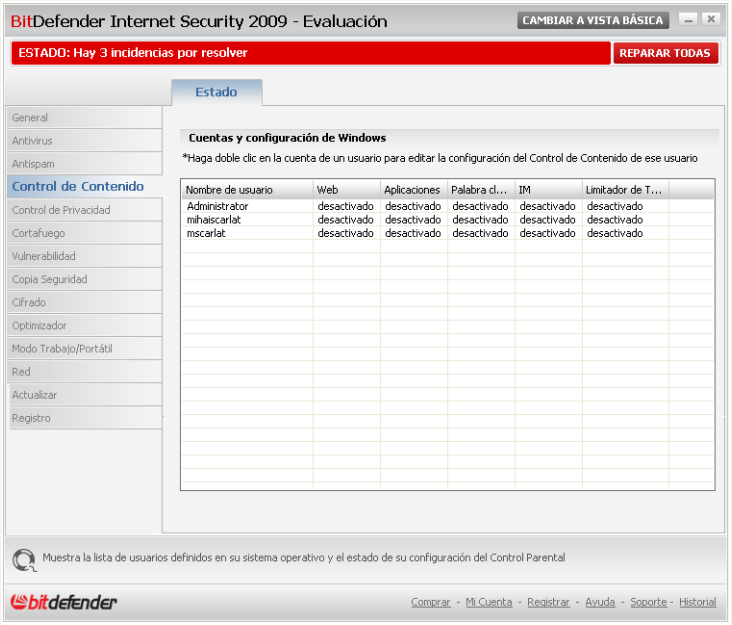
1. Crear una cuenta de usuario de Windows limitada (estándar) para sus hijos.

Nota

Para aprender a crear cuentas de usuario de Windows, diríjase al Centro de Ayuda y Soporte Técnico de Windows (en el menú Inicio, haga clic en **Ayuda y soporte técnico**).

2. Configure el Control de Contenido de las cuentas de usuario de Windows que ha creado para sus hijos.

Para configurar el Control de Contenido, diríjase al apartado **Control de Contenido** en la Vista Avanzada.



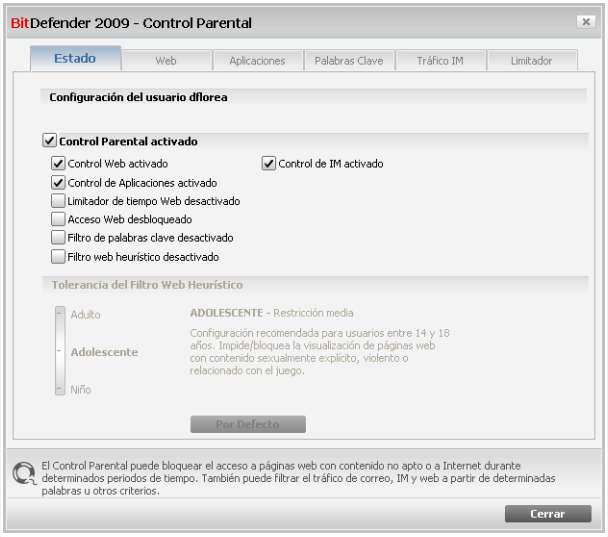
Control de Contenido

Podrá ver el estado de las opciones del Control de Contenido configuradas para cada una de las cuentas de usuario de Windows. Haga doble clic en el nombre de usuario para el que desea configurar el Control de Contenido.

En los siguientes apartados de este capítulo se le presentan las características del Control de Contenido y cómo configurarlas.

17.1. Estado de la Configuración por Usuario

Para configurar el Control de Contenido de un usuario concreto, haga doble clic sobre el nombre del usuario y diríjase a la pestaña **Estado**.



Estado del Control de Contenido

Para configurar el Control de Contenido de este usuario, siga estos pasos:

1. Active el Control de Contenido de ese usuario marcando la casilla situada junto a **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.

2. Establezca una contraseña para proteger la Configuración del Control de Contenido. Para más información, por favor, consulte el apartado "*Protegiendo la Configuración del Control de Contenido*" (p. 210) de esta guía.
3. Seleccione las casillas correspondientes a los controles de protección que desee utilizar:
   - **Control Web** - para filtrar la navegación web según las reglas establecidas en el apartado Web.
   - **Control de Aplicaciones** - para bloquear el acceso a las aplicaciones que ha especificado en el apartado Control de Aplicaciones.

- **Control de Mensajería Instantánea** - para permitir o bloquear los chats con los contactos IM según las reglas establecidas en el apartado Tráfico IM.
- **Limitador de Tiempo Web** - para permitir o bloquear el acceso web según el horario especificado en el apartado Limitador.
- **Acceso Web** - para bloquear el acceso a todas las páginas web (no sólo las que aparecen en el apartado Web).
- **Filtro de Palabras Clave** - para filtrar el acceso a páginas web, correo y mensajería instantánea según las reglas especificadas en el apartado Palabras Clave.
- **Filtro Web Heurístico** - para filtrar el acceso web según las reglas predefinidas basadas en categorías por edad.

4. 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.

17.1.1. 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 de BitDefender 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.

Cuando active el Control de Contenido, BitDefender le solicitara introducir una contraseña.

Establecer la Protección por 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.

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**.

17.1.2. 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:

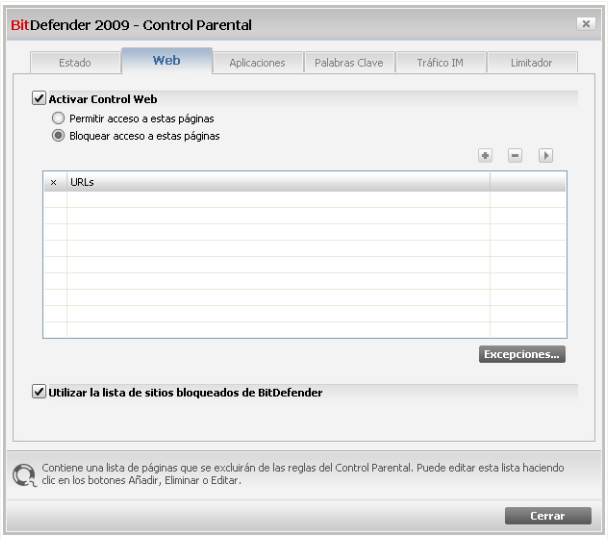
Nivel de tolerancia	Descripción
Niño	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios menores de 14 años. Se bloqueará el acceso a las páginas web con contenido potencialmente dañino para los niños (porno, sexualidad, drogas, hacking, etc).
Adolescente	Se bloqueará 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.

17.2. 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 de un usuario concreto, haga doble clic en el nombre de usuario correspondiente y a continuación haga clic en la pestaña **Web**.



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.

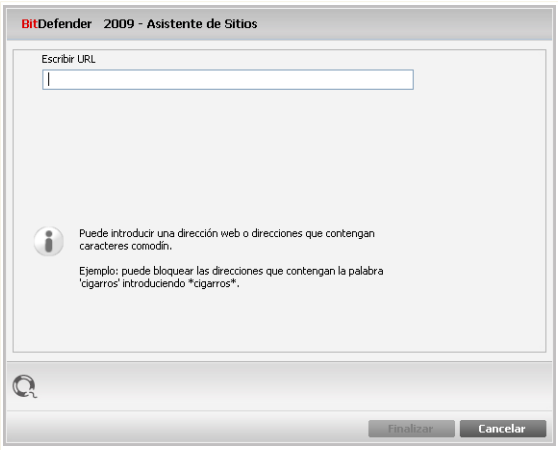
Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar una regla selecciónela y haga clic en el botón **Editar..** o haga doble clic sobre la regla. Para desactivar temporalmente una regla sin eliminarla, desmarque la casilla correspondiente a la regla.

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

17.2.1. 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**.

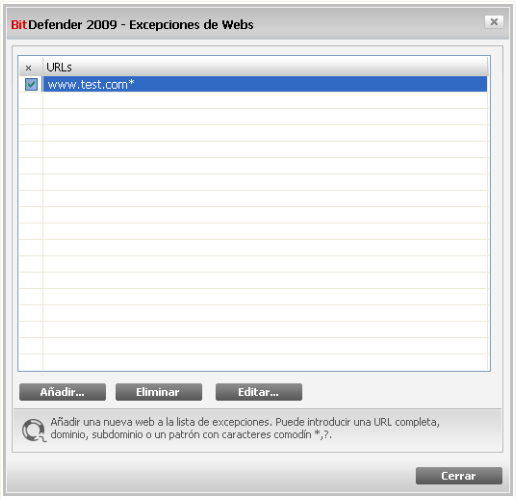
Importante
Sintaxis:

- `*.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.

17.2.2. 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.

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.

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

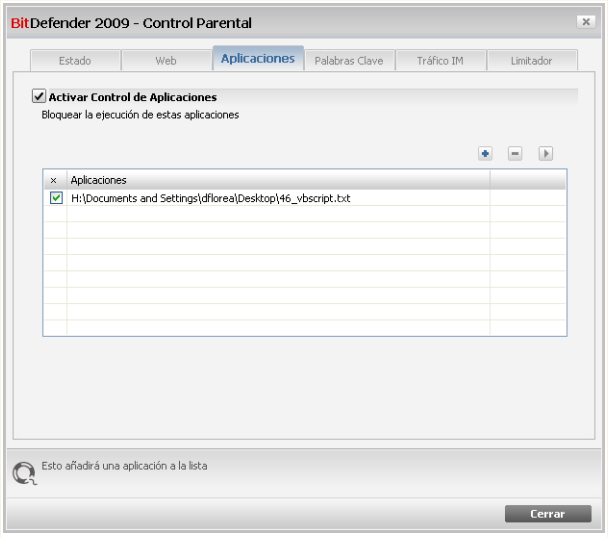
17.2.3. Lista Negra de Webs de BitDefender

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**.

17.3. 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 de un usuario concreto, haga doble clic en el nombre de usuario correspondiente, y a continuación haga clic en la pestaña **Aplicaciones**.



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.

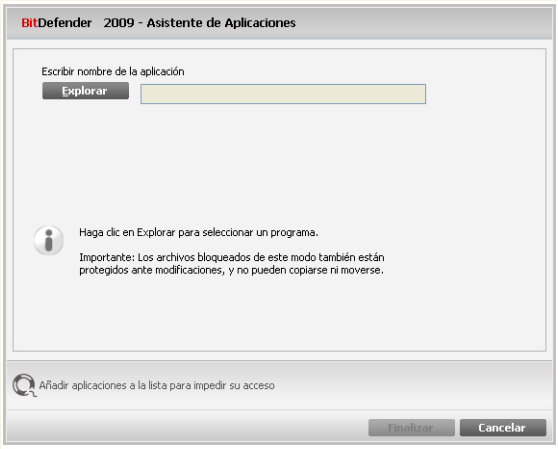
Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar una regla selecciónela y haga clic en el botón **Editar..** o haga doble clic sobre la regla. Para desactivar temporalmente una regla sin eliminarla, desmarque la casilla correspondiente a la regla.

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

17.3.1. 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

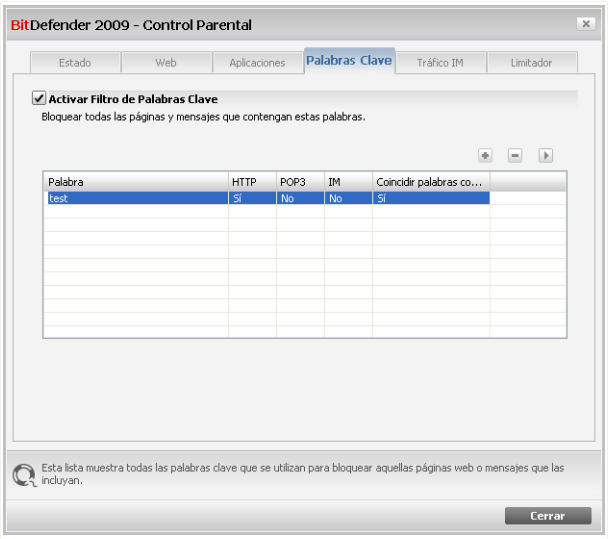
Haga clic en **Añadir**, clic en **Explorar**, seleccione la aplicación a bloquear y haga clic en **Finalizar**.

17.4. Filtro de Palabras Clave

El Filtro de Palabras Clave le ayuda a bloquear el acceso a los correos, páginas web o conversaciones de chat que contengan las palabras especificadas. A través del Filtro de Palabras Clave puede impedir que sus hijos vean palabras o frases inapropiadas mientras están conectados a Internet.

Nota
El Filtro de Palabras Clave de la mensajería instantánea sólo está disponible para Yahoo Messenger y Windows Live (MSN) Messenger.

Para configurar el Filtro de Palabras Clave de un usuario concreto, haga doble clic en el correspondiente nombre de usuario, y a continuación haga clic en la pestaña **Palabras clave**.



Filtro de Palabras Clave

Marque la casilla **Activar Filtro de Palabras Clave** si desea utilizar esta característica.

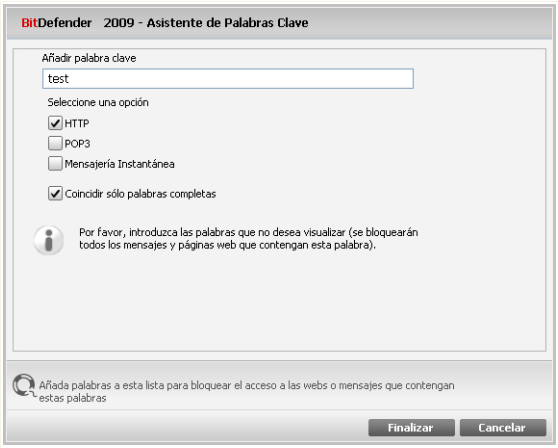
Deberá añadir reglas para indicar las palabras clave que deben bloquearse. Para añadir una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para editar una regla existente, haga doble clic encima de la regla o haga clic en el botón **Editar** y realice los cambios oportunos en la ventana de configuración.

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

17.4.1. Ventana de Configuración

Cuando edite o añada reglas, aparecerá una ventana de configuración.



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.

Opción	Descripción
POP3	Los e-mails que contengan la palabra clave serán bloqueados.
HTTP	Las páginas web que contengan la palabra clave serán bloqueados.

Opción	Descripción
Mensajería Instantánea	Los mensajes de mensajería instantánea que contengan la palabra clave serán bloqueados.

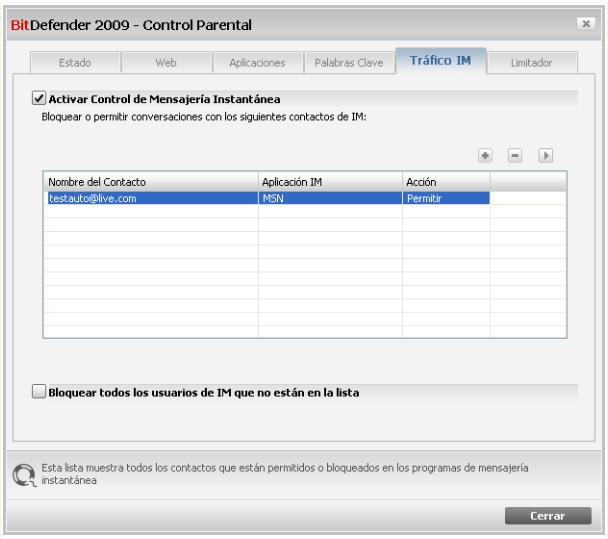
Haga clic en **Finalizar** para añadir la regla.

17.5. Control de Mensajería Instantánea (IM)

El Control de Mensajería Instantánea (IM) le permite especificar los contactos con los que sus hijos pueden chatear.

Nota
El Control de Mensajería Instantánea (IM) sólo está disponible para Yahoo Messenger y Windows Live (MSN) Messenger.

Para configurar el Control IM de un usuario concreto, haga doble clic en el correspondiente nombre de usuario, y a continuación haga clic en la pestaña **Tráfico IM**.



Control de Mensajería Instantánea

Marque la casilla **Control de Mensajería Instantánea** si desea utilizar esta característica.

Deberá añadir reglas para especificar los contactos IM con los puede comunicarse o no un usuario. Para añadir una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

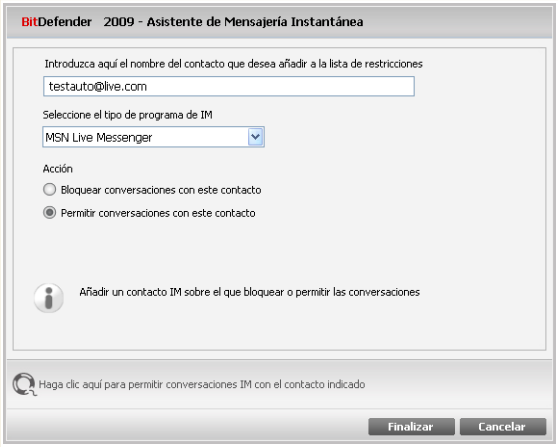
Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para editar una regla existente, haga doble clic encima de la regla o haga clic en el botón **Editar** y realice los cambios oportunos en la ventana de configuración.

Cuando haya definido todos los contactos IM con los que el usuario está autorizado a comunicarse, seleccione la opción **Bloquear todos los usuarios de IM que no están en la lista**. De esta manera, el usuario sólo podrá recibir los mensajes instantáneos de los contactos IM autorizados de forma explícita.

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

17.5.1. Ventana de Configuración

Cuando edite o añada reglas, aparecerá una ventana de configuración.



