

**bitdefender**



**ANTIVIRUS<sub>2009</sub>**

*Guía de usuario*

 **bitdefender**



## BitDefender Antivirus 2009

### Guía de usuario

publicado 2008.08.22

Copyright© 2008 BitDefender

#### Advertencia legal

Todos los derechos reservados. Ninguna parte de este documento puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico, mecánico, por fotocopia, grabación o de otra manera, almacenada o introducida en un sistema de recuperación, sin la previa autorización expresa por escrito por un representante de BitDefender. La inclusión de breves citas en críticas sólo puede ser posible con la mención de la fuente citada. El contenido no puede ser modificado en forma alguna.

**Advertencia y Exención de Responsabilidad.** El presente producto y su documentación están protegidos por copyright. La información en este documento se provee "tal como está", sin garantía. Aunque se ha tomado toda precaución en la preparación de este documento, los autores no tendrán ninguna responsabilidad con ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de BitDefender, por lo que BitDefender no se hace responsable por el contenido de cualquier sitio enlazado. Si usted accede a sitios web de terceros listados en este documento, lo hará bajo su responsabilidad. BitDefender proporciona estos enlaces sólo por conveniencia, y la inclusión del enlace no implica que BitDefender apruebe o acepte ninguna responsabilidad por el contenido del sitio del tercero.

**Marcas Registradas.** En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas en este documento son propiedad única de sus respectivos propietarios y les son respectivamente reconocidas.



*BitDefender Antivirus 2009*





# Tabla de contenidos

<b>LICENCIA DE USO DE SOFTWARE PARA EMPRESAS .....</b>	<b>ix</b>
<b>Prólogo .....</b>	<b>xiii</b>
1. Convenciones utilizadas en este libro .....	xiii
1.1. Convenciones Tipográficas .....	xiii
1.2. Advertencias .....	xiv
2. La Estructura del Manual .....	xiv
3. Petición de Comentarios .....	xv
<b>Pasos de la Instalación .....</b>	<b>1</b>
<b>1. Requisitos del Sistema .....</b>	<b>2</b>
1.1. Requisitos de Hardware .....	2
1.2. Requisitos de Software .....	3
<b>2. Instalando BitDefender .....</b>	<b>4</b>
2.1. Asistente de Registro .....	6
2.1.1. Paso 1/2 - Registrar BitDefender Antivirus 2009 .....	7
2.1.2. Paso 2/2 - Crear una Cuenta de BitDefender .....	8
2.2. Asistente de Configuración .....	10
2.2.1. Paso 1/8 - Ventana de Bienvenida .....	11
2.2.2. Paso 2/8 - Seleccione el Modo de Vista .....	12
2.2.3. Paso 3/8 - Configure la Red de Administración .....	13
2.2.4. Paso 4/8 - Configure el Control de Identidad .....	14
2.2.5. Paso 5/8 - Configure el Informe de Virus en Tiempo Real .....	18
2.2.6. Paso 6/8 - Seleccione la Tarea a Ejecutar .....	19
2.2.7. Paso 7/8 - Esperar a que Finalicen las Tareas .....	20
2.2.8. Paso 8/8 - Finalizar .....	21
<b>3. Reparar o Desinstalar BitDefender .....</b>	<b>22</b>
<b>Administración Básica .....</b>	<b>24</b>
<b>4. Primeros Pasos .....</b>	<b>25</b>
4.1. Iniciar BitDefender Antivirus 2009 .....	25
4.2. Modo de Vista de la Interfaz de Usuario .....	25
4.2.1. Vista Básica .....	25
4.2.2. Vista Avanzada .....	27
4.3. Icono de BitDefender en el Área de Notificación del Sistema .....	30
4.4. Barra de Actividad del Análisis .....	31
4.5. Análisis Manual de BitDefender .....	31
4.6. Modo Trabajo .....	32
4.6.1. Usando el Modo Trabajo .....	32



4.6.2. Cambiando el Atajo de Teclado del Modo Trabajo .....	33
4.7. Integración con Navegadores Web .....	33
4.8. Integración con Programas de Mensajería .....	35
<b>5. Visualizador .....</b>	<b>37</b>
5.1. General .....	96
5.2. Tareas .....	39
5.2.1. Analizando con BitDefender .....	39
5.2.2. Actualizando BitDefender .....	40
<b>6. Antivirus .....</b>	<b>42</b>
6.1. Componentes Monitorizados .....	42
6.1.1. Seguridad local .....	86
6.2. Tareas .....	44
6.2.1. Analizando con BitDefender .....	44
6.2.2. Actualizando BitDefender .....	50
<b>7. Antiphishing .....</b>	<b>53</b>
7.1. Componentes Monitorizados .....	53
7.1.1. Seguridad online .....	87
7.2. Tareas .....	55
7.2.1. Analizando con BitDefender .....	55
7.2.2. Actualizando BitDefender .....	61
<b>8. Vulnerabilidad .....</b>	<b>64</b>
8.1. Componentes Monitorizados .....	64
8.1.1. Análisis de Vulnerabilidad .....	88
8.2. Tareas .....	66
8.2.1. Buscando Vulnerabilidades .....	66
<b>9. Red .....</b>	<b>74</b>
9.1. Tareas .....	75
9.1.1. Unirse a la Red de BitDefender .....	191
9.1.2. Añadiendo Equipos a la Red de BitDefender .....	191
9.1.3. Administrando la Red de BitDefender .....	78
9.1.4. Analizando Todos los Equipos .....	80
9.1.5. Actualizando Todos los Equipos .....	81
9.1.6. Registrando Todos los Equipos .....	82
<b>10. Configuración Básica .....</b>	<b>83</b>
10.1. Seguridad local .....	84
10.2. Seguridad online .....	84
10.3. Configuración General .....	85
<b>11. Barra de Estado .....</b>	<b>86</b>
11.1. Seguridad local .....	86
11.2. Seguridad online .....	87
11.3. Análisis de Vulnerabilidad .....	88



<b>12. Registro</b> .....	<b>90</b>
12.1. Paso 1/1 - Registrar BitDefender Antivirus 2009 .....	90
<b>13. Historial</b> .....	<b>92</b>
<b>Administración Avanzada</b> .....	<b>94</b>
<b>14. General</b> .....	<b>95</b>
14.1. Visualizador .....	95
14.1.1. Estadísticas .....	96
14.1.2. General .....	96
14.2. Configuración .....	97
14.2.1. Configuración General .....	98
14.2.2. Configuración del Informe de Virus .....	99
14.3. Información del Sistema .....	99
<b>15. Antivirus</b> .....	<b>101</b>
15.1. Protección en Tiempo Real .....	101
15.1.1. Configurando el Nivel de Protección .....	102
15.1.2. Personalizando el Nivel de Protección .....	103
15.1.3. Configurando el Análisis de Comportamiento .....	107
15.1.4. Desactivando la Protección en Tiempo Real .....	110
15.1.5. Configurando la Protección Antiphishing .....	110
15.2. Análisis Bajo Demanda .....	111
15.2.1. Tareas de Análisis .....	113
15.2.2. Utilizando el Menú Contextual .....	115
15.2.3. Creando tareas de análisis .....	116
15.2.4. Configurando una Tarea de Análisis .....	116
15.2.5. Analizando Objetos .....	129
15.2.6. Viendo los Informes del Análisis .....	135
15.3. Objetos Excluidos del Análisis .....	137
15.3.1. Excluyendo Rutas del Análisis .....	139
15.3.2. Excluyendo Extensiones del Análisis .....	143
15.4. Área de Cuarentena .....	147
15.4.1. Administrando los Archivos en Cuarentena .....	148
15.4.2. Configurando las Opciones de Cuarentena .....	149
<b>16. Control de Privacidad</b> .....	<b>151</b>
16.1. Estado del Control de Privacidad .....	151
16.1.1. Configurando el Nivel de Protección .....	152
16.2. Control de Identidad .....	153
16.2.1. Creando Reglas de Identidad .....	155
16.2.2. Definiendo las Excepciones .....	159
16.2.3. Administrando Reglas .....	160
16.3. Control del registro .....	161
16.4. Control de las Cookies .....	163