Añadir un Contacto IM

Siga estos pasos:

1. Introduzca el nombre de usuario (ID) del contacto IM.

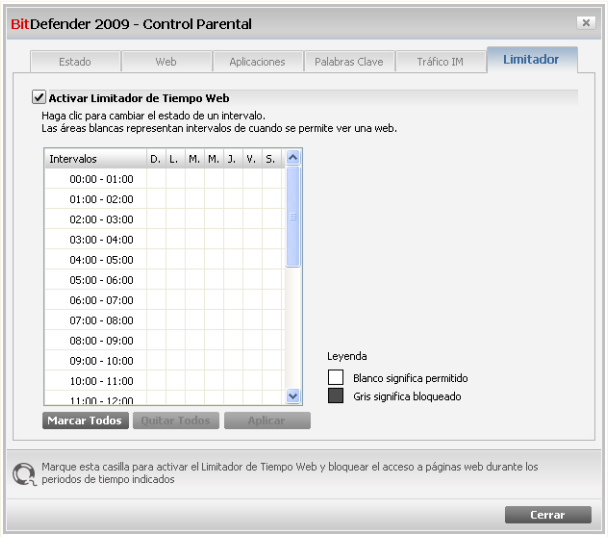
2. Seleccione el programa de mensajería asociado a este contacto.
3. Seleccione la acción de la regla:
   - **Bloquear conversaciones con este contacto**
   - **Permitir conversaciones con este contacto**
4. Haga clic en **Finalizar** para añadir la regla.

17.6. 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 Web de un usuario concreto, haga doble clic en el correspondiente nombre de usuario, y a continuación haga clic en la pestaña **Limitador**.



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.

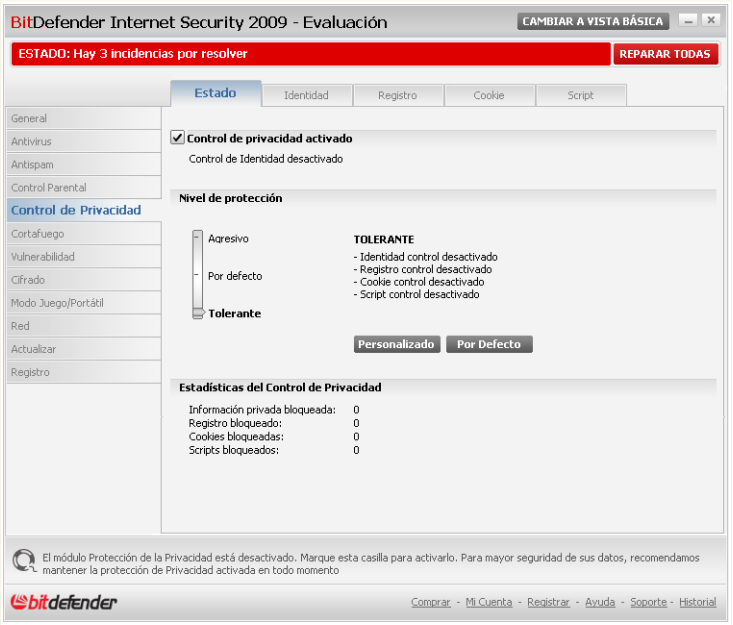
Haga clic en **Aplicar** para guardar los cambios.

18. 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.

18.1. 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 Vista Avanzada.



Estado del Control de Privacidad

Puede ver si el Control de Privacidad está activado o desactivado. Si desea cambiar el estado del Control de Privacidad, desmarque o marque la casilla correspondiente.

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 los siguientes importantes controles de protección:

- Control de Identidad - protege sus datos confidenciales filtrando todo el tráfico web (HTTP), de correo (SMTP) y mensajería instantánea saliente según las reglas creadas en el apartado Identidad.
- Control del Registro - le pedirá permiso cada vez que un programa intente modificar un entrada del registro para 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.

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

18.1.1. 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 de protección adecuado.

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 Scripts** 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.

18.2. 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 como de su número de tarjeta de crédito, cuando esta información no cae en buenas manos puede resultar peligrosa: puede ahogarse entre una multitud de mensajes de spam o encontrar vacía su cuenta bancaria.

El Control de Identidad le protege del robo de información personal mientras está conectado a Internet. En función de las reglas que cree, el Control de Identidad analizará el tráfico web, e-mail y mensajería instantánea que sale de su equipo en busca de las cadenas de texto indicadas (por ejemplo, su número de tarjeta de crédito). En caso de coincidencia, se bloqueará la página web, correo o mensaje instantáneo correspondiente.

Puede crear reglas para proteger cualquier tipo de información que considere personal o confidencial, desde su número de teléfono o e-mail hasta información de su cuenta bancaria. BitDefender incluye soporte multiusuario, para que los usuarios que inicien sesión en diferentes cuentas de usuario de Windows puedan usar sus propias reglas de protección de la identidad. Las reglas que ha creado sólo serán accesibles y se aplicarán cuando inicie sesión con su cuenta de Windows.

¿Por qué usar el Control de Identidad?

- El Control de Identidad es muy efectivo bloqueando spyware de tipo keylogger. Este tipo de aplicaciones maliciosas capturan lo que escribe a través del teclado y lo envían a hackers o cibercriminales a través de Internet. El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.

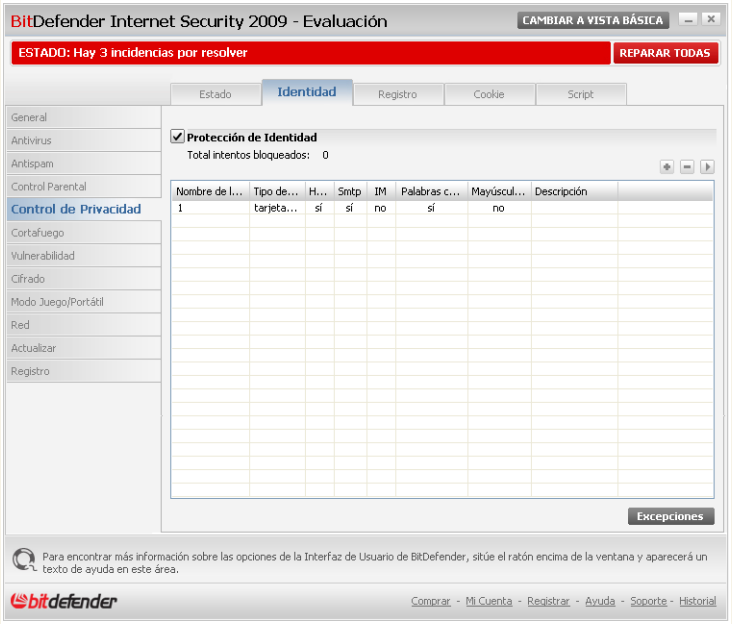
  Imaginemos que una aplicación de este tipo consigue eludir la detección antivirus. Si ha creado las reglas de protección de la identidad adecuadas, el keylogger no podría enviar información personal por e-mail web ni mensajería instantánea.

- El Control de Identidad puede protegerle de tentativas de phishing (intentos de robo de información personal). El tipo de phishing más habitual utiliza mensajes engañosos para inducirle a enviar información personal a través de una página web falsa.

  Por ejemplo, puede recibir mensajes que simulan provenir de su banco/caja y le soliciten actualizar su información bancaria urgentemente. Este mensaje incluye un enlace a una página web en la que debe introducir la información personal actualizada. Aunque puedan parecer legítimos, tanto la dirección de correo como la página a la que le dirige el enlace engañoso son falsos. Si hace clic en el enlace del mensaje y envía su información personal a través de la página web falsa, en realidad estará revelando sus datos a las personas que han organizado el intento de phishing.

  Si configura las reglas de protección de la identidad adecuadas, no podrá enviar información personal (como el número de su tarjeta de crédito) a través de una página web, a menos que la haya definido explícitamente como excepción a las reglas.

Para configurar el Control de Identidad, diríjase al apartado **Control de Privacidad > Identidad** en la Vista Avanzada.



Control de Identidad

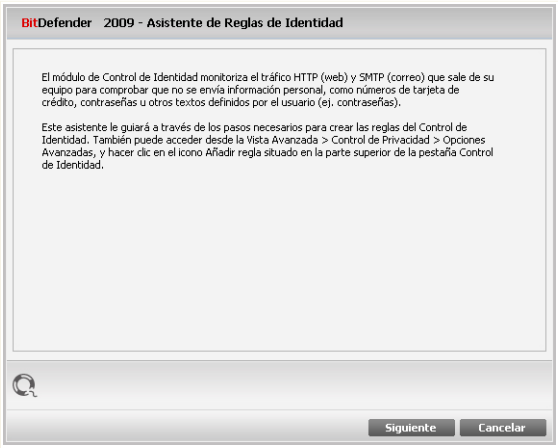
Si desea usar el Control de Identidad, siga estos pasos:

1. Marque la casilla **Protección de Identidad**.
2. Cree las reglas necesarias para proteger su información personal. Para más información, por favor, consulte el apartado "*Creando Reglas de Identidad*" (p. 228) de esta guía.
3. En caso necesario, puede definir excepciones a las reglas que ha creado. Para más información, por favor, consulte el apartado "*Definiendo las Excepciones*" (p. 232).

18.2.1. Creando Reglas de Identidad

Para crear una regla de protección de la identidad, haga clic en el botón **Añadir** y siga los pasos del Asistente de Configuración.

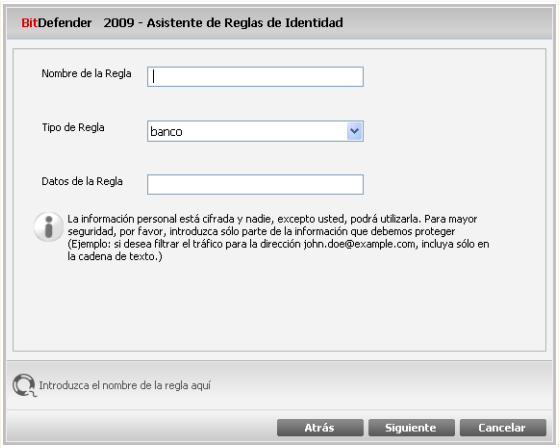
Paso 1/4 - Ventana de Bienvenida



Ventana de Bienvenida

Haga clic en **Siguiente**.

Paso 2/4 - Seleccione el Tipo de Regla y los Datos



Seleccionar el tipo y datos de la regla

Debe configurar los siguientes parámetros:

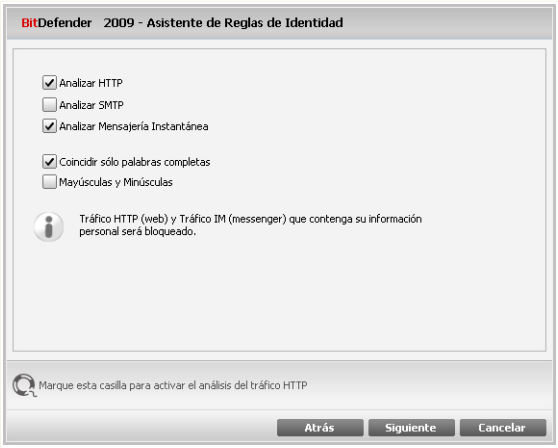
- **Nombre de la Regla** - introduzca el nombre de la regla en este campo editable.
- **Tipo de Regla** - elija el tipo de regla (dirección, nombre, tarjeta de crédito, PIN, etc).
- **Datos de la Regla** - introduzca los datos que desee proteger en este campo editable. Por ejemplo, si quiere proteger su número de tarjeta de crédito, introduzca toda la secuencia de números, o parte de ésta, en este campo.

> ***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 3/4 - Seleccione el Tráfico



Seleccionar Tráfico

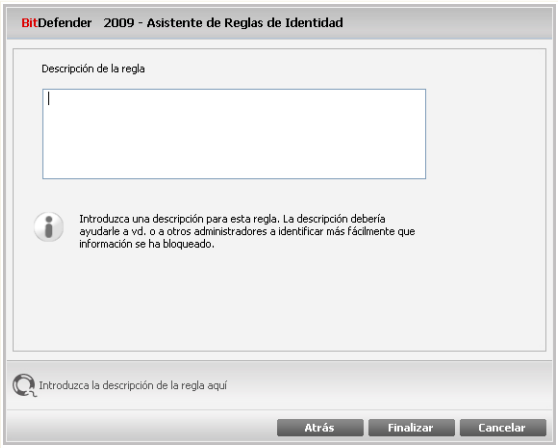
Debe seleccionar el tipo de tráfico que BitDefender analizará. Dispone de las siguientes opciones:

- **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 (correo) y bloquea los mensajes salientes que coinciden con los datos de la regla.
- **Analizar Mensajería Instantánea** - analiza el tráfico de Mensajería Instantánea y bloquea los mensajes de chat 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 de texto detectada coinciden en mayúsculas y minúsculas.

Haga clic en **Siguiente**.

Paso 4/4 – Describa la Regla



Describa la regla

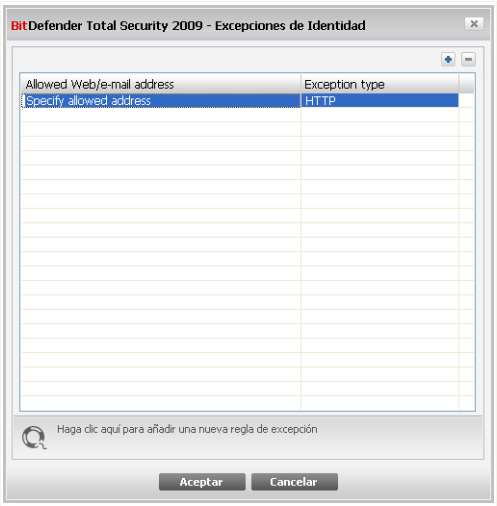
Introduzca una breve descripción de la regla en el campo editable. Como los datos bloqueados (las cadena de texto) no se muestran en texto plano cuando accede a la regla, es importante introducir una breve descripción que le ayude a identificar fácilmente los datos que protege.

Haga clic en **Finalizar**. La nueva regla aparecerá en la tabla.

18.2.2. 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 **Indique las direcciones permitidas** e introduzca la dirección de la página, el correo electrónico o el contacto de mensajería 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**.
   - Si ha introducido un contacto de mensajería instantánea, seleccione **IM**.

Para eliminar una excepción de la lista, selecciónela y haga clic en **Eliminar**.

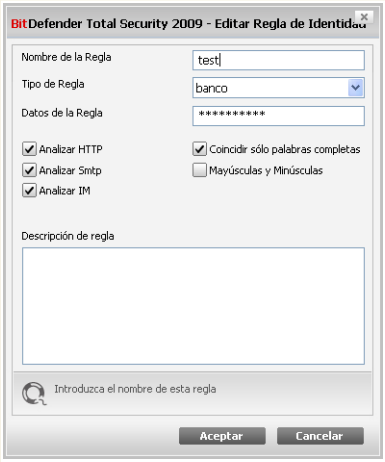
Haga clic en **Aplicar** para guardar los cambios.

18.2.3. Administrando Reglas

Puede ver las reglas listadas hasta el momento en la tabla.

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

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

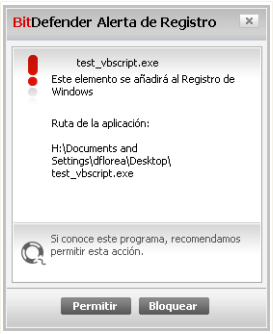
Aquí puede cambiar el nombre, la descripción y los parámetros de la regla (tipo, datos y tráfico). Haga clic en **Aceptar** para guardar los cambios.

18.3. 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

Podrá ver el nombre de la aplicación que intenta modificar el Registro de Windows.

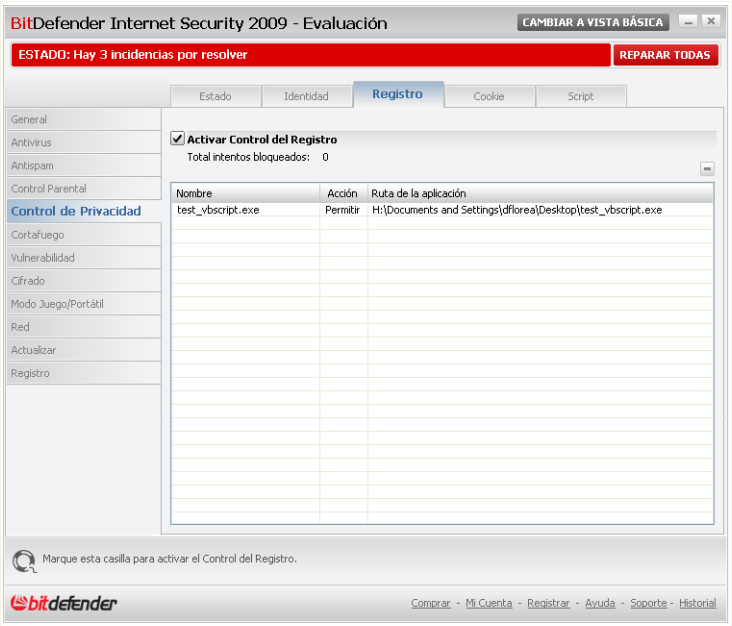
Si no reconoce esta aplicación y le parece sospechosa, haga clic en **Bloquear** para impedir que modifique el Registro de Windows. De lo contrario, haga clic en **Permitir** para autorizar la modificación.

A partir de su respuesta, se creará una regla que quedará listada en la tabla de reglas. Se aplicará la acción que ha indicado cada vez que esta aplicación intente modificar el Registro de 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.

Para configurar el Control del Registro, diríjase al apartado **Control de Privacidad > Registro** en la Vista Avanzada.



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**.

18.4. 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.

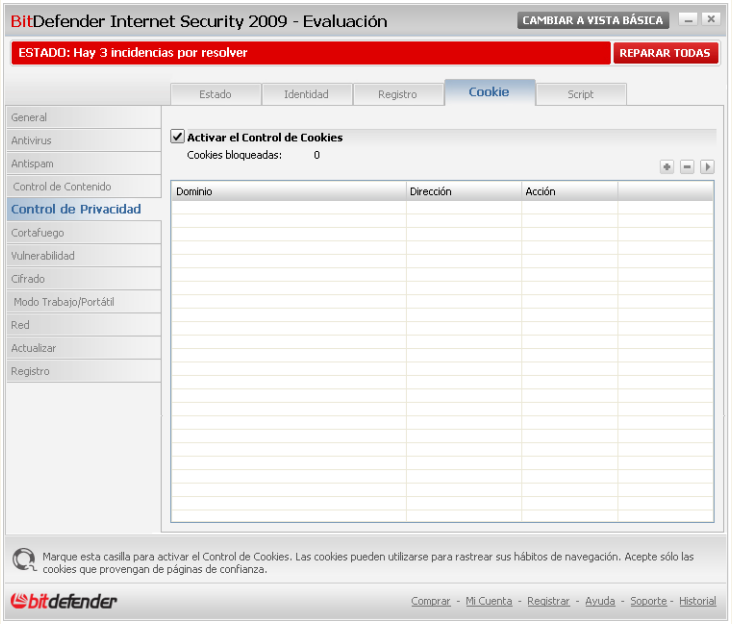
Marque la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No**, para crear una nueva regla de permiso, que se aplicará y aparecerá en la tabla de reglas. La próxima vez que se conecte al mismo sitio no recibirá esta notificación.

Esto le ayudará a decidir cuáles son los sitios web de confianza y cuáles no.

Nota

Debido al gran número de cookies que se usan hoy en día en Internet, el **Control de Cookies** puede resultar un poco molesto al principio. Recibirá muchas preguntas sobre las páginas que intentan enviar cookies a su equipo. Pero, en cuanto añada sus páginas de confianza al listado de reglas, navegar por Internet volverá a ser tan fácil como antes.

Para configurar el Control de Cookies, diríjase al apartado **Control de Privacidad > Cookie** en la Vista Avanzada.



Control de las Cookies

Puede ver las reglas listadas hasta el momento en la tabla.

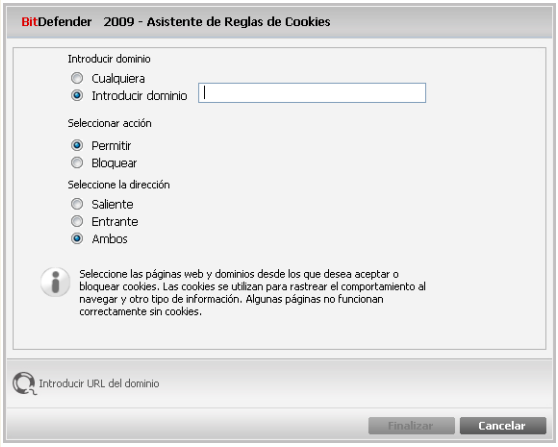
Importante
Las reglas se muestran por orden de prioridad, de mayor a menor prioridad. Puede arrastrar y soltar las reglas para modificar su orden de prioridad.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar los parámetros de la regla, haga doble clic en la regla y realice las modificaciones necesarias en la ventana de configuración.

Para añadir manualmente una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

18.4.1. Ventana de Configuración

Cuando edite una regla o al añadir una regla manualmente, aparecerá la ventana de configuración.



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 se aplicará sólo a las cookies enviadas a la página web indicada.
Entrante	La regla se aplicará sólo a las cookies recibidas desde la página web indicada.
Ambos	La regla se aplicará en ambas direcciones.

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 **Finalizar**.

18.5. 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.

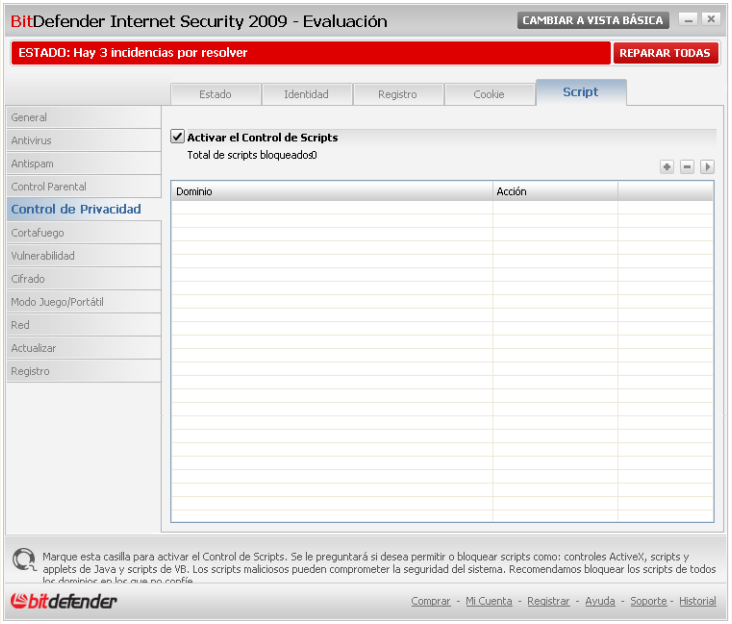
Con el **Control del Script** usted decide cuáles son las páginas web de confianza. BitDefender le pedirá una confirmación cada vez que una web intente activar un script u otro contenido activo:

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.

Para configurar el Control de Script, diríjase al apartado **Control de Privacidad > Script** en la Vista Avanzada.



Control de Scripts

Puede ver las reglas listadas hasta el momento en la tabla.

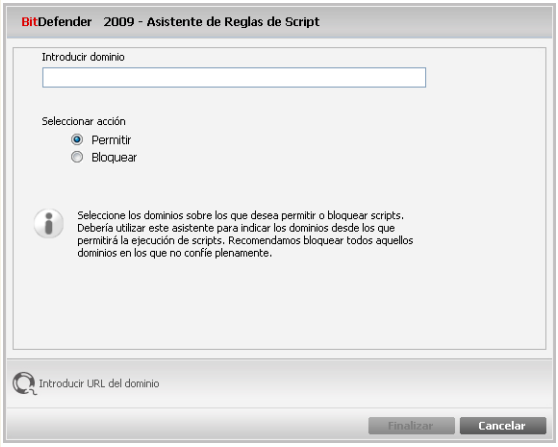
Importante
Las reglas se muestran por orden de prioridad, de mayor a menor prioridad. Puede arrastrar y soltar las reglas para modificar su orden de prioridad.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar los parámetros de la regla, haga doble clic en la regla y realice las modificaciones necesarias en la ventana de configuración.

Para añadir manualmente una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

18.5.1. Ventana de Configuración

Cuando edite una regla o al añadir una regla manualmente, aparecerá la ventana de configuración.



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**.

19. Cortafuego

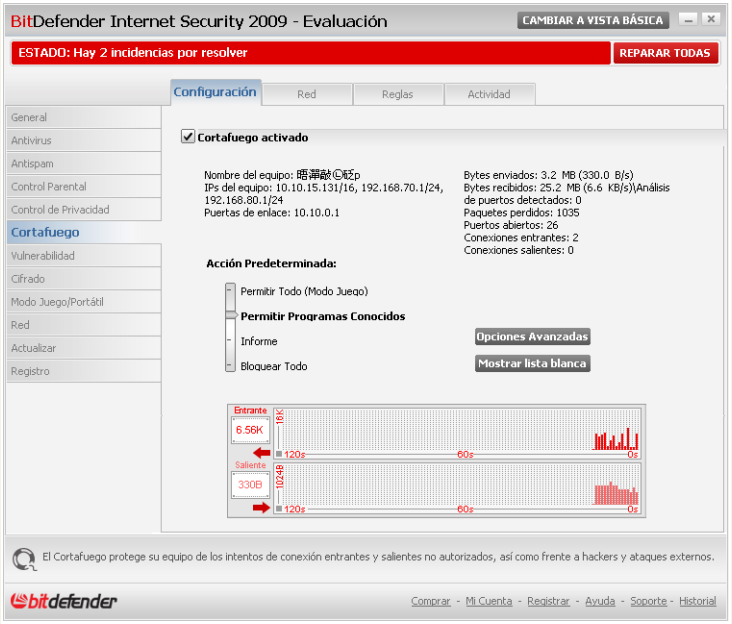
El Cortafuego protege su sistema de los intentos de conexión externos o internos no autorizados. Es algo parecido a tener un guardia en la puerta – vigilará su conexión a Internet y controlará todas las conexiones que decida autorizar o bloquear.

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).

19.1. Configuración

Para configurar la protección del Cortafuego, diríjase al apartado **Cortafuego > Configuración** en la Vista Avanzada.



Configuración del Cortafuego

Podrá ver si el Cortafuego está activado o desactivado. Si desea cambiar el estado del Cortafuego, marque o desmarque la casilla correspondiente.

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

Existen dos tipos de categorías de información:

- **Resumen de la Configuración de la Red.** Puede ver el nombre de su equipo, su dirección IP y la puerta de enlace predeterminada. Si dispone de más de un adaptador de red (es decir, si está conectado a más de una red), verá la dirección IP y puerta de enlace de cada uno de los adaptadores.
- **Estadísticas.** Puede ver varias estadísticas relacionadas con la actividad del Cortafuego:
  - número de bytes enviados.

- número de bytes recibidos.
- número de análisis de puertos detectados y bloqueados por BitDefender. Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers que buscan puertos abiertos en su equipo para intentar aprovecharse de ellos.
- número de paquetes perdidos.
- número de puertos abiertos.
- número de conexiones entrantes activas.
- número de conexiones salientes activas.

Para ver las conexiones activas y los puertos abiertos, diríjase a la pestaña Actividad.

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.

19.1.1. Estableciendo la Acción Predeterminada

Por defecto, BitDefender permite el acceso a Internet y a la red a todas los programas conocidos recopilados en su lista blanca. Para el resto de programas, BitDefender le preguntará la acción a realizar a través de una ventana de alerta. La acción indicada se aplicará siempre que la aplicación intente acceder a Internet o a la red.

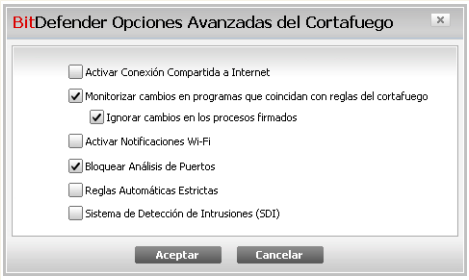
Arrastre el control deslizante a través de la escala para establecer la acción predeterminada que se realizará cuando una aplicación intente conectarse a la red/Internet. Dispone de las siguientes acciones:

Acción predeterminada	*Descripción*
Permitir todo	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 Programas Conocidos	Aplica las reglas existentes y permite que los programas reconocidos por BitDefender (en la lista blanca) puedan establecer conexiones salientes sin preguntarle. Para

Acción predeterminada	Descripción
	el resto de intentos de conexión, BitDefender solicitará su permiso. 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.
Informe	Aplica las reglas y le consulta sobre el tráfico que no coincide con ninguna de las reglas actuales.
Bloquear todo	Aplica las reglas existentes y bloquea todos los intentos de conexión que no coincidan con ninguna de las reglas existentes.

19.1.2. Modificando las Opciones Avanzadas del Cortafuego

Haga clic en **Avanzado** para modificar la configuración avanzada del Cortafuego.



Configuración Avanzada del Cortafuego

Dispone de las siguientes opciones:

- **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).

- **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** - si está conectado a una red Wi-Fi, se mostrarán ventanas con información sobre diferentes eventos de red (por ejemplo, cuando un equipo se conecta a la red).

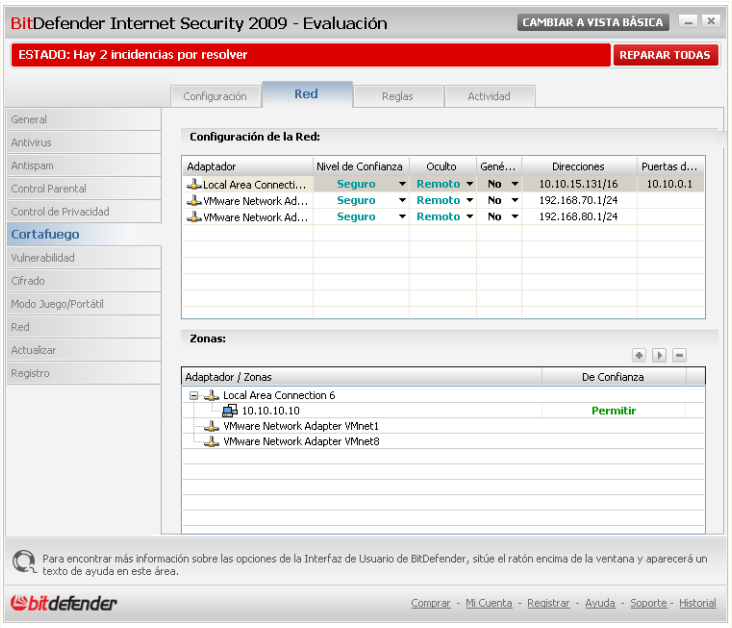
- **Bloquear Análisis de Puertos** - detecta y bloquea los ataques que intentan averiguar qué puertos tiene abiertos.

  Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers para averiguar los puertos abiertos en su equipo. Si encuentran un puerto vulnerable o inseguro, pueden intentar entrar en su equipo sin su autorización.

- **Reglas Automáticas Estrictas** - crea reglas estrictas a través de las alertas del Cortafuego. Con esta opción seleccionada, BitDefender le preguntará la acción a realizar y creará reglas para cada uno de los procesos que abran la aplicación que solicita el acceso a la red o Internet.
- **Sistema de Detección de Intrusiones (SDI)** - activa la monitorización heurística de las aplicaciones que intentan acceder a los servicios de la red o a Internet.

19.2. Red

Para modificar la configuración del Cortafuego, diríjase al apartado **Cortafuego > Red** en la Vista Avanzada.



Red

Las columnas de la tabla **Configuración de la Red** muestra información sobre las redes a las que está conectado:

- **Adaptador** - el adaptador de red que utiliza su equipo para conectarse a Internet.

- **Tipo** - el nivel de confianza asignado al adaptador de red. En función de la configuración del adaptador de red, BitDefender puede asignar automáticamente un nivel de confianza al adaptador o solicitarle más información.
- **Oculto** - indica si quiere que otros ordenadores detecten a su equipo o no.
- **Genérico** - indica si las reglas genéricas se aplican a esta conexión o no.
- **Direcciones** - la dirección IP configurada en el adaptador.
- **Puertas de Enlace** - la dirección IP que utiliza su equipo para disponer de conexión a Internet.

19.2.1. Cambiando el Nivel de Confianza

BitDefender asigna un nivel de confianza a cada adaptador de red. El nivel de confianza asignado al adaptador de red indica la fiabilidad de la red correspondiente.

A partir del nivel de confianza, se crean reglas específicas para el adaptador que indican cómo accederán a la red / Internet los procesos del sistema y BitDefender.

Puede ver el nivel de confianza configurado en cada adaptador en la tabla **Configuración de Red**, columna **Tipo**. Par cambiar el nivel de confianza, haga clic en la flecha de la columna **Tipo** y seleccione el nivel deseado.

Nivel de confianza	*Descripción*
Confianza Total	Desactiva el Cortafuego en el respectivo adaptador.
Confianza Local	Permite todo el tráfico entre su equipo y los equipos de la red local.
Seguro	Permite compartir recursos con los equipos de la red local. Este es el nivel que se establece automáticamente para las redes local (doméstica u oficina).
Inseguro	Impide que los equipos de la red o Internet se conecten a su equipo. Este es el nivel que se establece automáticamente para las redes públicas (si recibe una dirección IP desde un Proveedor de Servicios de Internet).
Bloqueo Local	Bloquea todo el tráfico entre su equipo y los equipos de la red local, aunque le ofrecerá acceso a Internet. Este es el nivel que se establece automáticamente para las redes Wi-Fi inseguras (abiertas).

Nivel de confianza	Descripción
Bloqueado	Bloquea por completo el tráfico de la red e Internet del adaptador de red correspondiente.

19.2.2. Configurando el Modo Oculto

El Modo Oculto hace que su ordenador sea invisible al software malintencionado y a los hackers de la red / Internet. Para configurar el Modo Oculto, haga clic en la flecha ▾ de la columna **Oculto** y seleccione la opción deseada.

Opciones del Modo Oculto	Descripción
Activado	El Modo Oculto está activado. Su equipo no será visible ni desde la red local ni desde Internet.
Desactivado	El Modo Oculto está desactivado. Cualquier usuario de la red local o Internet puede enviarle un ping y detectar su equipo.
Remoto	Su equipo no puede ser detectado desde Internet. Los usuarios de la red pueden enviarle pings y detectar su equipo.

19.2.3. Modificando la Configuración Genérica

Si la dirección IP del adaptador de red cambia, BitDefender modificará el nivel de confianza en consecuencia. Si desea mantener el mismo nivel de confianza, haga clic en la flecha ▾ de la columna **Genérico** y seleccione **Si**.