16.4.1. Ventana de Configuración .....	165
16.5. Control de Scripts .....	167
16.5.1. Ventana de Configuración .....	168
<b>17. Cifrado de Mensajería Instantánea (IM) .....</b>	<b>170</b>
17.1. Desactivando el Cifrado para Usuarios Específicos .....	172
<b>18. Vulnerabilidad .....</b>	<b>173</b>
18.1. Estado .....	173
18.1.1. Comprobando Vulnerabilidades .....	174
18.2. Configuración .....	180
<b>19. Modo Trabajo / Portátil .....</b>	<b>182</b>
19.1. Modo Trabajo .....	182
19.1.1. Configurando el Modo Trabajo Automático .....	183
19.1.2. Administrando la Lista de Juegos .....	184
19.1.3. Modificando la Configuración del Modo Trabajo .....	186
19.1.4. Cambiando el Atajo de Teclado del Modo Trabajo .....	186
19.2. Modo Portátil .....	187
19.2.1. Configurando las Opciones del Modo Portátil .....	188
<b>20. Red .....</b>	<b>190</b>
20.1. Unirse a la Red de BitDefender .....	191
20.2. Añadiendo Equipos a la Red de BitDefender .....	191
20.3. Administrando la Red de BitDefender .....	193
<b>21. Actualización .....</b>	<b>196</b>
21.1. Actualización automática .....	196
21.1.1. Solicitando una Actualización .....	198
21.1.2. Desactivando la Actualización Automática .....	198
21.2. Configuración de la Actualización .....	199
21.2.1. Configuración de la Ubicaciones de las Actualizaciones .....	200
21.2.2. Configurando la Actualización Automática .....	200
21.2.3. Configurando la Actualización Manual .....	201
21.2.4. Modificando las Opciones Avanzadas .....	201
21.2.5. Administrando los Proxies .....	201
<b>22. Registro .....</b>	<b>204</b>
22.1. Registrando BitDefender Antivirus 2009 .....	204
22.2. Creando una Cuenta de BitDefender .....	206
<b>Conseguir Ayuda .....</b>	<b>209</b>
<b>23. Soporte .....</b>	<b>210</b>
23.1. BitDefender Knowledge Base .....	210
23.2. Solicitando Ayuda .....	211
23.2.1. Ir a la Web de Ayuda On-Line .....	211



23.2.2. Abrir un ticket de soporte .....	211
23.3. Información de Contacto .....	212
23.3.1. Direcciones Web .....	212
23.3.2. Filiales .....	212
<b>CD de Rescate de BitDefender .....</b>	<b>215</b>
<b>24. General .....</b>	<b>216</b>
24.1. Requisitos del Sistema .....	216
24.2. Software Incluido .....	217
<b>25. Cómo Utilizar el CD de Rescate de BitDefender .....</b>	<b>220</b>
25.1. Iniciar el CD de Rescate de BitDefender .....	220
25.2. Detener el CD de Rescate de BitDefender .....	221
25.3. ¿Cómo realizo un análisis antivirus? .....	222
25.4. ¿Cómo puedo configurar la conexión a Internet? .....	223
25.5. ¿Cómo puedo actualizar BitDefender? .....	224
25.5.1. ¿Cómo puedo actualizar BitDefender a través de un servidor proxy? ...	225
25.6. Cómo guardar mis datos? .....	226
<b>Glosario .....</b>	<b>229</b>



# 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 términos 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 automáticamente 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 elección 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, evalúe 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 aérea, centrales nucleares, comunicaciones, armamento, sistemas o equipos de vida asistida, control del tráfico aéreo, 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 Antivirus 2009** como solución de seguridad para sus ordenadores personales. La información presentada en este libro está orientada no sólo para los usuarios avanzados, sino a todas aquellas personas que trabajan bajo Windows.

Este manual le describirá el uso de **BitDefender Antivirus 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 Antivirus 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.

<i>Apariencia</i>	<i>Descripción</i>
sample syntax	Los ejemplos de sintaxis se muestran con caracteres <code>monoespaciados</code> .
<a href="http://www.bitdefender.com">http://www.bitdefender.com</a>	Los enlaces URL le dirigen a algunas ubicaciones externas, a servidores http o ftp.
<a href="mailto:support@bitdefender.com">support@bitdefender.com</a>	Las direcciones de e-mail se incluyen en el texto como información de contacto.
“Prólogo” (p. xiii)	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 <code>monoespaciada</code> .
<b>option</b>	Todas las opciones del producto se muestran usando letra en <b>negrita</b> .



Apariencia	Descripción
<code>sample code listing</code>	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 extrema 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 Antivirus 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 desinstalación 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 mostrará como configurar de manera eficaz todos los módulos



de BitDefender para proteger su equipo en contra de malware (virus, spyware, rootkits etc...)

**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](mailto:documentation@bitdefender.com).



#### ***Importante***

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



*BitDefender Antivirus 2009*

# Pasos de la Instalación



# 1. Requisitos del Sistema

Sólo podrá instalar BitDefender Antivirus 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 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.

The collage shows the following steps:

- 1. Bienvenido al Instalador de BitDefender:** Welcome screen with instructions to click 'Sí' to continue or 'No' to abort.
- 2. Recomendaciones:** Screen with recommendations to disable other security products and to have two antivirus programs installed.
- 3. Contrato de licencia:** License agreement screen for 'LICENCIA DE USO DE SOFTWARE PARA EMPRESAS'. Buttons: 'Acepto', 'Edito de acuerdo', 'Cancelar'.
- 4. Seleccione la ubicación de la instalación:** Screen to choose the installation location. Location: 'H:\Program Files\BitDefender\'. Buttons: '< Atrás', 'Finalizar'.
- 5. Configuración de acceso:** Screen to choose file access options. 'Abrir fichero Home' is unchecked, 'Crear acceso directo' is checked. Buttons: '< Atrás', 'Finalizar'.
- 6. Finalizando la instalación del programa BitDefender Antivirus 2009:** Final screen with instructions to click 'Finalizar' to complete the installation. Buttons: '< Atrás', 'Finalizar', 'Cancelar'.

Pasos de la Instalación



Siga estos pasos para instalar BitDefender Antivirus 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 Antivirus 2009 le alertará 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 las condiciones, haga clic en **Cancelar**. Abandonará el proceso de instalación y saldrá del asistente.

4. Por defecto, BitDefender Antivirus 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 Antivirus 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 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**. Siga los pasos de estos asistentes para registrar y configurar BitDefender Antivirus 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>.

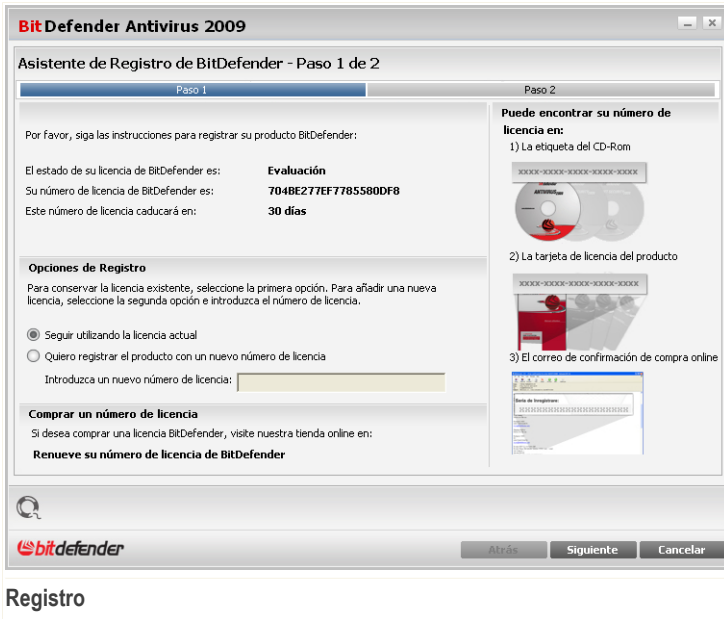


### **Nota**

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 Antivirus 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 Antivirus 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

**BitDefender Antivirus 2009**

Asistente de Registro de BitDefender - Paso 2 de 2

**Registro en Mi Cuenta**

La Cuenta de BitDefender le da acceso al soporte técnico, así como a ofertas y promociones especiales. En caso de pérdida de su número de licencia de BitDefender, puede recuperarlo iniciando sesión en <http://myaccount.bitdefender.com>. Puede elegir entre iniciar sesión con una Cuenta de BitDefender existente o crear una nueva cuenta.