19.2.4. Zonas de Red

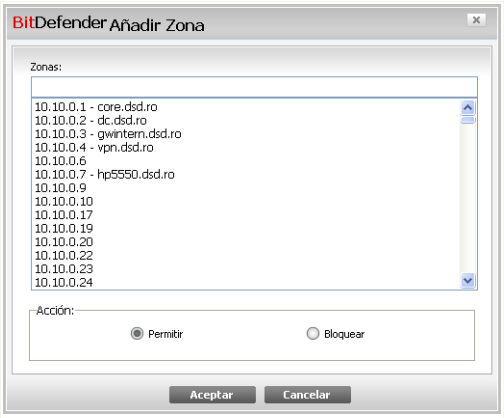
Puede añadir equipos de confianza o inseguros a un adaptador de red específico.

Una zona de confianza es un equipo en el que confía plenamente. Se permitirá todo el tráfico entre su equipo y el equipo de confianza. Para compartir recursos con algunos de los equipos que forman parte de una red Wi-Fi insegura, añádalos como equipos permitidos.

Una zona bloqueada es un equipo en el que no confía y con el que no desea comunicarse.

La tabla **Zonas** muestra las zonas de red existentes en cada adaptador.

Para añadir una zona, haga clic en el botón **Añadir** .



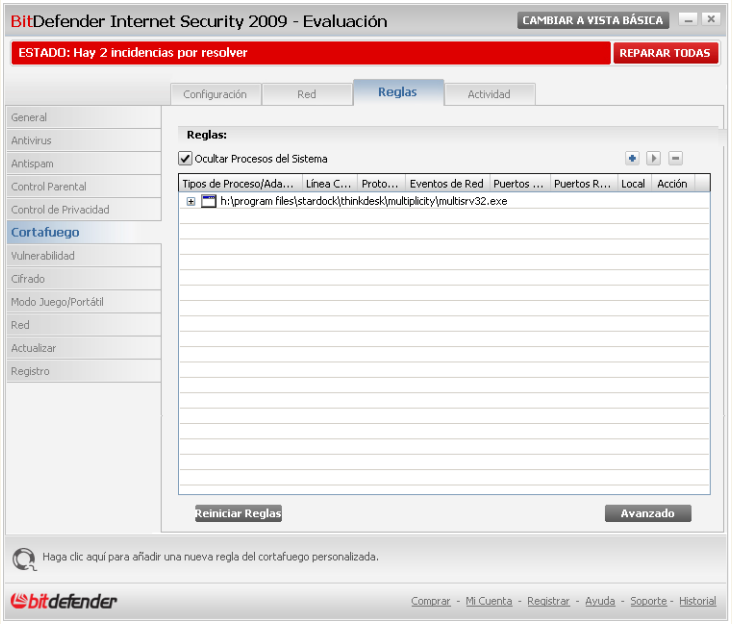
Añadir zona

Siga estos pasos:

1. Seleccione la dirección IP del equipo que desea añadir.
2. Seleccione la acción:
   - **Permitir** - para permitir todo el tráfico entre su equipo y el equipo seleccionado.
   - **Bloquear** - para bloquear todo el tráfico entre su equipo y el equipo seleccionado.
3. Haga clic en **Aceptar**.

19.3. Reglas

Para administrar las reglas del Cortafuego que controlan el acceso de las aplicaciones, diríjase al apartado **Cortafuego > Reglas** en la Vista Avanzada.



Reglas del Cortafuego

Puede ver las aplicaciones (procesos) para las cuales se han creado reglas del cortafuego. Desmarque la casilla **Ocultar procesos del sistema** para ver las reglas correspondientes a los proceso del sistema o BitDefender.

Para ver las reglas creadas para una aplicación específica, haga clic en la casilla + situada junto a la respectiva aplicación. Puede ver más información sobre cada regla a partir de las columnas de la tabla:

- **Tipos de Proceso/Adaptador** - los tipos de proceso y adaptador de red a los que se aplica la regla. Las reglas se crean automáticamente para filtrar el tráfico de la red / Internet a través de cualquier adaptador. Puede crear reglas manualmente o editar reglas existentes y así filtrar el acceso a la red/Internet de una aplicación en un adaptador de red específico (por ejemplo, un adaptador de red Wi-Fi).
- **Línea de Comando** - el comando utilizado para iniciar el proceso en la interfaz de línea de comandos de Windows (**cmd**).

- **Protocolo** - el protocolo IP sobre el que se aplica la regla. Puede ver uno de los siguientes:

Protocolo	Descripción
Cualquiera	Incluye todos los protocolos IP.
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.
Un número	Representa un protocolo IP específico (que no sea TCP ni UDP). Puede encontrar una lista completa de los números asignados a los protocolos IP en www.iana.org/assignments/protocol-numbers.

- **Eventos de Red** - los eventos de red a los que se aplica la regla. Puede producirse los siguientes eventos:

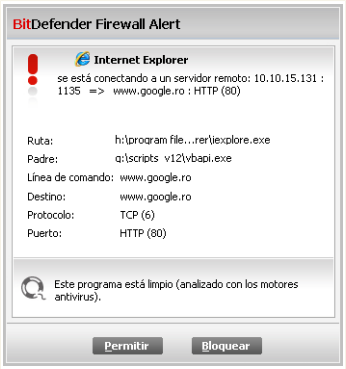
Evento	Descripción
Conectar	Intercambio preliminar de mensajes estándar usados por protocolos orientados a conexiones (como TCP) para establecer una conexión. En los protocolos orientados a conexiones, el tráfico de datos entre dos equipos sólo se produce después de establecer la conexión.
Tráfico	Flujo de datos entre dos equipos.
Escucha	Estado en el cual una aplicación monitoriza la red a la espera de establecer una conexión o de recibir información desde una aplicación igual.

- **Puertos Locales** - los puertos de su equipo sobre los que se aplica la regla.
- **Puertos Remotos** - los puertos del equipo remoto sobre los que se aplica la regla.
- **Local** - indica si la regla sólo se aplica a los equipos de la red local o no.

- **Acción** - indica si la aplicación tiene acceso o no a la red/Internet bajo las circunstancias especificadas.

19.3.1. 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.

19.3.2. Eliminando Reglas

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar Regla(s)**. Puede seleccionar y eliminar varias reglas a la vez.

Si desea eliminar todas las reglas creadas para una aplicación concreta, seleccione la aplicación en la lista y haga clic en el botón **Eliminar Regla(s)**.

19.3.3. Creando y Modificando Reglas

Crear nuevas reglas manualmente o modificar las existentes, consiste en configurar los parámetros de la regla en la ventana de configuración.

Creando reglas. Para crear una nueva regla manualmente, siga estos pasos:

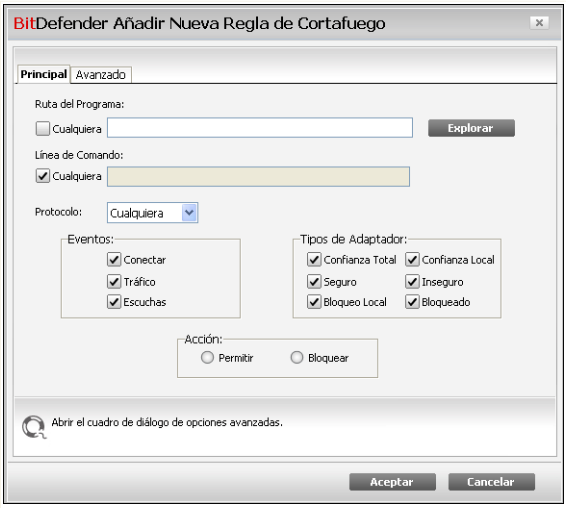
1. Haga clic en el botón **Añadir regla**. Aparecerá la ventana de configuración.
2. Configure los parámetros principales y avanzados según sus necesidades.
3. Haga clic en **Aceptar** para añadir la nueva regla.

Modificando las reglas. Para modificar una regla existente, siga estos pasos:

1. Haga clic en el botón **Editar regla** o haga doble clic en la regla. Aparecerá la ventana de configuración.
2. Configure los parámetros principales y avanzados según sus necesidades.
3. Haga clic en **Aplicar** para guardar los cambios.

Configurando los Parámetros Principales

La pestaña **Principal** de la ventana de configuración le permite configurar los parámetros básicos.



Parámetros Principales

Puede configurar los siguientes parámetros:

- **Ruta del Programa.** Haga clic en **Explorar** y seleccione la aplicación a la que quiere aplicar la regla. Si desea aplicar la regla a todas las aplicaciones, seleccione **Cualquiera**.
- **Línea de comando.** Si sólo desea aplicar la regla cuando la aplicación seleccionada se abra con un comando específico de la interfaz de línea de comandos de Windows, desmarque la casilla **Cualquiera** e introduzca el comando correspondiente en el campo de texto editable.
- **Protocolo.** En el menú, seleccione el protocolo IP sobre el que desea aplicar la regla.
  - Si desea aplicar la regla a todos los protocolos, seleccione la casilla **Cualquiera**.
  - Si sólo desea aplicar la regla a un protocolo concreto, seleccione la casilla **Otros**. Aparecerá un campo de texto editable. Introduzca el número asignado al protocolo que desea filtrar en el campo editable.

Nota

Los números de los protocolos IP están asignados por la Internet Assigned Numbers Authority (IANA). Puede encontrar una lista completa de los números asignados a los protocolos IP en www.iana.org/assignments/protocol-numbers.

- **Eventos.** Según el protocolo seleccionado, seleccione los eventos de la red a los que se aplica la regla. Puede producirse los siguientes eventos:

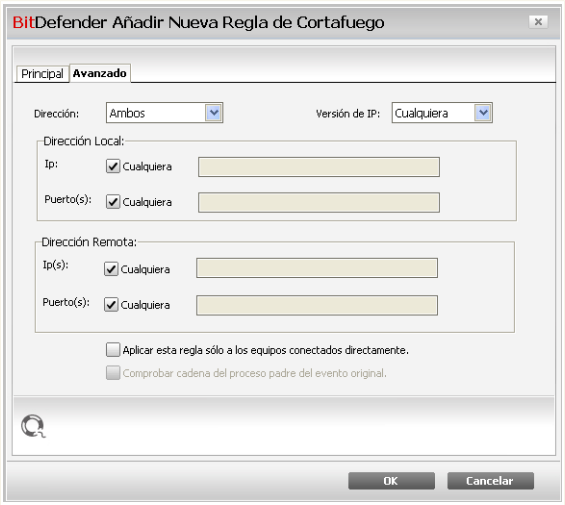
Evento	*Descripción*
Conectar	Intercambio preliminar de mensajes estándar usados por protocolos orientados a conexiones (como TCP) para establecer una conexión. En los protocolos orientados a conexiones, el tráfico de datos entre dos equipos sólo se produce después de establecer la conexión.
Tráfico	Flujo de datos entre dos equipos.
Escucha	Estado en el cual una aplicación monitoriza la red a la espera de establecer una conexión o de recibir información desde una aplicación igual.

- **Nivel de confianza.** Seleccione los niveles de confianza a los que se aplicará la regla.
- **Acción.** Seleccione una de las acciones disponibles:

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.

Configurando los Parámetros Avanzados

La pestaña **Avanzado** de la ventana de configuración le permite configurar los parámetros avanzados de la regla.



Parámetros Avanzados

Puede configurar los siguientes parámetros avanzados:

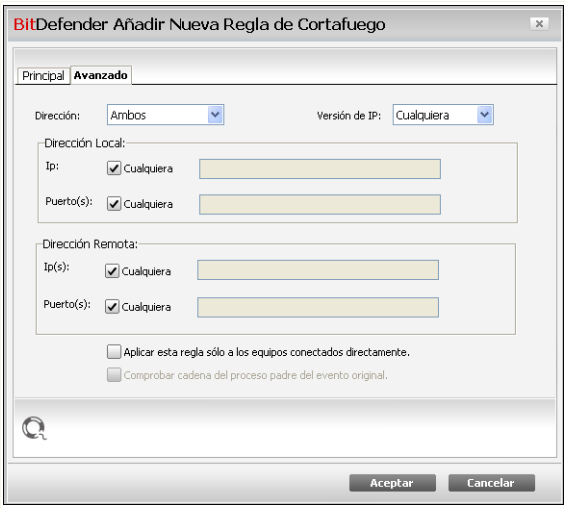
- **Dirección.** En el menú, seleccione la dirección del tráfico a la que se aplicará la regla.

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

- **Versión de IP.** En el menú, seleccione la versión de IP (IPv4, IPv6 o cualquiera) a la que se aplicará la regla.
- **Dirección Local.** Indique la dirección IP local y el puerto a los que se aplicará la regla, como se indica:
  - Si dispone de más de un adaptador de red, puede desmarcar la casilla **Cualquiera** e introduzca una dirección IP específica.
  - 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 Remota.** Indique la dirección IP remota y el puerto a los que se aplicará la regla, como se indica:
  - Para filtrar el tráfico entre su equipo y un equipo concreto, desmarque la casilla **Cualquiera** e introduzca una dirección IP específica.
  - 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**.
- **Aplicar esta regla sólo a los equipos conectados directamente.** Seleccione esta opción desea que la regla se aplique sólo a los intentos de tráfico local.
- **Comprobar cadena del proceso padre del evento original.** Sólo puede modificar esta parámetro si ha seleccionado la opción **Reglas Automáticas Estrictas** (diríjase a la pestaña Configuración y haga clic en **Opciones Avanzadas**). Las reglas estrictas harán que BitDefender le solicite la acción a realizar cada vez que el proceso padre de una aplicación que intenta acceder a la red/Internet sea diferente.

19.3.4. Configuración Avanzada de las Reglas

Si necesita un control avanzado sobre las reglas del Cortafuego, haga clic en **Avanzado**. Aparecerá una nueva ventana.



Configuración Avanzada de las Reglas

Puede ver las reglas del Cortafuego listadas para poder consultarlas. Las columnas de la tabla le proporcionan información sobre cada regla.

Nota

Cuando se produce un intento de conexión (tanto entrante como saliente), BitDefender aplica la acción de la primera regla que coincide con la respectiva conexión. Por lo tanto, es muy importante el orden con el que se comprueban la reglas.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar Regla(s)**.

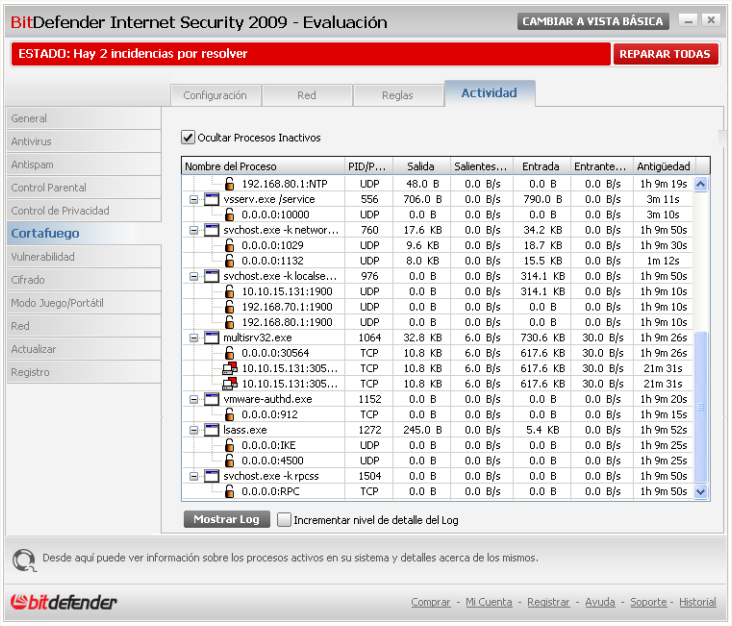
Para editar una regla existente, selecciónela y haga clic en el botón **Editar regla** o simplemente haga doble clic en la regla.

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**.

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

19.4. Control de Conexiones

Para monitorizar la actividad en la red / Internet (TCP o UDP) de las aplicaciones o para abrir el informe del Cortafuego, diríjase al apartado **Cortafuego > Actividad** en la Vista Avanzada.



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.

Si también quiere ver los procesos inactivos, desmarque la opción **Ocultar procesos inactivos**.

A continuación se indica el significado de los iconos:

- Indica una conexión abierta en su equipo.
- Indica un puerto abierto en su equipo.

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.

Para ver una lista completa de los eventos relacionados con el uso del módulo Cortafuego (activación/desactivación del cortafuego, bloqueo de tráfico, modificación de la configuración) o las actividades detectadas (análisis de puertos, bloqueo de intentos de conexión o tráfico según las reglas), puede consultar el log del Cortafuego de BitDefender haciendo clic en **Mostrar Log**. El archivo está ubicado en la carpeta Archivos Comunes del usuario en uso de Windows, en la ruta: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Si desea que el archivo log registre más información, marque la opción **Incrementar nivel de detalle del Log**.

20. Cifrado

BitDefender ofrece funciones de cifrado para proteger sus documentos confidenciales y las conversaciones de mensajería instantánea a través de Yahoo Messenger y MSN Messenger.

20.1. Cifrado de Mensajería Instantánea (IM)

Por defecto, BitDefender cifra todas sus sesiones de chat por mensajería instantánea siempre y cuando:

- Su contacto de chat tenga instalada una versión de BitDefender que soporte el Cifrado de IM, y esta función esté activada para la aplicación utilizada para conversar.
- Su contacto de chat utilice Yahoo Messenger o Windows Live (MSN) Messenger.

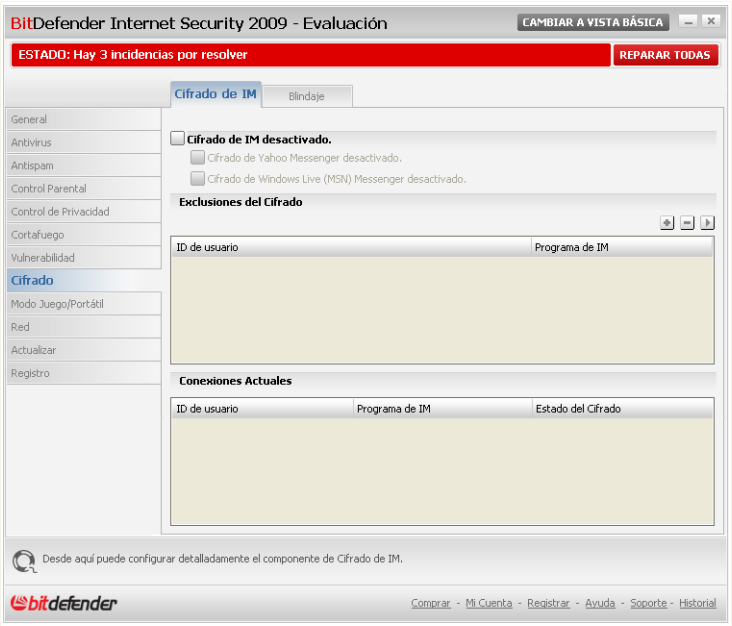
Importante

BitDefender no cifrará la conversación si su contacto utiliza una aplicación web para chatear, como Meebo, u otras aplicaciones que soportan Yahoo Messenger o MSN.

Para configurar el cifrado de la mensajería instantánea, diríjase al apartado **Cifrado > Cifrado de IM** en la Vista Avanzada.

Nota

Puede configurar fácilmente el cifrado de la mensajería instantánea usando la barra de herramientas de BitDefender en la ventana de chat. Para más información, por favor, consulte el capítulo "*Integración con Programas de Mensajería*" (p. 52) de esta guía.



Cifrado de la Mensajería Instantánea

Por defecto, el Cifrado de IM está activado tanto para Yahoo Messenger como para Windows Live (MSN) Messenger. Puede elegir entre desactivar el Cifrado de IM por completo, o sólo para alguna de las aplicaciones citadas.

Se mostrarán dos tablas:

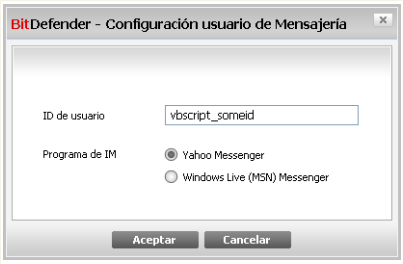
- **Exclusiones del Cifrado** - lista los IDs de usuario y el programa de mensajería asociado para el cual el cifrado está desactivado. Para eliminar un contacto de la lista, selecciónelo y haga clic en el botón **Quitar**.
- **Conexiones Actuales** - lista las conexiones de mensajería instantánea establecidas actualmente (ID de usuario y programa IM asociado) e indica si el cifrado está activado o no. Una conexión puede no cifrarse por alguna de las siguientes razones:
  - Ha desactivado explícitamente el cifrado para las conversaciones con el respectivo contacto.

- Su contacto no tiene instalada ninguna versión de BitDefender que soporte el cifrado de IM.

20.1.1. Desactivando el Cifrado para Usuarios Específicos

Para desactivar el cifrado de un contacto determinado, siga estos pasos:

1. Haga clic en el botón **Añadir** para abrir la ventana de configuración.



Añadiendo Contactos

2. Introduzca el ID de usuario de su contacto en el campo de texto editable.
3. Seleccione la aplicación de mensajería instantánea asociada a este contacto.
4. Haga clic en **Aceptar**.

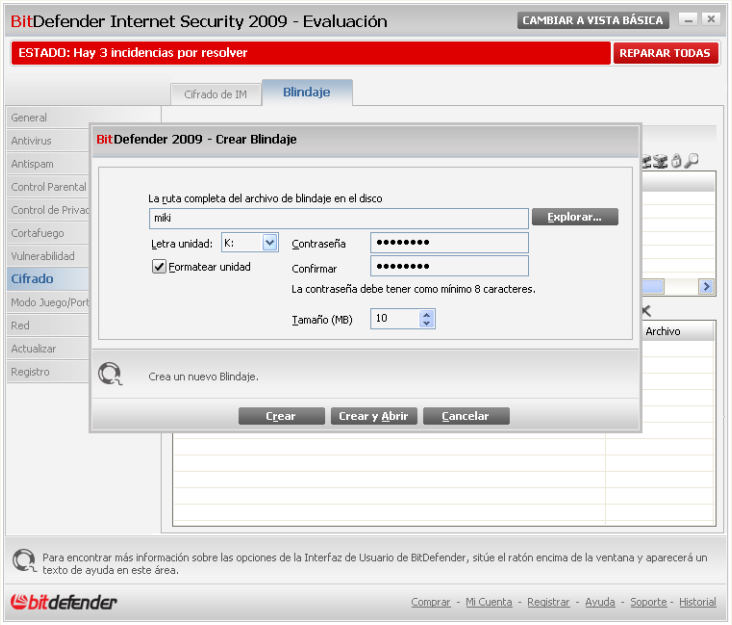
20.2. Blindaje de Archivos

El Blindaje de Archivos de BitDefender le permite crear unidades lógicas (o blindajes) cifrados y protegidos por contraseña en su equipo, en los que puede almacenar sus documentos confidenciales y sensibles. Sólo la persona que conozca la contraseña podrá acceder a los datos almacenados en los blindajes.

La contraseña le permite abrir el blindaje, almacenar datos en éste y cerrarlo, a la vez que asegura su protección. Cuando un blindaje está abierto, puede añadir nuevos archivos, abrir los archivos que contiene y modificarlos.

Físicamente, el blindaje es un archivo cifrado almacenado en su equipo cuya extensión es `bvd`. Aunque es posible acceder a los archivos físicos de las unidades blindadas desde diferentes sistemas operativos (como Linux), la información almacenada en los mismos no puede leerse al estar cifrada.

Para administrar los Blindajes de su equipo, diríjase al apartado **Cifrado > Blindaje** en la Vista Avanzada.



Blindaje de Archivos

Para desactivar el Blindaje de Archivos, desmarque la casilla **Blindaje de Archivos activado** y haga clic en **Si** para confirmar la acción. Si desactiva el Blindaje de Archivos, se bloquearán todos los blindajes existentes y no podrá acceder a los archivos que contienen.

La tabla de la parte superior muestra los blindajes de su equipo. Puede ver el nombre, el estado (abierto/bloqueado), la letra de la unidad y la ruta completa del blindaje. La tabla de la parte inferior muestra el contenido del blindaje seleccionado.

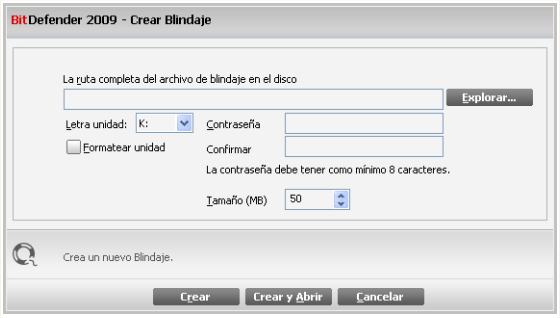
20.2.1. Creando un Blindaje

Para crear un nuevo blindaje, siga cualquiera de estos métodos:

- Haga clic en **Crear Blindaje**.

- Haga clic derecho en la tabla de blindajes y seleccione la opción **Crear**.
- Haga clic derecho en el Escritorio o en una carpeta de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de BitDefender** y seleccione **Crear**.

Aparecerá una nueva ventana.



Creación del Blindaje de Archivos

Siga estos pasos:

1. Indique la ubicación y el nombre del archivo de blindaje.
   - Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.
   - Introduzca la ruta completa del archivo de blindaje en el disco.
2. Seleccione la letra de la unidad en el menú. Al abrir un blindaje, en Mi PC aparecerá un nuevo disco virtual con la letra de unidad seleccionada.
3. Introduzca la contraseña del blindaje en el campo **Contraseña**. Cada vez que alguien que intente abrir el blindaje y acceder a sus archivos, deberá introducir la contraseña.
4. Seleccione la opción **Formatear unidad** para formatear la unidad virtual asignada al blindaje.
5. Si desea modificar el tamaño predeterminado del blindaje (50 MB), introduzca el valor deseado en el campo **Tamaño del Blindaje**.
6. Haga clic en **Crear** si sólo desea crear el Blindaje en la ubicación deseada. Para crear un blindaje y mostrarlo como una unidad de disco virtual en Mi PC, haga clic en **Crear y Abrir**.

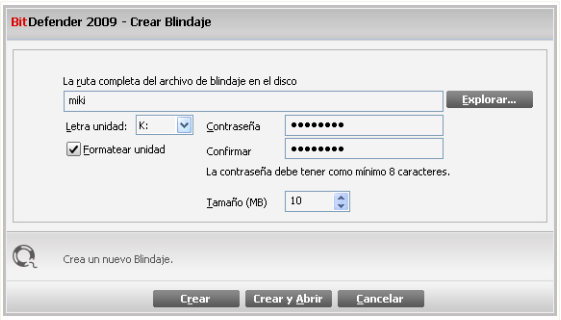
20.2.2. Abriendo un Blindaje

Para poder acceder y trabajar con los archivos almacenados en el Blindaje, antes debería abrirlo. Al abrir un Blindaje, aparecerá una unidad de disco virtual en Mi PC. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

Para abrir un blindaje, use cualquiera de estos métodos:

- Seleccione un blindaje de la lista y haga clic en **Abrir Blindaje**.
- Haga clic derecho en la tabla y seleccione la opción **Abrir**.
- Haga clic derecho en el archivo de blindaje de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de BitDefender** y seleccione **Abrir**.

Aparecerá una nueva ventana.



Abrir Blindaje de Archivos

Siga estos pasos:

1. Seleccione la letra de la unidad en el menú.
2. Introduzca la contraseña del blindaje en el campo **Contraseña**.
3. Haga clic en **Abrir**.

20.2.3. Bloqueando un Blindaje

Cuando acabe de trabajar con el blindaje de archivos, debería bloquearlo para proteger sus datos.

Para bloquear un blindaje, use cualquiera de estos métodos:

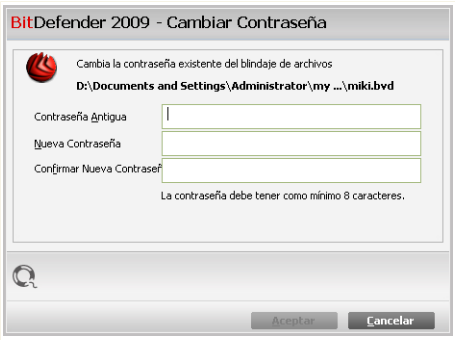
- Seleccione un blindaje de la tabla y haga clic en **Bloquear Blindaje**.
- Haga clic derecho en un blindaje de la tabla y seleccione **Bloquear**.
- Haga clic derecho en el archivo de blindaje de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de BitDefender** y seleccione **Bloquear**.
- Haga clic derecho en la unidad de disco virtual de Mi PC correspondiente al Blindaje, sitúe el cursor encima de la opción **Blindaje de Archivos de BitDefender** y seleccione **Bloquear**.

20.2.4. Cambiando la Contraseña del Blindaje

Para cambiar la contraseña del blindaje, use cualquiera de estos métodos:

- Seleccione un blindaje de la tabla y haga clic en **Cambiar contraseña**.
- Haga clic derecho en un blindaje de la tabla y seleccione la opción **Cambiar contraseña**.
- Haga clic derecho en el archivo de blindaje de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de BitDefender** y seleccione **Cambiar contraseña del blindaje**.

Aparecerá una nueva ventana.



Cambiar Contraseña del Blindaje

Siga estos pasos:

1. Introduzca la contraseña del blindaje existente en el campo **Contraseña Antigua**.

2. Introduzca la nueva contraseña del blindaje en los campos **Nueva Contraseña** y **Confirmar Nueva Contraseña**.

   Nota

   La contraseña debe contener 8 caracteres como mínimo. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

3. Haga clic en **Aceptar** para cambiar la contraseña.

20.2.5. Añadiendo Archivos a un Blindaje

Para añadir archivos a un blindaje, siga estos pasos:

1. Haga clic **Añadir archivo**. Aparecerá una nueva ventana.
2. Seleccione el archivo / carpeta que desea añadir al blindaje.
3. Haga clic en **Aceptar** para copiar los objetos seleccionados al blindaje.

Nota

No puede añadir archivos ni aplicaciones del sistema al blindaje.

20.2.6. Eliminando Archivos de un Blindaje

Para eliminar un archivo de un blindaje, siga estos pasos:

1. Seleccione el blindaje de la tabla que contiene el archivo a eliminar.
2. Seleccione el archivo a eliminar en la tabla que muestra el contenido del blindaje.
3. Haga clic en **Quitar archivo**.

Nota

Si el blindaje está abierto, puede eliminar directamente los archivos en la unidad de disco virtual asignada al blindaje.

21. Vulnerabilidad

Un requisito importante para la protección de su equipo frente a aplicaciones malintencionadas y atacantes, es mantener actualizado su sistema operativo y las aplicaciones que utiliza habitualmente. Además, para impedir el acceso físico no autorizado a su equipo, debería utilizar contraseñas seguras (que no puedan adivinarse fácilmente) en todas las cuentas de usuario de Windows.

BitDefender comprobará regularmente la existencia de vulnerabilidades en su sistema y le avisará en caso que existan incidencias.

21.1. Estado

Para configurar la Comprobación Automática de Vulnerabilidades, diríjase al apartado **Vulnerabilidad > Estado** en la Vista Avanzada.

Estado de Vulnerabilidad

Importante
Para recibir notificaciones automáticas sobre las vulnerabilidades de su sistema o aplicaciones, mantenga activada la **Comprobación Automática de Vulnerabilidades**.

21.1.1. Comprobando Vulnerabilidades

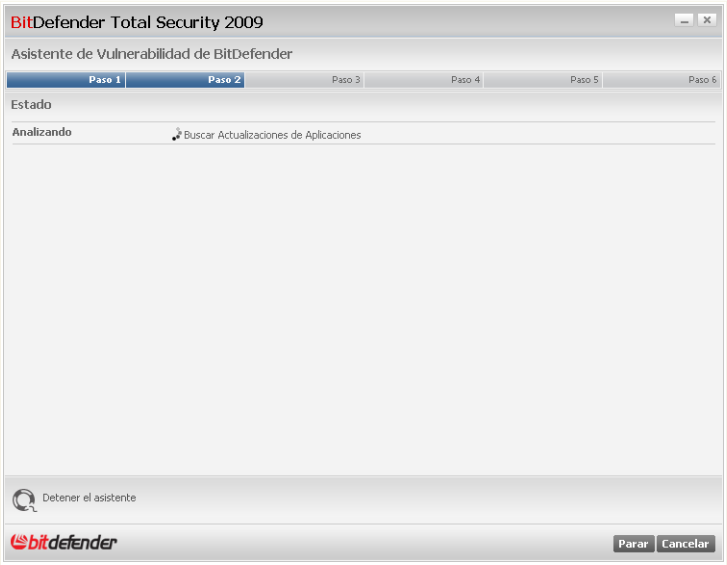
Para comprobar las vulnerabilidades de su equipo, haga clic en **Comprobar** y siga los pasos del Asistente.

Paso 1/6 – Seleccione las Vulnerabilidades a Comprobar

Vulnerabilidades

Haga clic en **Siguiente** para analizar su sistema en busca de las vulnerabilidades seleccionadas.

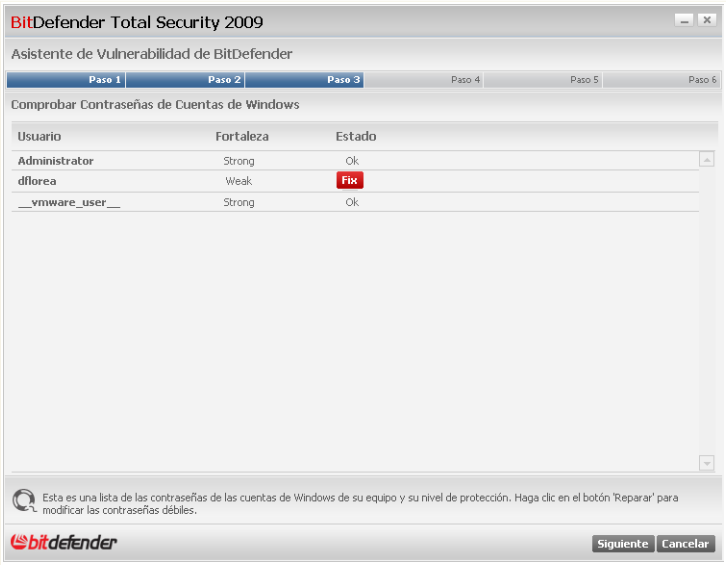
Paso 2/6 - Comprobando Vulnerabilidades



Comprobación de Vulnerabilidades

Espere hasta que BitDefender finalice la comprobación de vulnerabilidades.

Paso 3/6 - Cambie las Contraseñas Inseguras



Contraseñas de los Usuarios

Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo y el nivel de protección de sus contraseñas.

Haga clic en **Reparar** para modificar las contraseñas inseguras. Aparecerá una nueva ventana.