Iniciar sesión con una Cuenta de BitDefender existente

E-mail:

Contraseña:

[¿Ha olvidado su contraseña?](#)

Omitir Registro

Crear una Cuenta de BitDefender nueva

E-mail:

Contraseña:

Repetir contraseña:

Nombre:

Apellidos:

País:

Enviarme todos los mensajes de BitDefender

Enviarme sólo los mensajes más importantes

No enviarme ningún mensaje

bitdefender

Atrás Finalizar Cancelar

**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 Antivirus 2009 esté instalado.

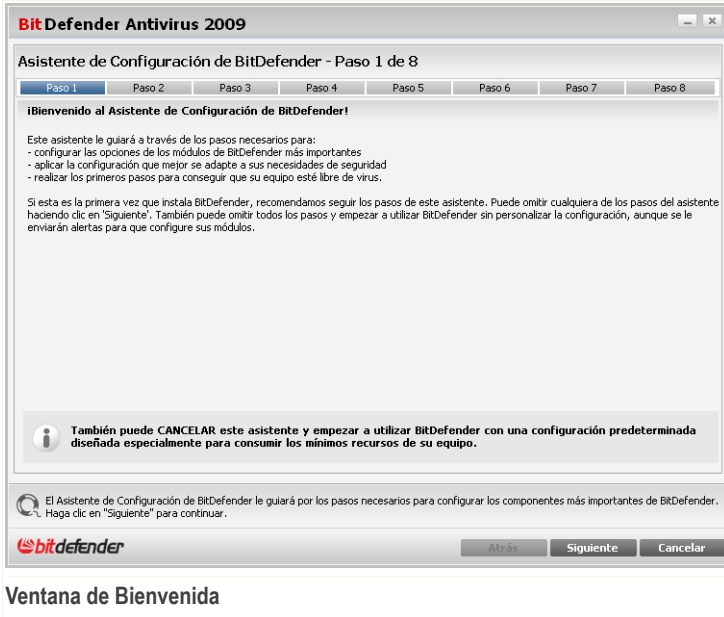


### **Nota**

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 1/8 - Ventana de Bienvenida



### Ventana de Bienvenida

Haga clic en **Siguiente** para continuar.



## 2.2.2. Paso 2/8 - Seleccione el Modo de Vista

**BitDefender Antivirus 2009**

Asistente de Configuración de BitDefender - Paso 2 de 8

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6 Paso 7 Paso 8

**Modos de Vista de la Interfaz de Usuario**

Puede elegir entre una vista Básica o Avanzada de BitDefender, en función de su experiencia como usuario y con el producto

**Vista Básica**  
Interfaz Básica que le permite acceder a todos los módulos a un nivel muy básico. Podrá solucionar rápidamente todas las incidencias que afectan la seguridad de su sistema.

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

Podrá cambiar entre las dos vistas en cualquier momento mientras utiliza BitDefender

Haga clic aquí para cambiar la Interfaz de Usuario de BitDefender a Vista Básica.

**bitdefender** Atrás Siguiente Cancelar

### 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 3/8 - Configure la Red de Administración

**BitDefender Antivirus 2009**

Asistente de Configuración de BitDefender - Paso 3 de 8

Paso 1 Paso 2 **Paso 3** Paso 4 Paso 5 Paso 6 Paso 7 Paso 8

**Configuración de Administración de Red**

BitDefender 2009 incluye un nuevo módulo, Administración de Red, que le permite crear una red virtual de todos los equipos y administrar los productos BitDefender instalados en esta red. Puede actuar como administrador de la red creada, o bien formar parte de ella y permitir la administración de su sistema desde otro equipo.

Marque la casilla de debajo si desea formar parte de la Red de Administración de BitDefender. Se le solicitará introducir una contraseña de Administración de Red, que permitirá al administrador de la red el control de la configuración de BitDefender y la ejecución de tareas remotas en su equipo.

Quiero Formar parte de la Red de Administración de BitDefender

Contraseña de Administración de Red:

Repetir contraseña:

Para encontrar más información sobre las opciones de la Interfaz de Usuario de BitDefender, sitúe el ratón encima de la ventana y aparecerá un texto de ayuda en esta área.

**bitdefender** Atrás Siguiente Cancelar

### 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.





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.

**Añadir Regla de Identidad**

Nombre de la Regla   Analizar HTTP

Tipo de Regla Tarjeta de crédito  Analizar SMTP

Datos de la Regla   Coincidir palabras completas

Mayúsculas y Minúsculas

Analizar Mensajería Instantánea

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:

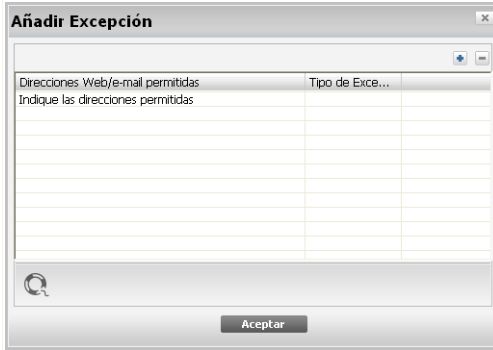
- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (correo) y bloquea los mensajes salientes que coinciden con los datos de la regla.
- **Analizar Mensajería Instantánea** - analiza el 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 5/8 – Configure el Informe de Virus en Tiempo Real

**BitDefender Antivirus 2009**

Asistente de Configuración de BitDefender - Paso 5 de 8

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6 Paso 7 Paso 8

**Bienvenido a la Configuración del Informe de Virus Anónimo**

Cuando realiza un análisis, BitDefender crea automáticamente informes de actividad con estadísticas sobre las amenazas detectadas y el número de archivos analizados, entre otros. Recomendamos enviar estos informes a los Laboratorios BitDefender para su análisis. Para enviarlos, marque la opción correspondiente situada más abajo. Estos informes no contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.

Enviar Informe de Virus

Activar Detección de Epidemias de BitDefender

Para encontrar más información sobre las opciones de la Interfaz de Usuario de BitDefender, sitúe el ratón encima de la ventana y aparecerá un texto de ayuda en este área.

**bitdefender** Atrás Siguiente Cancelar

**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.



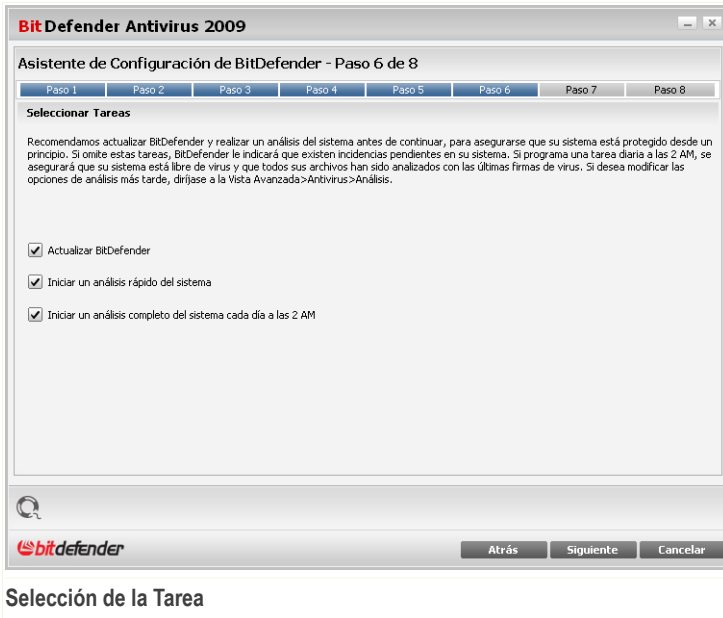
### Nota

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.

## 2.2.6. Paso 6/8 – Seleccionar la Tarea a Ejecutar



Configure BitDefender Antivirus 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.



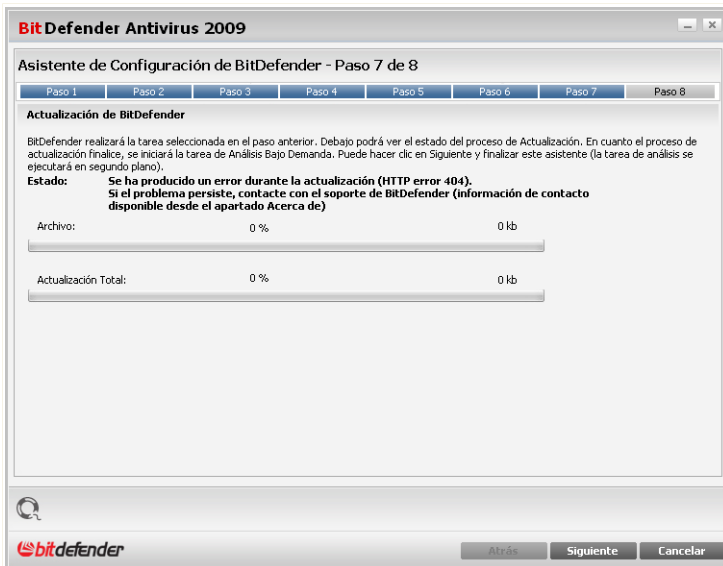
## Importante

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.

## 2.2.7. Paso 7/8 - Esperar a que Finalicen las Tareas



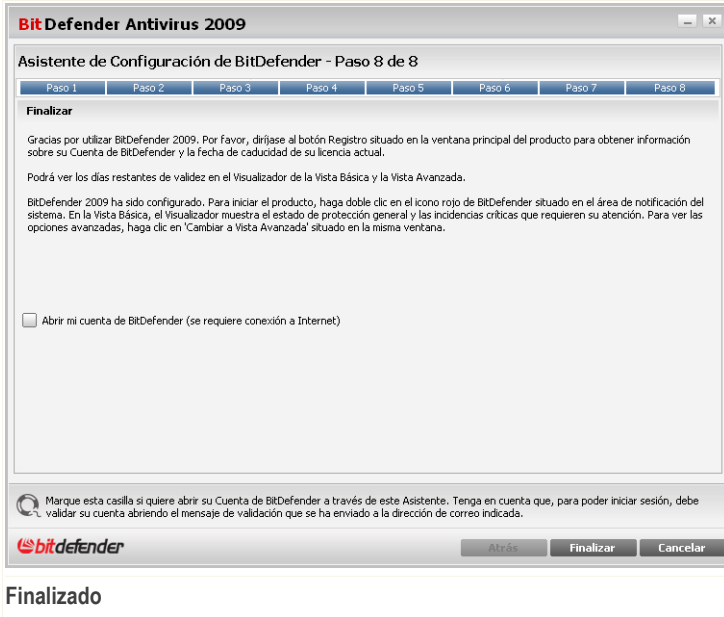
### Estado de la Tarea

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

Haga clic en **Siguiente** para continuar.



## 2.2.8. Paso 8/8 - Finalizar



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 Antivirus 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 equipo cuando se le indique y, a continuación, haga clic en **Instalar** para reinstalar BitDefender Antivirus 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**

**¡Sólo para Windows Vista!** Al desinstalar BitDefender, no estará protegido contra las amenazas de malware, como virus o spyware. Si desea activar Windows Defender al finalizar la desinstalación de BitDefender, seleccione la casilla correspondiente.

Haga clic en **Desinstalar** para iniciar la desinstalación de BitDefender Antivirus 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 Antivirus 2009

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

Para acceder a la interfaz de BitDefender Antivirus 2009, haga clic en el menú Inicio de Windows y siga estos pasos: **Inicio** → **Programas** → **BitDefender 2009** → **BitDefender Antivirus 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 Antivirus 2009 satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes.

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.



- 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 fácilmente los módulos de seguridad importantes.
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.



<b>Pestaña</b>	<b>Descripción</b>
Visualizador	Muestra estadísticas representativas sobre la actividad del producto, el estado de su registro y enlaces a las tareas bajo demanda más importantes.
Antivirus	Muestra el estado del módulo antivirus que le ayudará a mantener actualizado BitDefender y su equipo libre de virus.
Antiphishing	Muestra el estado del módulo antiphishing que le asegura que todas las páginas a las que accede a través de Internet Explorer o Firefox son seguras.
Vulnerabilidad	Muestra el estado del módulo vulnerabilidad que le ayuda a mantener actualizado el software crucial de su PC.
Red	Muestra la estructura de la red de administración.

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

<b>Enlace</b>	<b>Descripción</b>
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.
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.



<b>Módulo</b>	<b>Descripción</b>
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.
Control de Privacidad	Le ayuda a impedir el robo de datos de su equipo y protege su privacidad mientras está conectado a Internet.
Cifrado	Le permite cifrar las conversaciones de Yahoo y Windows Live (MSN) Messenger.
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.
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 Antivirus 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.

<b>Enlace</b>	<b>Descripción</b>
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.



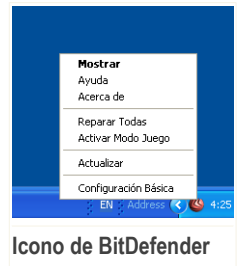
Enlace	Descripción
Soporte	Le permite ponerse en contacto con el equipo de soporte de BitDefender.
Historial	Le permite ver un historial detallado sobre las tareas que BitDefender ha realizado en su sistema.

### 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.

- **Mostrar** - abre BitDefender.
- **Ayuda** - abre el archivo de ayuda en el que se explica el funcionamiento y uso de BitDefender Antivirus 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.



Icono de BitDefender

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

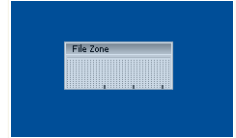
La **barra de análisis de la actividad** es una vista gráfica de la actividad de análisis de su sistema.

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



### Nota

La barra de actividad del análisis le avisa cuando la protección en tiempo real está desactivada mostrando una cruz roja sobre la **Archivos**.



Barra de Actividad

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. 130) de esta guía de usuario.

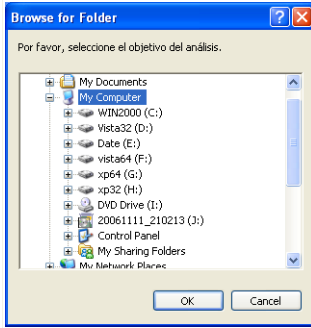
Para ocultar la barra de actividad haga clic derecho encima y seleccione **Ocultar**. Para ocultar completamente esta ventana, siga estos pasos:

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 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



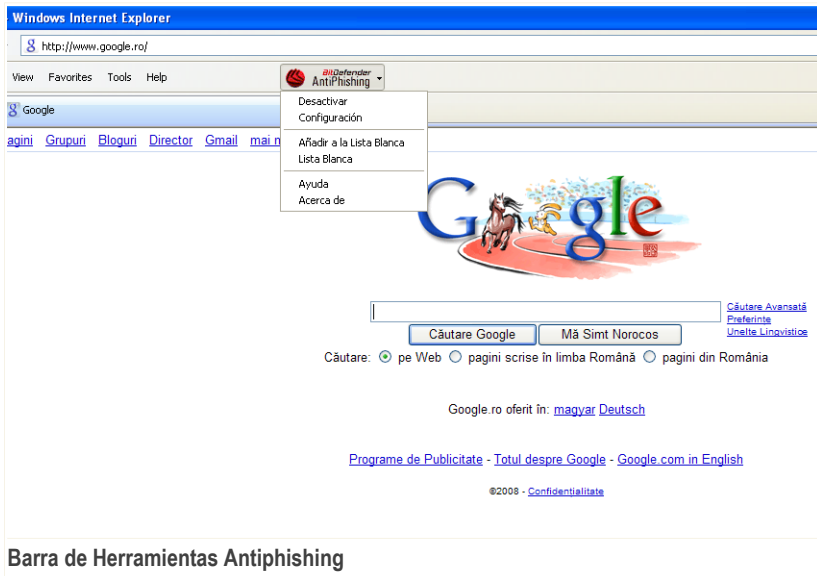
Puede administrar la protección antiphishing y la Lista Blanca fácilmente a través de la barra de herramientas de BitDefender Antiphishing, integrada en los navegadores citados anteriormente.

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**.