Cambiar Contraseña

Seleccione el método de reparación de esta incidencia:

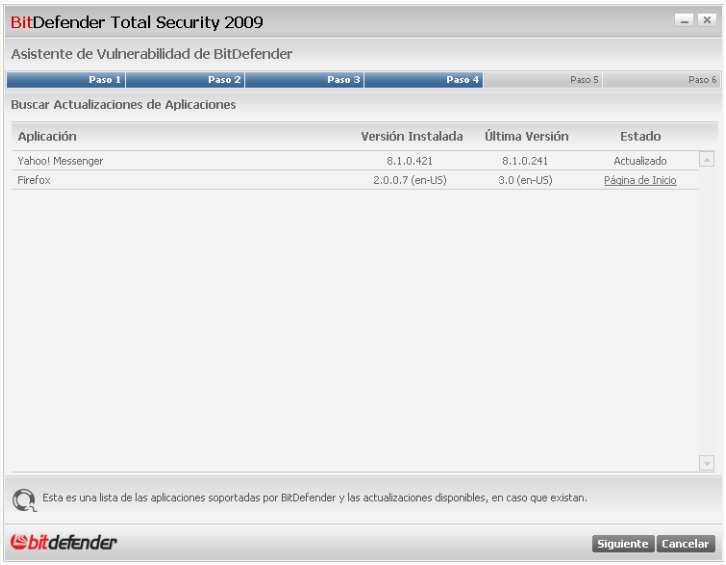
- **Forzar al usuario a cambiar la contraseña la próxima vez que inicie sesión.** BitDefender solicitará al usuario que cambie su contraseña la próxima vez que este usuario inicie sesión en Windows.
- **Cambiar contraseña del usuario.** Debe introducir la nueva contraseña en los campos de texto.

Nota
Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Haga clic en **Aceptar** para cambiar la contraseña.

Haga clic en **Siguiente**.

Paso 4/6 – Actualizar Aplicaciones



Aplicaciones

Puede ver la lista de todas las aplicaciones comprobadas por BitDefender y su estado de actualización. Si una aplicación no está actualizada, haga clic en el enlace indicado para descargar la nueva versión.

Haga clic en **Siguiente**.

Paso 4/6 – Actualizar Windows

Actualizaciones de Windows

Puede ver la lista de las actualizaciones críticas y no-críticas que actualmente no están instaladas en su equipo. Haga clic en **Instalar Todas las Actualizaciones del Sistema** para instalar todas las actualizaciones disponibles.

Haga clic en **Siguiente**.

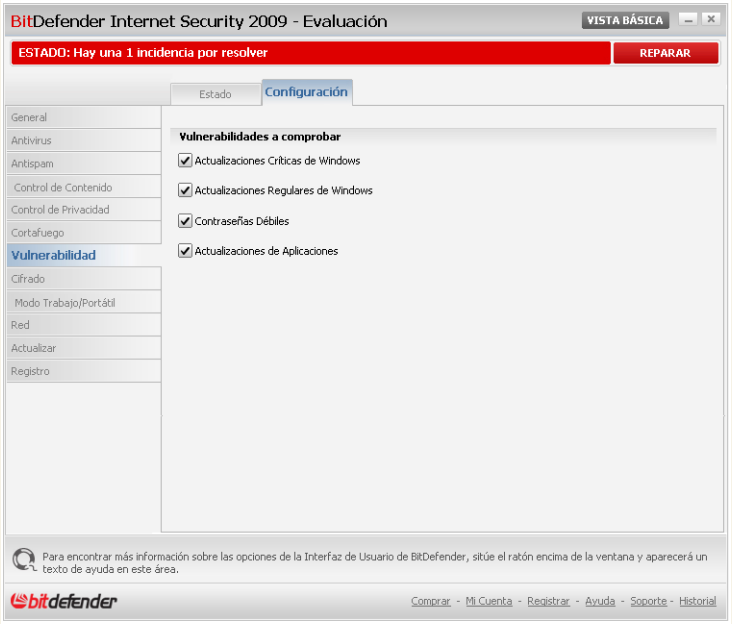
Paso 6/6 – Ver Resultados

Resultados

Haga clic en **Cerrar**.

21.2. Configuración

Para modificar la configuración de la Comprobación Automática de Vulnerabilidades, diríjase al apartado **Vulnerabilidad > Configuración** en la Vista Avanzada.



Configuración de la Comprobación Automática de Vulnerabilidades

Marque las casillas correspondientes a las vulnerabilidades del sistema que desee comprobar con regularidad.

- **Actualizaciones Críticas de Windows**
- **Actualizaciones Regulares de Windows**
- **Contraseñas Débiles**
- **Actualizaciones de Aplicaciones**

Nota
Si desmarca la casilla correspondiente a una vulnerabilidad específica, BitDefender dejará de informarle sobre las incidencias relacionadas con la ésta.

22. Modo Trabajo / Portátil

Los Modos Trabajo / Portátil le permiten configurar modos especiales de funcionamiento de BitDefender:

- El Modo Trabajo modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
- El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.

22.1. Modo Trabajo

El Modo Trabajo modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento 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 **Permitir Todo**. Esto significa que todas las conexiones nuevas (tanto entrantes como salientes) se aceptarán de forma automática, independientemente del puerto y protocolo que utilicen.
- Por defecto, no se realizarán actualizaciones.

Nota
Para modificar esta opción, diríjase al apartado Actualización > Configuración y desmarque la casilla **No actualizar si el Modo Trabajo está activado**.

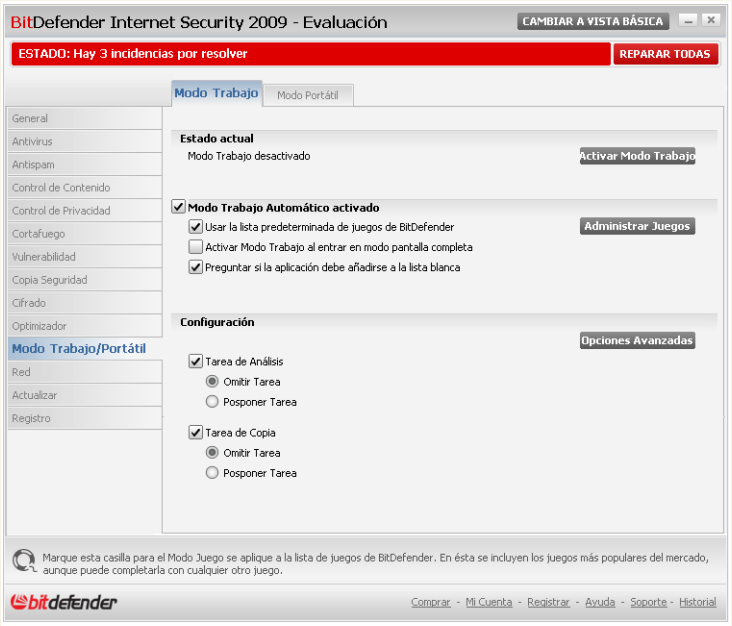
- Las tareas de análisis programadas se desactivarán de forma predeterminada.

Por defecto, BitDefender activa automáticamente el Modo Trabajo al iniciar un juego que se encuentra en la lista de juegos de BitDefender, o al ejecutar una aplicación en modo pantalla completa. Puede activar manualmente el Modo Trabajo usando la combinación de teclas predeterminada, `Ctrl+Alt+Shift+G`. Es sumamente recomendable desactivar el Modo Trabajo cuando acabe de jugar (puede utilizar la misma combinación de teclas, `Ctrl+Alt+Shift+G`).

Nota

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

Para configurar el Modo Trabajo, diríjase al apartado **Modo Trabajo/Portátil > Modo Trabajo** en la Vista Avanzada.



Modo Trabajo

En la parte superior de este apartado puede ver el estado del Modo Trabajo: Haga clic en **Activar Modo Trabajo** o **Salir del Modo Trabajo** para cambiar el estado.

22.1.1. Configurando el Modo Trabajo Automático

El Modo Trabajo Automático permite que BitDefender active automáticamente el Modo Trabajo cuando se detecte un juego. Puede configurar las siguientes opciones:

- **Usar la lista predeterminada de juegos de BitDefender** - para activar automáticamente el Modo Trabajo cuando inicie un juego de la lista de juegos

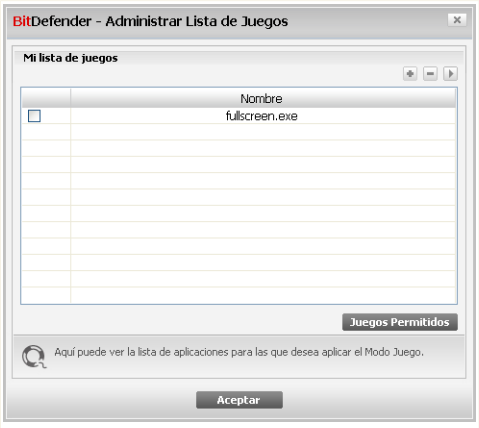
reconocidos por BitDefender. Para ver esta lista, haga clic en **Administrar Juegos** y a continuación haga clic en **Juegos Permitidos**.

- **Activar Modo Trabajo al entrar en modo pantalla completa** - para activar automáticamente el Modo Trabajo cuando inicie una aplicación en modo pantalla completa.
- **¿Añadir la aplicación a la lista de juego?** - para preguntar si desea añadir la nueva aplicación a la lista de juegos cuando salga del modo pantalla completa. Al añadir una nueva aplicación a la lista de juegos, BitDefender activará automáticamente el Modo Trabajo la próxima vez que la inicie.

Nota
Si no desea que BitDefender active automáticamente el Modo Trabajo, desmarque la casilla **Modo Trabajo Automático**.

22.1.2. Administrando la Lista de Juegos

BitDefender activará automáticamente el Modo Trabajo cuando inicie una aplicación de la lista de juegos. Para ver y gestionar la lista de juegos, haga clic en **Administrar Juegos**. Aparecerá una nueva ventana.



Lista de Juegos

Se añadirán automáticamente nuevas aplicaciones a la lista cuando:

- Cuando inicie un juego de la lista de juegos reconocidos por BitDefender. Para ver esta lista, haga clic en **Juegos Permitidos**.
- Cuando salga del modo pantalla completa, añada la aplicación a la lista de juegos desde la ventana de aviso.

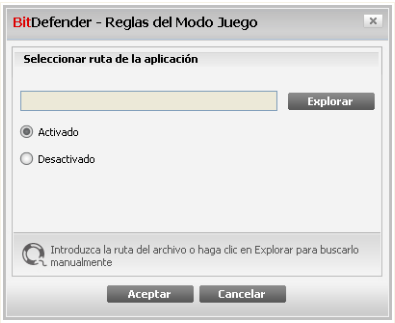
Si desea desactivar el Modo Trabajo Automático para una aplicación concreta de la lista, desmarque su casilla correspondiente. Debe desactivar el Modo Trabajo Automático para aquellas aplicaciones de uso habitual que utilizan el modo pantalla completa, como navegadores web o reproductores de vídeos y películas.

Para administrar la lista de juegos, puede utilizar los botones situados en la parte superior de la tabla:

- **Add** - add a new application to the game list.
- **Remove** - remove an application from the game list.
- **Edit** - edit an existing entry in the game list.

Añadiendo o Editando Juegos

Cuando añada o edite una entrada de la lista de juegos, aparecerá la siguiente ventana:



Añadir Juego

Haga clic en **Explorar** para seleccionar la aplicación deseada, o introduzca la ruta de la aplicación en el campo de texto editable.

Si no desea activar automáticamente el Modo Trabajo al iniciar la aplicación seleccionada, seleccione **Desactivar**.

Haga clic en **Aceptar** para añadir la entrada a la lista de juegos.

22.1.3. Modificando la Configuración del Modo Trabajo

Para modificar el comportamiento de las tareas programadas, utilice las siguientes opciones:

- **Tarea de Análisis** - para impedir que las tareas de análisis programadas se ejecuten mientras el Modo Trabajo está activado. Puede seleccionar una de de las siguientes opciones:

Opción	Descripción
Omitir Tarea	Para no iniciar la tarea programada.
Posponer Tarea	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Trabajo.

Para desactivar automáticamente el Cortafuego cuando el Modo Trabajo esté activado, siga estos pasos:

1. Haga clic en **Opciones Avanzadas**. Aparecerá una nueva ventana.
2. Marque la casilla **No usar cortafuego**.
3. Haga clic en **Aplicar** para guardar los cambios.

22.1.4. Cambiando el Atajo de Teclado del Modo Trabajo

Puede activar manualmente el Modo Trabajo usando la combinación de teclas predeterminada, `Ctrl+Alt+Shift+G`. Si desea cambiar el atajo de teclado, siga estos pasos:

1. Haga clic en **Opciones Avanzadas**. Aparecerá una nueva ventana.

Opciones Avanzadas

2. Debajo de la opción **Usar Atajos de Teclado**, configure la combinación de teclas deseada:
   - Elija las teclas que desea utilizar seleccionado alguna de las siguientes: 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`.
3. Haga clic en **Aplicar** para guardar los cambios.

Nota
Si desmarca la casilla correspondiente a **Usar Atajos de Teclado**, desactivará las combinaciones de teclas.

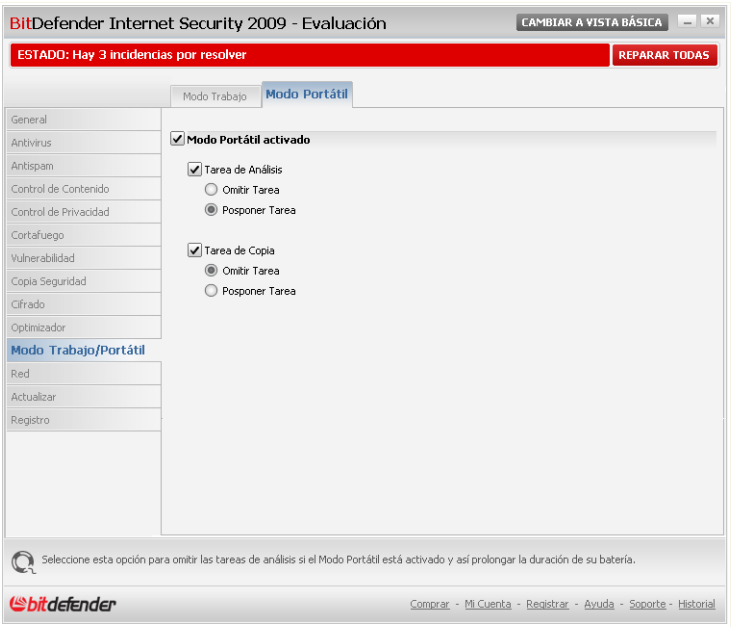
22.2. Modo Portátil

El Modo Portátil está diseñado especialmente para los usuarios de ordenadores portátiles. Su objetivo es minimizar el impacto de BitDefender sobre el consumo de energía mientras estos dispositivos funcionan con batería.

Cuando el Modo Portátil esté activado, por defecto, las tareas programadas no se realizarán.

BitDefender detecta cuando su portátil hace uso de la batería y activa automáticamente el Modo Portátil. Asimismo, BitDefender desactivará automáticamente el Modo Portátil cuando detecte que el portátil ha dejado de funcionar con batería.

Para configurar el Modo Portátil, diríjase al apartado **Modo Trabajo/Portátil > Modo Portátil** en la Vista Avanzada.



Modo Portátil

Podrá ver si el Modo Portátil está activado o no. Si el Modo Portátil está activado, BitDefender aplicará la configuración definida mientras el equipo funcione con batería.

22.2.1. Configurando las Opciones del Modo Portátil

Para modificar el comportamiento de las tareas programadas, utilice las siguientes opciones:

- **Tarea de Análisis** - para impedir que las tareas de análisis programadas se ejecuten mientras el Modo Portátil está activado. Puede seleccionar una de de las siguientes opciones:

Opción	Descripción
Omitir Tarea	Para no iniciar la tarea programada.
Posponer Tarea	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Portátil.

23. Red

El módulo Red le permite administrar los productos BitDefender instalados en los equipos de una pequeña red desde un único equipo.

Mapa de la Red

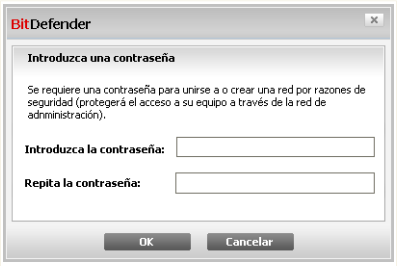
Para poder administrar los productos BitDefender de los otros equipos de la pequeña red, debe seguir estos pasos:

1. Únase a la red de administración de BitDefender desde su equipo. Unirse a una red consiste en establecer una contraseña de administración para gestionar la red de administración.
2. Diríjase a cada unos de los equipos que desee administrar remotamente y únalos a la red (defina una contraseña).
3. Vuelva a su equipo y añada los equipos que desee administrar.

23.1. Unirse a la Red de BitDefender

Para unirse a la red de administración de BitDefender, siga estos pasos:

1. Haga clic en **Unirse a/Crear Red**. Se le solicitará configurar la contraseña de administración de red.



Configurar Contraseña

2. Introduzca la misma contraseña en cada uno de los campos de texto.
3. Haga clic en **Aceptar**.

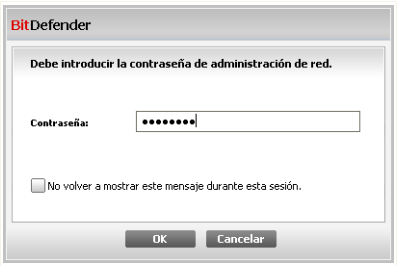
Podrá ver como el nombre del equipo aparece en el mapa de la red.

23.2. Añadiendo Equipos a la Red de BitDefender

Antes de añadir un equipo a la red de administración de BitDefender, debe configurar la contraseña de administración de red en el equipo correspondiente.