Windows Internet Explorer

http://www.google.ro/

View Favorites Tools Help

Google

agini Grupuri Bloguri Directori Gmail mai n

BitDefender Antiphishing

- Desactivar
- Configuración
- Añadir a la Lista Blanca
- Lista Blanca
- Ayuda
- Acerca de

Căutare Avansată  
Preferințe  
Unește linkurile

Căutare Google Mă Simt Norocos

Căutare:  pe Web  pagini scrise în limba Română  pagini din România

Google.ro oferit în: [magyar](#) [Deutsch](#)

[Programe de Publicitate - Totul despre Google - Google.com in English](#)

©2008 - [Confidentialitate](#)

### 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.

## 4.8. 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

Desactivar permanentemente el cifrado para matey\_alex  
Invitar a matey\_alex a utilizar el cifrado  
Añadir matey\_alex a la Lista Negra del Control Parental

### **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.

BitDefender Antivirus 2009 - Evaluación

CONFIGURACIÓN CAMBIAR A VISTA AVANZADA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

VISUALIZADOR ANTIVIRUS ADVERTENCIA CRÍTICA ANTIPHISHING PROTEGIDO VULNERABILIDAD PROTEGIDO RED

Estado

Estado global de Mi PC:  
**ADVERTENCIA CRÍTICA**

Hay 2 incidencias que afectan a la seguridad de su sistema.  
REPARAR TODAS

Tareas

- Actualizar
- Análisis Completo
- Análisis en Profundidad

General

Registro:	Válido	Última actualización:	Nunca
Caduca en:		Último análisis:	Nunca
	30 días	Próximo análisis:	Nunca

El módulo Visualizador muestra estadísticas representativas sobre la actividad del producto, el estado de su registro y enlaces a las tareas más importantes.

bitdefender

Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial

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
<b>Mi Cuenta</b>	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.
<b>Registro</b>	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.
<b>Caduca en</b>	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 Antivirus 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 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. 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
<b>Análisis Completo de Sistema</b>	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.
<b>Análisis en Profundidad</b>	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.

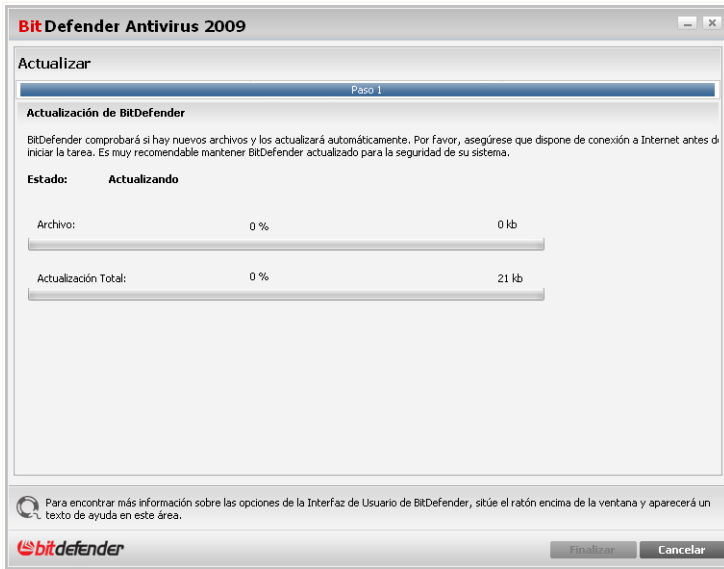


Siga el proceso guiado de tres pasos para completar el proceso de análisis.

## 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. Antivirus

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

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

The screenshot shows the BitDefender Antivirus 2009 interface. At the top, there's a title bar with 'BitDefender Antivirus 2009 - Evaluación' and buttons for 'CONFIGURACIÓN' and 'CAMBIAR A VISTA AVANZADA'. Below the title bar, a red banner indicates 'ESTADO: Hay 2 incidencias por resolver' and a 'REPARAR TODAS' button. The main area features five tabs: 'VISUALIZADOR', 'ANTIVIRUS ADVERTENCIA CRÍTICA', 'ANTIPHISHING PROTEGIDO', 'VULNERABILIDAD PROTEGIDO', and 'RED'. The 'ANTIVIRUS ADVERTENCIA CRÍTICA' tab is selected. Below the tabs, there's a section for 'Componentes Monitorizados' with a 'Mostrar/Ocultar Todo' link. A table lists the monitored components under 'Seguridad Local':

Componente	Monitorizar	Estado
Protección de archivos en tiempo real activada	<input checked="" type="checkbox"/> Sí	Aceptar
Nunca ha analizado su equipo en busca de malware	<input checked="" type="checkbox"/> Sí	Reparar
Nunca ha realizado una actualización	<input checked="" type="checkbox"/> Sí	Reparar

To the right of the table is a 'Tareas' section with links for 'Actualizar', 'Analizar Mis Documentos', 'Análisis Completo', and 'Análisis en Profundidad'. At the bottom, there's a footer with the BitDefender logo and links for 'Comprar', 'Mi Cuenta', 'Registrar', 'Ayuda', 'Soporte', and 'Historial'.

### Antivirus

El módulo Antivirus 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

El componente monitorizado es el siguiente:



<i>Categoría</i>	<i>Descripción</i>
<b>Seguridad Local</b>	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.).

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 Antivirus 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**.

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

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 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:

<i>Tarea</i>	<i>Descripción</i>
<b>Análisis Completo de Sistema</b>	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.
<b>Análisis en Profundidad</b>	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.



Tarea	Descripción
<b>Analizar Mis Documentos</b>	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.
<b>Análisis personalizado</b>	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.

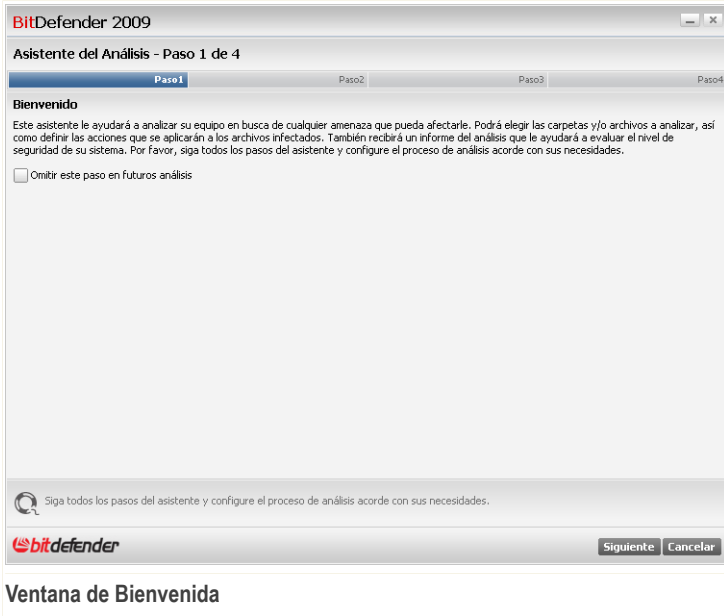
Siga el proceso guiado de tres pasos para completar el proceso de análisis.

### **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.



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.



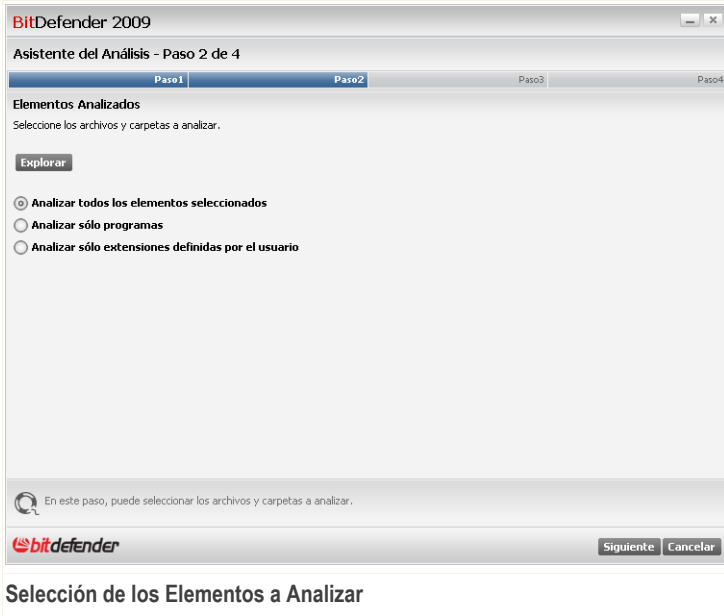
### Nota

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
<b>Analizar todos los elementos seleccionados</b>	Seleccione esta opción para analizar sólo los elementos seleccionados anteriormente.
<b>Analizar sólo programas</b>	Seleccione esta opción para analizar únicamente archivos de programas y aplicaciones.
<b>Analizar sólo extensiones definidas por el usuario</b>	Seleccione esta opción para analizar sólo los archivos con determinadas extensiones. Aparecerá un cuadro de texto en el que podrá indicar estas extensiones.
	<b>Nota</b>  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.