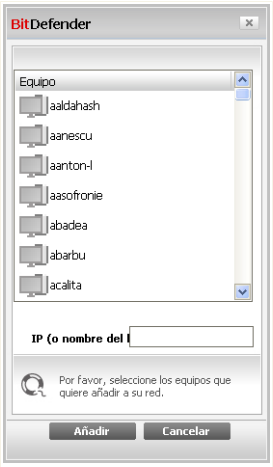
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

1. Haga clic en **Administración de Red**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**. Aparecerá una nueva ventana.



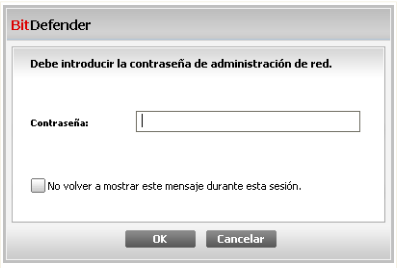
Añadir Equipo

Podrá ver la lista de los equipos de la red. A continuación se explica el significado de los iconos:

- Indica un equipo conectado con ningún producto BitDefender instalado.
- Indica un equipo conectado con BitDefender instalado.

- Indica un equipo desconectado con BitDefender instalado.

3. Realice una de estas acciones:
   - Seleccione un equipo de la lista para añadirlo.
   - Introduzca la dirección IP o el nombre del equipo a añadir en el campo editable correspondiente.
4. Haga clic en **Añadir**. Se le solicitará la contraseña de administración de red del equipo correspondiente.



Autentificar

5. Introduzca la contraseña de administración de red configurada en el equipo correspondiente.
6. Haga clic en **Aceptar**. Si ha introducido la contraseña correcta, el nombre del equipo seleccionado aparecerá en el mapa de la red.

Nota
Puede añadir hasta cinco equipos en el mapa de la red.

23.3. Administrando la Red de BitDefender

Una vez haya creado con éxito una red de administración de BitDefender, podrá gestionar todos los productos BitDefender desde un único equipo.

Mapa de la Red

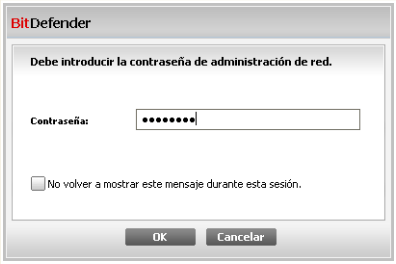
Si sitúa el cursor del ratón encima de un equipo del mapa de la red, podrá ver información sobre el equipo (nombre, dirección IP, número de incidencias que afectan a la seguridad del sistema y estado de registro de BitDefender).

Si hace clic derecho en el nombre de un equipo del mapa de la red, podrá ver todas las tareas de administración que puede ejecutar remotamente.

- **Registrar este equipo**
- **Establecer contraseña de configuración**
- **Ejecutar una tarea de Análisis**
- **Reparar incidencias de este equipo**
- **Ver historial de este equipo**
- **Iniciar una Actualización en este equipo**
- **Aplicar Perfil**

- **Iniciar una tarea de Optimizador en este equipo**
- **Establecer como Servidor de Actualizaciones de esta Red**

Antes de ejecutar una tarea en un equipo determinado, se le solicitará la contraseña de administración de red local.



Introducir Contraseña

Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**.

Nota

Si tiene previsto ejecutar varias tareas, puede interesarle la opción **No volver a mostrar este mensaje durante esta sesión**. Al seleccionar esta opción, no se le volverá a solicitar esta contraseña durante la actual sesión.

24. 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.

Al detectar una actualización, se le puede solicitar su confirmación para realizar la actualización o puede realizarse de forma automática, según lo que haya definido en la Configuración de la actualización automática.

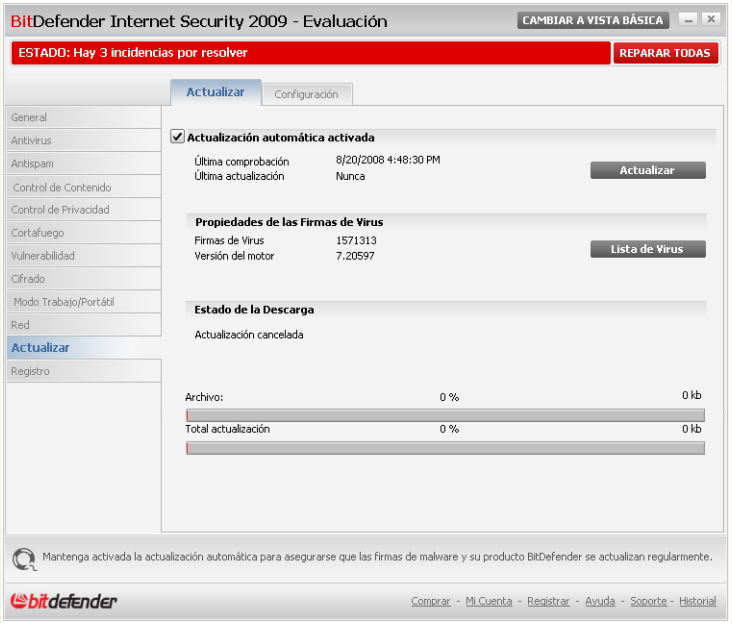
El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afecta al rendimiento del producto a la vez que se evita cualquier riesgo.

Las actualizciones se presentan de las siguientes maneras:

- **Actualización de los motores antivirus** - a medida que se detecten nuevas amenazas, los archivos 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**.

24.1. Actualización automática

Para ver la información relacionada con las actualizaciones, diríjase al apartado **Actualización > Actualizar** en la Vista Avanzada.



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.

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.

Puede ver las firmas de malware de BitDefender haciendo clic en **Lista de Virus**. Se abrirá un documento HTML con la lista de firmas disponibles en su navegador web. Puede buscar la firma para una amenaza en concreto, o hacer clic en **BitDefender Virus List** para ir a la base de datos online de BitDefender.

24.1.1. Solicitando una Actualización

Puede realizar una actualización automática en cualquier momento haciendo clic en **Actualizar**. Este tipo de actualización también se conoce como **Actualización por petición del usuario**.

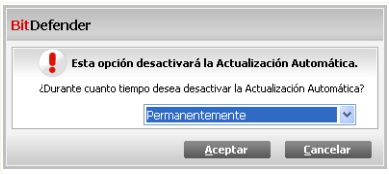
El módulo **Actualizar** se conectará al servidor de actualizaciones de BitDefender y comprobará si hay alguna actualización disponible. Si se detecta una actualización, según las opciones elegidas en el apartado de Configuración de la Actualización Manual se le pedirá que confirme la actualización o 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.

24.1.2. 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.

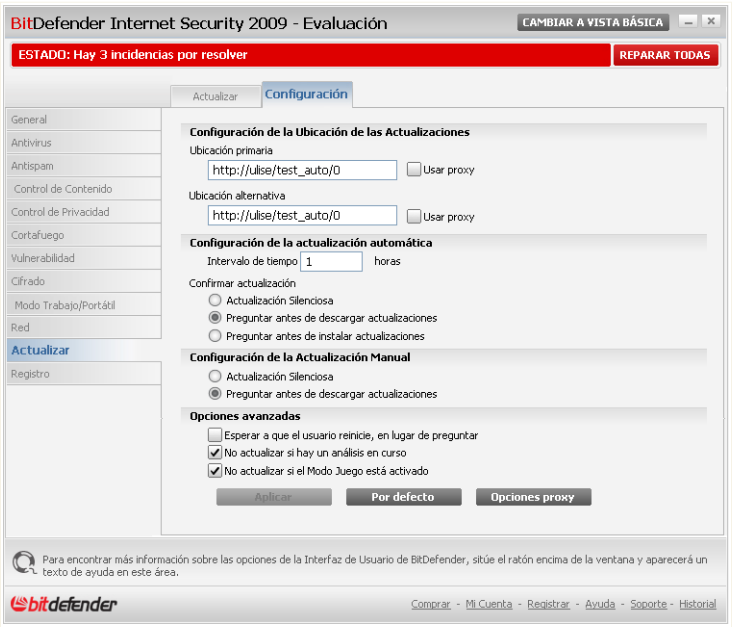
Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Mientras la

protección esté desactivada, no tendrá protección contra las amenazas de malware más recientes.

24.2. 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 **Actualización > Configuración** en la Vista Avanzada.



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.

24.2.1. 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. Para más información, por favor, consulte el apartado "*Administrando los Proxies*" (p. 298).

24.2.2. 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.
- **Preguntar antes de instalar actualizaciones** - cada vez que se haya descargado una actualización, se le pedirá permiso para instalarla.

24.2.3. 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.

24.2.4. 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.

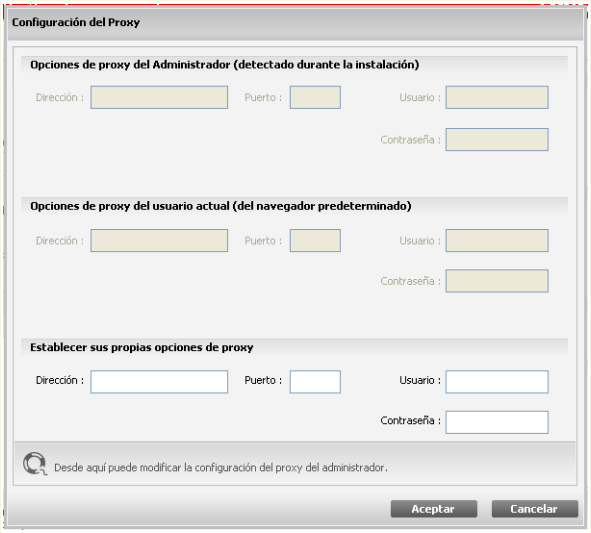
- **No actualizar si el Modo Trabajo está activado** - BitDefender no se actualizará mientras el Modo Trabajo esté activado. De esta manera podrá minimizar el impacto del producto en el rendimiento del sistema mientras juega.

24.2.5. 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** - escriba un nombre de usuario que el proxy reconozca.
  - **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.

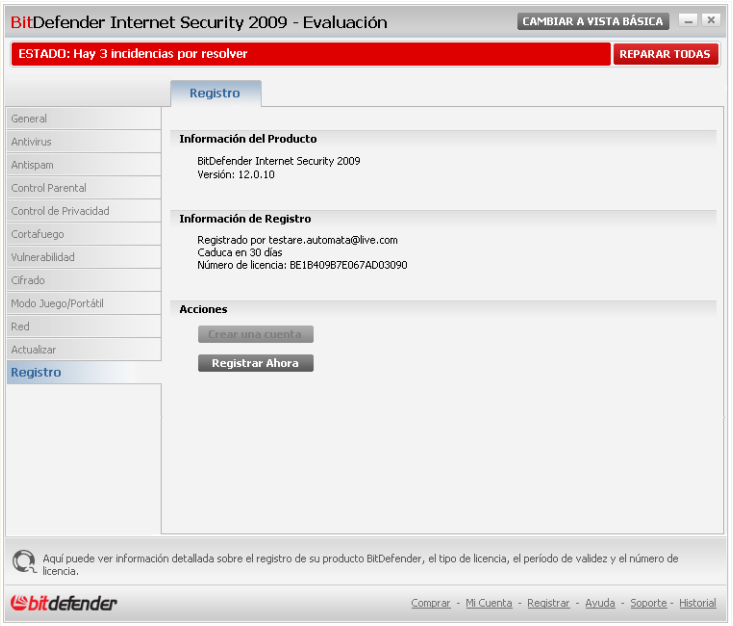
En primer lugar se prueba su propia configuración para conectarse a Internet. Si no funciona, se probará la configuración detectada durante la instalación. Finalmente, si tampoco funciona, se importará la configuración desde el navegador predeterminado para intentar conectarse.

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.

25. Registro

Para encontrar más información sobre su producto BitDefender y el estado del registro, diríjase al apartado **Registro** en la Vista Avanzada.



Registro

Esta sección muestra:

- **Información del Producto**: el producto BitDefender product y la versión.
- **Información del Registro**: la dirección de correo utilizada para iniciar sesión con su Cuenta de BitDefender (si está configurada), la licencia actual y lo días restantes hasta que caduque la licencia.

25.1. Registrando BitDefender Internet Security 2009

Haga clic en **Registrar** para abrir la ventana de registro del producto.

Registro

Puede ver el estado del registro de BitDefender, el número de licencia actual y los días restantes hasta la fecha de caducidad de la licencia.

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

Para registrar BitDefender Internet Security 2009:

1. Seleccione la opción **Quiero registrar el producto con un nuevo número de licencia**.
2. Introduzca el número de licencia en el campo editable.

Nota

Puede encontrar su número de licencia en:

- la etiqueta del CD.
- la tarjeta de licencia del producto.
- el mensaje de confirmación de compra online.

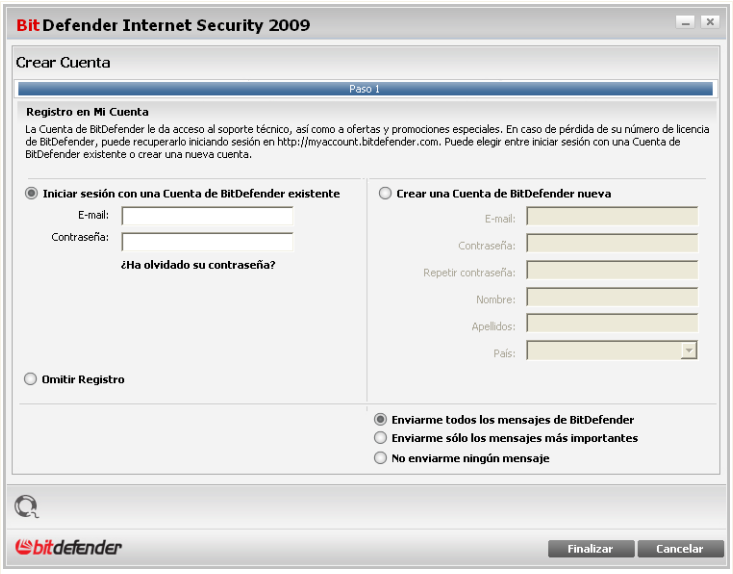
Si no dispone de ningún número de licencia de BitDefender, haga clic en el enlace indicado para dirigirse a la tienda online de BitDefender y adquirir una.

Haga clic en **Finalizar**.

25.2. Creando una Cuenta de BitDefender

La cuenta de BitDefender da acceso al soporte técnico gratuito, ofertas especiales y promociones. En caso de pérdida del número de licencia, puede recuperarlo iniciando sesión en http://myaccount.bitdefender.com.

Si todavía no ha creado una cuenta de BitDefender, haga clic en **Crear una cuenta** para abrir la ventana de registro de cuenta.



Creación de la Cuenta

Si no desea crear ninguna cuenta de BitDefender por el momento, haga clic en **Omitir Registro** y a continuación haga clic en **Finalizar**. De lo contrario, siga los pasos indicados según su situación actual:

- “No tengo una cuenta de BitDefender” (p. 304)
- “Ya tengo una cuenta de BitDefender” (p. 305)

No tengo una cuenta de BitDefender

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. La contraseña debe contener 6 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 que aparecen en el mensaje enviado por el servicio de registro de BitDefender.

Opcionalmente, BitDefender puede informarle sobre ofertas especiales y promociones a través de la dirección de correo de su cuenta. Seleccione una de las opciones disponibles:

- **Enviarme todos los mensajes de BitDefender**
- **Enviarme sólo los mensajes importantes**
- **No enviarme ningún mensaje**

Haga clic en **Finalizar**.

Ya tengo una cuenta de BitDefender

BitDefender detectará automáticamente si previamente ha registrado una cuenta de BitDefender en su equipo. En este caso, introduzca la contraseña de su cuenta.

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.

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

Opcionalmente, BitDefender puede informarle sobre ofertas especiales y promociones a través de la dirección de correo de su cuenta. Seleccione una de las opciones disponibles:

- **Enviarme todos los mensajes de BitDefender**
- **Enviarme sólo los mensajes importantes**
- **No enviarme ningún mensaje**

Haga clic en **Finalizar**.

Conseguir Ayuda

26. 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 electrónico 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.

26.1. 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.

26.2. Solicitando Ayuda

26.2.1. 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/

Alemán

http://www.bitdefender.com/de/KnowledgeBase/

Francés

http://www.bitdefender.com/fr/KnowledgeBase/

Rumano

http://www.bitdefender.com/ro/KnowledgeBase/

Español

http://www.bitdefender.com/es/KnowledgeBase/

26.2.2. 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/

26.3. 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.

26.3.1. 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

26.3.2. 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
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Tel: 1-954-776-6262
Web: http://www.bitdefender.com

Soporte Técnico (Sólo para Usuarios Registrados):
- E-mail: support@bitdefender.com
- Tel (Llamada Gratuita):

- Estados Unidos: 1-888-868-1873
- Canadá: 1-866-947-1873

Servicio de Atención al Cliente (Sólo para Usuarios Registrados):

- E-mail: customerservice@bitdefender.com
- Tel (Llamada Gratuita):
  - Estados Unidos: 1-888-868-1873
  - Canadá: 1-866-947-1873

Alemania

BitDefender GmbH
Headquarter Europa Occidental
Saarlandstrasse 84
44139 Dortmund
Alemania
Tel: +49 (0)231 99 33 98 0
Email: info@bitdefender.com
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.com
Soporte Técnico: support@bitdefender.com

Reino Unido e Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Tel: +44(0)1782664865
Email: info@bitdefender.com
Comercial: sales@bitdefender.com
Web: http://www.bitdefender.co.uk
Soporte técnico: soporte@bitdefender.es

España

BitDefender España, S.L
C/ Balmes 191, 2ª planta, 08006
Barcelona
Soporte Técnico: soporte@bitdefender.es
Comercial: comercial@bitdefender.es

Tel: +34 932189615
Fax: +34 932179128
Web: http://www.bitdefender.es

Rumania

BITDEFENDER
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Soporte técnico: soporte@bitdefender.es
Comercial: sales@bitdefender.com
Tel: +40 21 3001255
Tel: +40 21 3001254
Página del producto: http://www.bitdefender.es

CD de Rescate de BitDefender

27. General

BitDefender Internet Security 2009 se entrega en un CD de autoarranque (CD de Rescate de BitDefender), capaz de analizar y desinfectar todos los discos duros del equipo, antes de iniciar 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/

27.1. 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.