**BitDefender 2009**  
Asistente del Análisis - Paso 3 de 4

**Opciones de Acción**

Al encontrar un archivo infectado	Desinfectarlo
Al encontrar un archivo sospechoso	No realizar ninguna acción
Al encontrar un archivo oculto	No realizar ninguna acción

**Nivel de Análisis**

Alto  
Medio  
Bajo  
Personalizado

**Nivel medio**

- predeterminado, consumo moderado de recursos
- analizar todos los archivos
- analizar en busca de virus y spyware

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

**bitdefender**    Atrás    Siguiente    Cancelar

### 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:

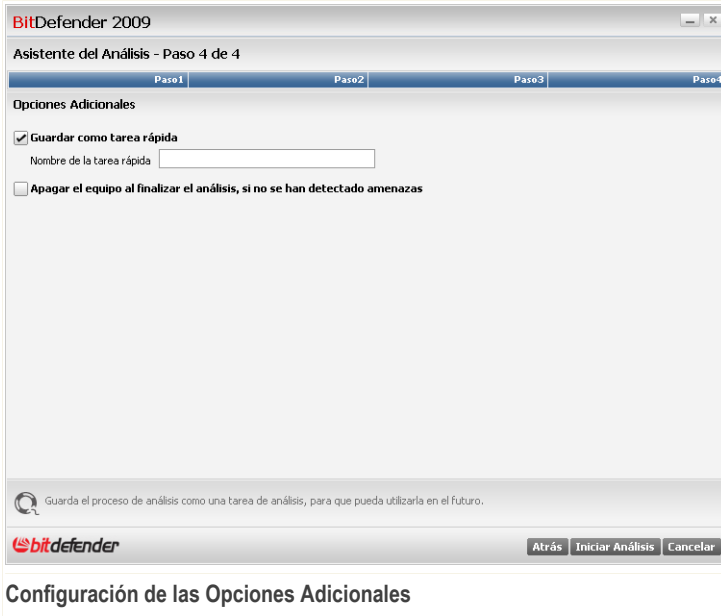


<b>Nivel de Protección</b>	<b>Descripción</b>
<b>Alto</b>	<p>Ofrece un alto nivel de seguridad. El nivel de consumo de recursos es alto.</p> <ul style="list-style-type: none"><li>■ analiza todos los archivos y comprimidos</li><li>■ analiza en busca de virus y spyware</li><li>■ analiza en busca de procesos ocultos</li></ul>
<b>Mediana</b>	<p>Ofrece un nivel de seguridad medio. El nivel de consumo de recursos es moderado.</p> <ul style="list-style-type: none"><li>■ analiza todos los archivos</li><li>■ analiza en busca de virus y spyware</li></ul>
<b>Bajo</b>	<p>Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo.</p> <ul style="list-style-type: none"><li>■ analiza sólo archivos de programas</li><li>■ analiza en busca de virus</li></ul>
<b>Personalizado</b>	<p>Desde aquí puede seleccionar sus propias opciones de análisis. Haga clic en Personalizar y establezca el nivel de análisis deseado.</p> <p>Seleccione las casillas correspondientes al tipo de malware que desea buscar en su equipo durante el proceso de análisis.</p>

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.



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.

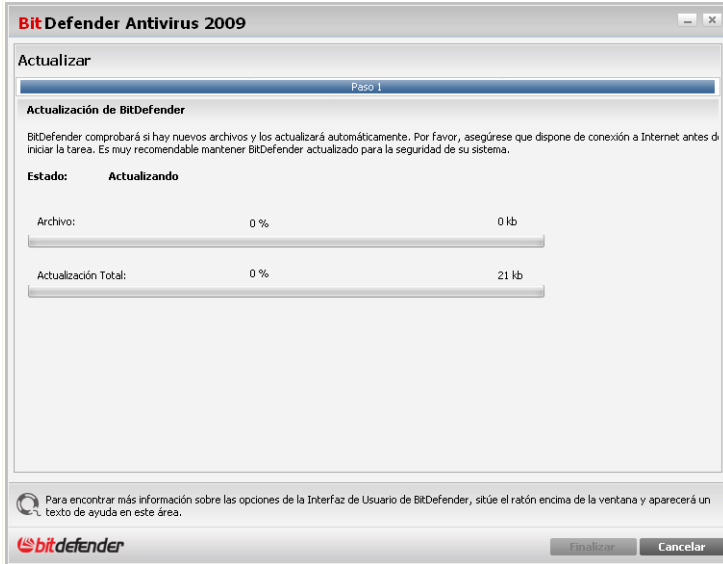
Haga clic en **Iniciar Análisis** y siga el asistente guiado de tres pasos para completar el proceso de análisis.

## 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.



## 7. Antiphishing

BitDefender incluye un módulo Antiphishing que le asegura que todas las páginas a las que accede a través de Internet Explorer o Firefox son seguras.

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

The screenshot shows the BitDefender Antivirus 2009 interface. At the top, there's a title bar with 'BitDefender Antivirus 2009 - Evaluación' and buttons for 'CONFIGURACIÓN' and 'CAMBIAR A VISTA AVANZADA'. Below the title bar, a red status bar indicates 'ESTADO: Hay 2 incidencias por resolver' and a 'REPARAR TODAS' button. The main interface has five tabs: 'VISUALIZADOR', 'ANTIVIRUS ADVERTENCIA CRÍTICA', 'ANTIPHISHING PROTEGIDO', 'VULNERABILIDAD PROTEGIDO', and 'RED'. The 'ANTIPHISHING PROTEGIDO' tab is selected. Below the tabs, there's a section for 'Componentes Monitorizados' with a dropdown menu showing 'Seguridad Online' and a status of 'Aceptar'. To the right, there's a 'Tareas' section with expandable options: 'Actualizar', 'Análisis Completo', and 'Análisis en Profundidad'. At the bottom, there's a description of the Antiphishing component and a footer with the BitDefender logo and links for 'Comprar', 'Mi Cuenta', 'Registrar', 'Ayuda', 'Soporte', and 'Historial'.

El módulo Antiphishing 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:



<b>Categoría</b>	<b>Descripción</b>
<b>Seguridad Online</b>	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.

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

### 7.1.1. 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**.

<b>Incidencia</b>	<b>Descripción</b>
<b>Cifrado de conversaciones de IM activado</b>	Si sus contactos de mensajería tienen instalado BitDefender 2009, se cifrarán todas las conversaciones de Yahoo! Messenger y Windows Live Messenger. Recomendamos mantener activado el Cifrado de conversaciones de IM para asegurarse la privacidad de sus conversaciones por mensajería.
<b>Antiphishing activado para Mozilla Firefox</b>	BitDefender le protege contra los intentos de phishing mientras navega por Internet.
<b>Antiphishing activado para Internet Explorer</b>	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**.



## 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.
- **Análisis personalizado**

### 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:

<i>Tarea</i>	<i>Descripción</i>
<b>Análisis Completo de Sistema</b>	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.
<b>Análisis en Profundidad</b>	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.
<b>Analizar Mis Documentos</b>	Utilice esta tarea para analizar las carpetas del usuario en uso: <i>Mis Documentos</i> , <i>Escritorio</i> e <i>Inicio</i> . Así asegurará el contenido de sus documentos, conseguirá un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.
<b>Análisis personalizado</b>	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.

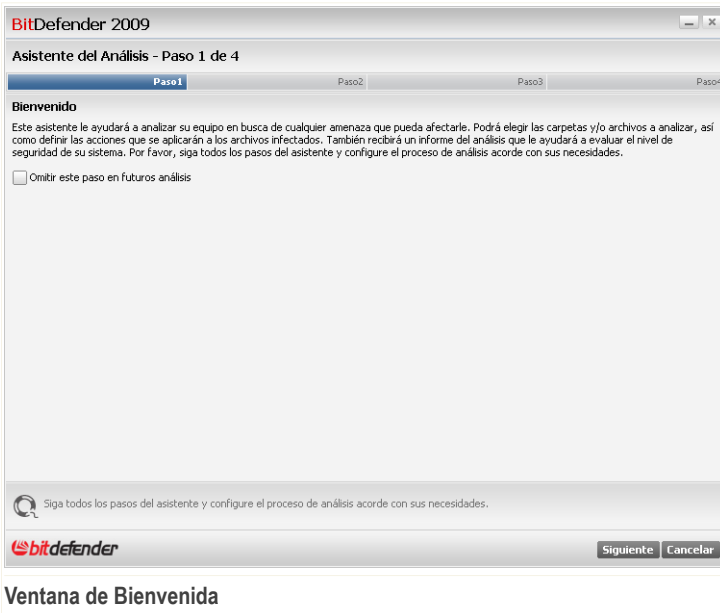
Siga el proceso guiado de tres pasos para completar el proceso de análisis.

## 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.





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.

BitDefender 2009

Asistente del Análisis - Paso 2 de 4

Paso 1 Paso 2 Paso 3 Paso 4

**Elementos Analizados**

Seleccione los archivos y carpetas a analizar.

Explorar

Analizar todos los elementos seleccionados

Analizar sólo programas

Analizar sólo extensiones definidas por el usuario

En este paso, puede seleccionar los archivos y carpetas a analizar.

bitdefender

Siguiente Cancelar


**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:

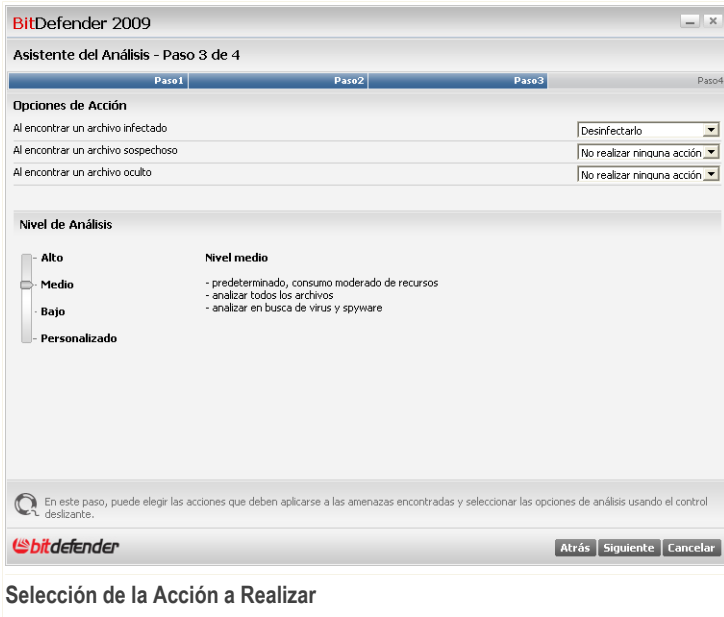
Opción	Descripción
<b>Analizar todos los elementos seleccionados</b>	Seleccione esta opción para analizar sólo los elementos seleccionados anteriormente.
<b>Analizar sólo programas</b>	Seleccione esta opción para analizar únicamente archivos de programas y aplicaciones.
<b>Analizar sólo extensiones definidas por el usuario</b>	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.



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:

<b>Nivel de Protección</b>	<b>Descripción</b>
<b>Alto</b>	Ofrece un alto nivel de seguridad. El nivel de consumo de recursos es alto.

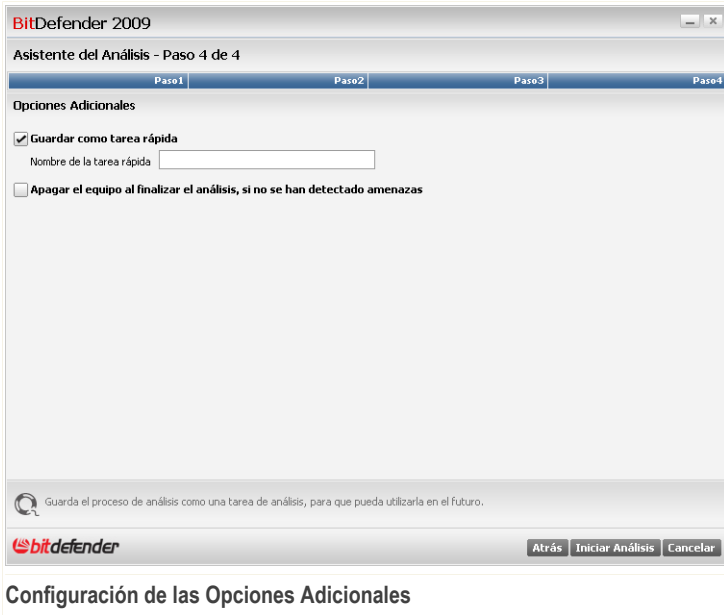


<b>Nivel de Protección</b>	<b>Descripción</b>
	<ul style="list-style-type: none"><li>■ analiza todos los archivos y comprimidos</li><li>■ analiza en busca de virus y spyware</li><li>■ analiza en busca de procesos ocultos</li></ul>
<b>Mediana</b>	<p>Ofrece un nivel de seguridad medio. El nivel de consumo de recursos es moderado.</p> <ul style="list-style-type: none"><li>■ analiza todos los archivos</li><li>■ analiza en busca de virus y spyware</li></ul>
<b>Bajo</b>	<p>Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo.</p> <ul style="list-style-type: none"><li>■ analiza sólo archivos de programas</li><li>■ analiza en busca de virus</li></ul>
<b>Personalizado</b>	<p>Desde aquí puede seleccionar sus propias opciones de análisis. Haga clic en Personalizar y establezca el nivel de análisis deseado.</p> <p>Seleccione las casillas correspondientes al tipo de malware que desea buscar en su equipo durante el proceso de análisis.</p>

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.



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.

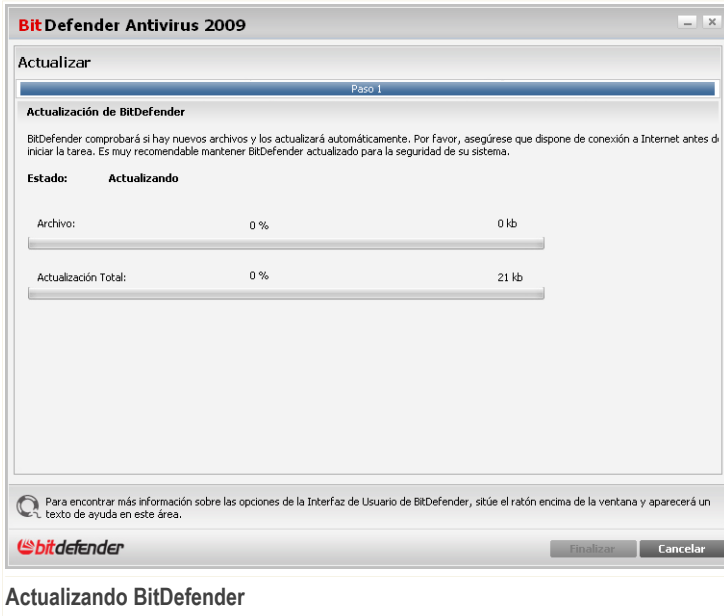
Haga clic en **Iniciar Análisis** y siga el asistente guiado de tres pasos para completar el proceso de análisis.

## 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:



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. Vulnerabilidad

BitDefender incluye un módulo Vulnerabilidad que le ayuda a mantener actualizado el software crucial de su PC.

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

**Vulnerabilidad**

El módulo Vulnerabilidad 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 un enlace a una de las tareas de seguridad más importantes.