27.2. 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
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 Wi-Fi.

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 .

28. Cómo 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.

28.1. 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.

Nota
Seleccione el idioma que desea utilizar para el CD de Rescate en la lista de idiomas disponibles.

Ventana de inicio de Boot

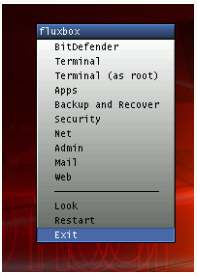
Durante la carga del sistema, se actualizan las firmas de virus automáticamente. Esta operación puede tardar unos minutos.

Una vez finalizado el inicio del CD, podrá ver el Escritorio y utilizar el CD de Rescate de BitDefender.

El Escritorio

28.2. Detener el CD de Rescate de BitDefender

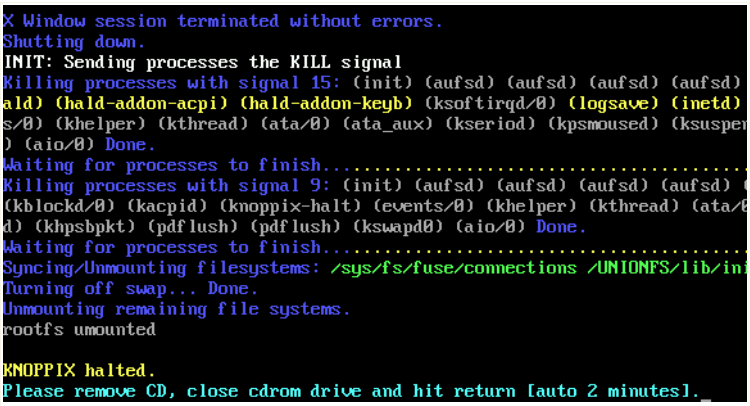
Puede apagar su equipo de forma segura seleccionado la opción **Exit** desde el menú contextual (clic derecho para abrirlo) o introduciendo el comando **halt** en la terminal de comandos.



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

28.3. ¿Cómo realizo 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:

Explore sus carpetas, haga clic derecho en el archivo o carpeta deseado y seleccione **Send to**. A continuación seleccione **BitDefender Scanner**.

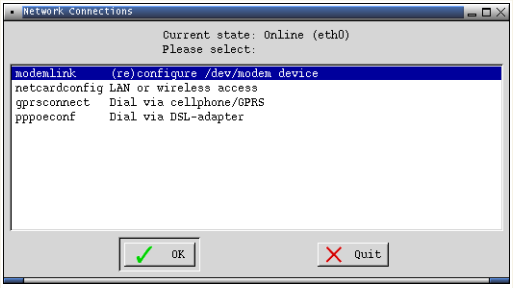
También puede utilizar el siguiente comando estando conectado como root en la terminal. El **Análisis Antivirus de BitDefender** comenzará a analizar los archivos y carpetas seleccionados.

```
# bdscan /path/to/scan/
```

28.4. ¿Cómo puedo configurar la conexión a Internet?

Si tiene una red con DHCP y tiene una tarjeta de red ethernet, Linux Defender debe detectar y configurar automáticamente la conexión de Internet. Para configurar manualmente la conexión de Internet debe seguir los pasos.

1. Haga doble clic en el acceso directo de Network Connections situado en el Escritorio. Aparecerá la siguiente ventana.



Network Connections (Conexiones de Red)

2. Seleccione el tipo de conexión que utiliza y haga clic en OK.

Conexión	Descripción
modemlink	Seleccione este tipo de conexión cuando utilice un módem y una línea de teléfono para acceder a Internet.
netcardconfig	Seleccione este tipo de conexión cuando utilice una conexión de área local (LAN) para acceder a Internet. Esta opción también es válida para conexiones Wi-Fi.
gprsconnect	Seleccione este tipo de conexión cuando acceda a Internet mediante un teléfono móvil y el protocolo GPRS (General Packet Radio Service). Utilice esta opción si en lugar de un teléfono móvil, utiliza un módem GPRS.
pppoeconf	Seleccione este tipo de conexión cuando utilice un módem DSL (Digital Subscriber Line) para acceder a Internet.

3. Siga las instrucciones que aparecen en pantalla. Si no está seguro de los datos que debe introducir, póngase en contacto con su administrador de sistema o red para más detalles.

Importante
Tenga en cuenta que, al seleccionar las opciones mencionadas anteriormente, sólo activará el módem. Para configurar la conexión de red, 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. Introduzca el siguiente comando:

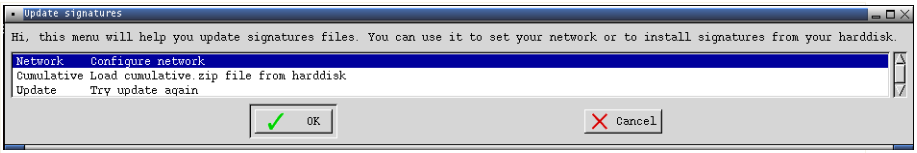
```
# pppconfig
```

4. Siga las instrucciones que aparecen en pantalla. Si no está seguro de los datos que debe introducir, póngase en contacto con su administrador de sistema o red para más detalles.

28.5. ¿Cómo puedo actualizar BitDefender?

Durante la carga del sistema, se actualizan las firmas de virus automáticamente. A continuación le indicamos como actualizar BitDefender, por si ha decidido omitir este paso.

1. Haga doble clic en el acceso directo de Update Signatures situado en el Escritorio. Aparecerá la siguiente ventana.



Update Signatures (Actualizar Firmas)

2. Realice una de estas acciones:
   - Seleccione **Cumulative** para instalar la firmas previamente guardadas en su disco y cargar el archivo `cumulative.zip`.
   - Seleccione **Update** para conectarse a Internet y descargar las últimas firmas de virus.
3. Haga clic en **Aceptar**.

28.5.1. ¿Cómo puedo actualizar BitDefender a través de 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**.

28.6. 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.

   Nota
   Si conecta una memoria USB en otro momento, deberá montar la unidad extraíble siguiendo estos pasos:
   a. Haga doble clic en el acceso directo de Terminal Emulator situado en el Escritorio.
   b. Introduzca el siguiente comando:

   ```
   # mount  /media/sdb1
   ```

   Por favor, tenga en cuenta que en función de la configuración de su equipo, puede ser `sda1` en lugar de `sdb1`.

2. Espere a que el CD de Rescate de BitDefender se cargue. Aparecerá la siguiente ventana:

Ventana del Escritorio

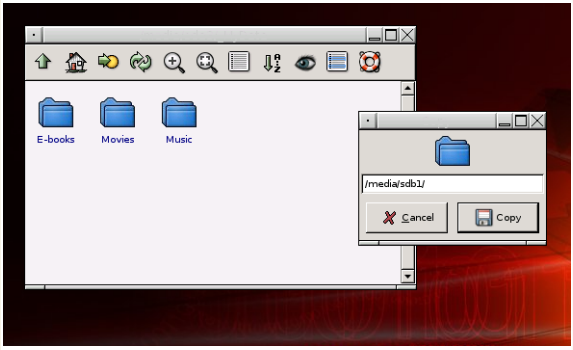
3. Haga doble clic en la partición donde están almacenados los datos que desea guardar (por ej: `[sda3]`).

> ***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.

> ***Importante***
> Si el equipo no se ha apagado correctamente, es posible que algunas particiones no se hayan montado automáticamente. Para montar una partición, siga estos pasos:
> a. Haga doble clic en el acceso directo de Terminal Emulator situado en el Escritorio.
> b. Introduzca el siguiente comando:

```
# mount  /media/partition_name
```

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**.

   Por favor, tenga en cuenta que en función de la configuración de su equipo, puede ser `sda1` en lugar de `sdb1`.

Glosario

ActiveX

El ActiveX es un modelo para escribir programas de manera que otros programas y sistemas operativos puedan usarlos. La tecnología ActiveX se utiliza junto con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y comporten como programas, y no como páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, pulsar botones, interactuar de otras formas con una página web. Los controles ActiveX normalmente están escritos en Visual Basic.

Los ActiveX destacan por la ausencia de controles de seguridad; los expertos en seguridad informática no recomiendan su uso en Internet.

Adware

El Adware habitualmente se combina con aplicaciones que se ofrecen de forma gratuita a cambio que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan después que el usuario acepte los términos de licencia que declaran el propósito de la aplicación, no se comete ningún delito.

Sin embargo, las ventanas emergentes de publicidad pueden resultar molestas, incluso en algunos casos pueden afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar atentar contra la privacidad de aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Archivo Comprimido

Disco, cinta o carpeta que contenga archivos a modo de copia de seguridad.

Archivo que contiene uno o varios archivos en formato comprimido.

Backdoor

Se trata de un agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. El objetivo de estos agujeros no es siempre dañino; algunos sistemas operativos funcionan con unas cuentas privilegiadas, creadas para el servicio técnico o los operadores de mantenimiento.

Sector de arranque

Un sector situado al principio de cada disco que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). En el caso de los discos desde los que se inicia el sistema, el sector de arranque también incluye un programa para cargar el sistema operativo.

Virus de boot

Es un virus que infecta el sector de arranque de un disco duro o disquete. Al intentar arrancar el sistema desde un disco infectado con un virus de boot, el virus quedará cargado en la memoria. A partir de ese momento, cada vez que intente arrancar el sistema, tendrá el virus activo en la memoria.

Navegador

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y 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 textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Línea de comando

En una interfaz de línea de comandos, el usuario puede introducir comandos en el espacio correspondiente de la pantalla, usando un lenguaje de comando.

Cookie

En la industria del Internet, las cookies se describen como pequeños archivos que contienen información sobre los equipos individuales y que pueden ser utilizados por analistas para determinar los intereses y preferencias online de los usuarios. En estos términos, las cookies se desarrollan con la intención de construir reclamos publicitarios adecuados a sus intereses. Es un arma de doble filo porque, por un lado, es más efectivo recibir publicidad relacionada con sus intereses; pero por otro lado, esto supone "seguir" y "rastrear" cada uno de los sitios que visite o los clics que haga. En consecuencia, es normal que se haya abierto un debate sobre la privacidad y que mucha gente se sienta ofendida al ser tratada como "código de barras". Aunque esta perspectiva pueda parecer extremista, en algunos casos se acerca mucho a la realidad.

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 disquetera se encarga de acceder a los disquetes.

Las unidades de disco pueden ser internas (situadas dentro del ordenador) o externas (alojadas en una caja separada que se conecta al ordenador).

Descarga

Para copiar información (normalmente un archivo) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un archivo desde un servicio online hacia un ordenador personal.

También se refiere al proceso de copiar archivos 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 a través de las redes locales o globales.

Eventos

Acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como hacer clic con el ratón o pulsar una tecla, pero también pueden ser acontecimientos del sistema, como quedarse sin espacio en la memoria.

Falso positivo

Se produce cuando se identifica erróneamente como infectado un archivo que en realidad no lo está.

Extensión de un archivo

La última parte del nombre de un archivo, que aparece después del punto e indica el tipo de información almacenada.

Hay varios sistemas operativos que utilizan extensiones de archivos (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Por ejemplo, "c" para archivos de código fuente en lenguaje C, "ps" para PostScript, "txt" para documentos de texto.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva variante de un virus existente. Sin embargo, ocasionalmente puede avisar de la existencia de códigos sospechosos en aplicaciones normales, generando lo que se denomina un "falso positivo".

IP

Internet Protocol (Protocolo de Internet) - Protocolo de direccionamiento y enrutamiento que forma parte del protocolo TCP/IP. Es el responsable del direccionamiento IP, enrutamiento, fragmentación y reagrupación de los paquetes IP.

Applet de Java

Es un programa de Java diseñado para funcionar únicamente en una página web. Para usar un applet, debe especificar su nombre del applet y sus dimensiones (ancho y largo, en píxeles). Al acceder a una página web, el navegador descarga el applet desde un servidor y lo ejecuta en el equipo del usuario (el cliente). Los applets difieren de las aplicaciones al estar regidos por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar en un equipo cliente, no pueden leer o escribir información en esta máquina. Además, los applets tienen restricciones y sólo pueden leer y escribir datos en el mismo domino al 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, que ésta se ejecute cada vez que se abre el documento.

Cliente de Correo

Un cliente de correo es una aplicación que le permite enviar y recibir correos electrónicos.

Memoria

Área de almacenamiento interno en el ordenador. El término memoria se refiere al almacenamiento de información en forma de chips, y la palabra almacenamiento se emplea para la memoria guardada en cintas o discos. Cada ordenador dispone de 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 con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

Programas Empaquetados

Son archivos en formato comprimido. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un archivo para que ocupe menos espacio. Por ejemplo: imagine que tiene un archivo de texto que contiene diez caracteres de espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que pueda empaquetar archivos reemplazaría los caracteres espacio por una serie especial de caracteres, seguidos del número de espacios a reemplazar. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, entre muchas otras.

Ruta

La dirección exacta de un archivo en el ordenador, generalmente descrita por medio de un sistema ordenado jerárquicamente del nivel más básico al más complejo.

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 motiva al usuario a visitar una página Web en la que se le solicita actualizar su información personal (como contraseñas, números de tarjetas de crédito, seguridad social y números de cuentas corrientes) que en realidad ya posee la organización legítima. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar este tipo de información a los usuarios.

Virus Polimórfico

Son virus que cambian de forma en cada archivo que infectan. Al no tener un patrón binario constante, son muy difíciles de identificar.

Puerto

Interfaz de un ordenador en la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar discos duros, pantallas, teclados. Los puertos externos permiten conectar módems, impresoras u otros dispositivos periféricos.

En las redes TCP/IP y UDP, un puerto representa el punto final de una conexión lógica. El número de puerto indica el tipo de dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico HTTP.

Archivo de informe

Es un archivo que lista las acciones realizadas. BitDefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos 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 se refería a las herramientas que proporcionaban 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 periféricos, si éstos incorporan el software apropiado.

Los rootkits no son maliciosos por naturaleza. Por ejemplo, los sistemas operativos y algunas aplicaciones esconden sus archivos críticos mediante 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 archivos o logs, y evitar su detección.

Script

Otro término denominar a los archivos macro o batch, que consiste en una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o los posts basura en grupos de noticias, también denominado correo no solicitado.

Spyware

Se trata de cualquier software que recopile información del usuario a través de su conexión a Internet sin su consentimiento ni conocimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, 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 terceros. El spyware también puede recoger información sobre 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 al instalar otras aplicaciones. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio, un archivo concreto que modifica el nombre de los objetos compartidos.

A parte de las cuestiones éticas y de privacidad, el spyware también roba recursos de memoria y ancho de banda cuando envía la información al creador del Spyware a través de la conexión de Internet del usuario. Este uso indebido de los recursos puede provocar errores en las aplicaciones que se ejecutan en segundo plano, errores del sistema o inestabilidad general del mismo.

Elementos en Inicio

Todos los archivos de esta carpeta se ejecutan al iniciar el ordenador. Por ejemplo: una pantalla de bienvenida, un archivo audio que se reproduce al iniciar el equipo, un recordatorio del calendario u otras aplicaciones pueden ser elementos de Inicio. Normalmente, en esta carpeta se coloca un alias del archivo en lugar del propio archivo.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95, el área de notificación del sistema está ubicada en la barra de tareas de Windows (normalmente en la parte inferior derecha, junto al reloj) y contiene iconos en miniatura que le permiten acceder fácilmente a funciones del sistema, como el fax, la impresora, el módem, el volumen, etc. Haga doble clic o clic derecho en un icono para ver y abrir los detalles y los opciones de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Conjunto de protocolos de red muy utilizados en Internet, que permiten la comunicación entre redes de ordenadorescon diferentes arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para la conexión de redes y enrutamiento del tráfico.

Troyano

Es un programa malintencionado que se hace pasar por una aplicación benigna. A diferencia de los virus, los troyanos no se auto-replican; sin embargo pueden ser igual de peligrosos. Uno de los tipos más peligrosos de Troyano son aquellos programas que pretenden desinfectar su equipo, pero que en realidad introducen virus en el ordenador.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Actualización

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 el 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 buscar manualmente las actualizaciones o dejar que el producto se actualice automáticamente.

Virus

Es un programa o código que se carga en su ordenador sin su consentimiento ni conocimiento, la mayoría de ellos con capacidad para auto-replicarse. Todos los virus informáticos son artificiales, creados por una persona. Es relativamente fácil crear un virus que se replique una y otra vez. Sin embargo, este tipo de virus son muy peligroso porque pueden consumir rápidamente la memoria del ordenador y dejarlo inoperativo. Otro tipo de virus todavía más peligroso son aquellos capaces de propagarse a través de redes y evitar 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.