### 8.1. Componentes Monitorizados

El componente monitorizado es el siguiente:



<i>Categoría</i>	<i>Descripción</i>
<b>Análisis de Vulnerabilidad</b>	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.

### 8.1.1. 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**.

<i>Incidencia</i>	<i>Descripción</i>
<b>Comprobación de Vulnerabilidades activada</b>	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.
<b>Actualizaciones Críticas de Microsoft</b>	Instala las actualizaciones críticas de Microsoft disponibles.
<b>Otras actualizaciones de Microsoft</b>	Instala las actualizaciones no-críticas de Microsoft disponibles.
<b>Actualizaciones Automáticas de Windows activadas</b>	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.
<b>Admin (Contraseña Segura)</b>	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**.

## **8.2. Tareas**

Aquí encontrará un enlace a una de las tareas de seguridad más importantes.

Dispone del siguiente botón:

- **Análisis de Vulnerabilidad**

### **8.2.1. 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

**BitDefender Total Security 2009**

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6

**Seleccionar tareas**

Este asistente le guiará a través de las acciones necesarias para identificar aplicaciones no actualizadas y cuentas de Windows con contraseñas inseguras. Por favor, seleccione los elementos a comprobar en busca de vulnerabilidades en la lista de abajo.

- Comprobar Contraseñas de Cuentas de Windows
- Buscar Actualizaciones de Aplicaciones
- Buscar Actualizaciones Críticas de Windows
- Buscar Actualizaciones Opcionales de Windows

Seleccione esta casilla para que BitDefender compruebe las contraseñas de las cuentas de Windows de su equipo. Estas contraseñas deben contener números, letras y símbolos para conseguir una mejor protección de sus cuentas.

**bitdefender** **Siguiente** **Cancelar**

**Vulnerabilidades**

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



## Paso 2/6 - Comprobando Vulnerabilidades



Espera hasta que BitDefender finalice la comprobación de vulnerabilidades.



## Paso 3/6 - Cambie las Contraseñas Inseguras

BitDefender Total Security 2009

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6

Comprobar Contraseñas de Cuentas de Windows

Usuario	Fortaleza	Estado
Administrator	Strong	ok
amirea	Strong	ok

Esta es una lista de las contraseñas de las cuentas de Windows de su equipo y su nivel de protección. Haga clic en el botón 'Reparar' para modificar las contraseñas débiles.

**bitdefender** Siguiente Cancelar

### Contraseñas de los Usuarios

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

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

BitDefender

Choose method to fix:

- Force user to change password at next login
- Change user password

Type password:

Confirm password:

OK Close

### 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

Aplicación	Versión Instalada	Última Versión	Estado
Adobe Reader	8.1.2	8.1.2	Actualizado
Yahoo! Messenger	8.1.0.421	8.1.0.241	Actualizado
Firefox	3.0 (en-US)	3.0 (en-US)	Actualizado

Esta es una lista de las aplicaciones soportadas por BitDefender y las actualizaciones disponibles, en caso que existan.

**Aplicaciones**

**Siguiente** **Cancelar**

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

**BitDefender Total Security 2009**

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 **Paso 4** Paso 5 Paso 6

Actualizaciones de Windows

Buscar Actualizaciones Críticas de Windows

- Security Update for Windows XP (KB901190)
- Security Update for Microsoft XML Core Services 6.0 and Microsoft XML Core Services 6.0 Service Pack 1 (KB933579)
- Microsoft .NET Framework 2.0 Service Pack 1 (KB110806)
- Microsoft .NET Framework 1.1 Service Pack 1
- Security Update for Windows XP (KB950749)
- Update for Windows XP (KB932823)
- Security Update for Windows XP (KB950762)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB936181)
- Security Update for Windows XP (KB951376)
- Security Update for Windows XP (KB951698)
- Windows XP Service Pack 3 (KB936929)
- Security Update for Windows XP (KB951748)
- Cumulative Security Update for ActiveX Killbits for Windows XP (KB953839)
- Windows Malicious Software Removal Tool - August 2008 (KB890830)
- Security Update for Outlook Express for Windows XP (KB951066)

**Instalar Todas las Actualizaciones del Sistema**

Esta es una lista de las actualizaciones críticas y no críticas de las aplicaciones de Windows

**bitdefender** Siguiente Cancelar

**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

BitDefender Total Security 2009

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6

El análisis de vulnerabilidad ha finalizado, pero no se han instalado ninguna actualización. Es sumamente recomendable mantener su equipo actualizado.

El análisis de vulnerabilidad ha finalizado, pero no se han instalado ninguna actualización. Es sumamente recomendable mantener su equipo actualizado.

bitdefender

Cerrar

### Resultados

Haga clic en **Cerrar**.



## 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**.

BitDefender Antivirus 2009 - Evaluación

CONFIGURACIÓN CAMBIAR A VISTA AVANZADA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

VISUALIZADOR ANTIVIRUS ADVERTENCIA CRÍTICA ANTIPHISHING PROTEGIDO VULNERABILIDAD PROTEGIDO RED

INTERNET 10.10.0.1

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Ningún PC (clic para añadir)

Tareas

Unirse a/Crear Red

El módulo Red muestra la estructura de la red de administración (si la red no está configurada aparecerá de color gris). Haga clic en "Unirse a/Crear Red" para empezar a crear su red de administración.

bitdefender

Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial

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 uno 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.

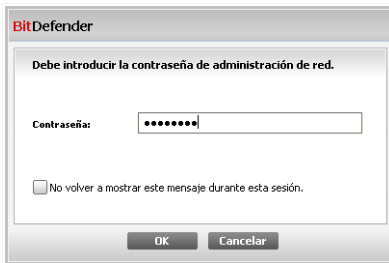


## 9.1.2. Añadiendo Equipos a la Red de BitDefender

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

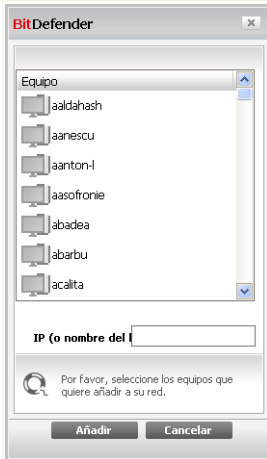
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

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.



The screenshot shows a dialog box titled "BitDefender". Inside, the text reads "Debe introducir la contraseña de administración de red." Below this is a text input field labeled "Contraseña:". At the bottom left, there is a checkbox with the text "No volver a mostrar este mensaje durante esta sesión." At the bottom right, there are two buttons: "OK" and "Cancelar". Below the dialog box, the word "Autenticar" is written in a larger font.

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.



The screenshot shows the BitDefender Antivirus 2009 interface. At the top, there's a title bar with "BitDefender Antivirus 2009 - Evaluación" and buttons for "CONFIGURACIÓN" and "CAMBIAR A VISTA AVANZADA". Below the title bar, a red status bar indicates "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. The main interface is divided into several sections: "VISUALIZADOR", "ANTIVIRUS ADVERTENCIA CRITICA", "ANTIPIHISHING PROTEGIDO", "VULNERABILIDAD PROTEGIDO", and "RED". The "RED" section is active, showing a network map with a globe icon and the IP address "10.10.0.1". A context menu is open over the network map, listing actions: "Registrar este equipo (con un número de licencia)", "Establecer la contraseña de configuración", "Ejecutar una tarea de Análisis", "Reparar incidencias de este equipo", "Ver historial de este equipo", "Iniciar una Actualización en este equipo", and "Establecer como Servidor de Actualizaciones de esta Red". On the right side, there's a "Tareas" section with buttons for "Abandonar Red", "Añadir Equipo", "Analizar Todos", "Actualizar Todos", and "Registrar Todos". At the bottom, there's a footer with the BitDefender logo and links for "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", and "Historial".

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:

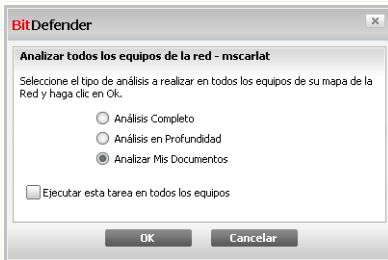
1. Haga clic en **Analizar Todos**. Se le solicitará introducir la contraseña de administración de red local.

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.



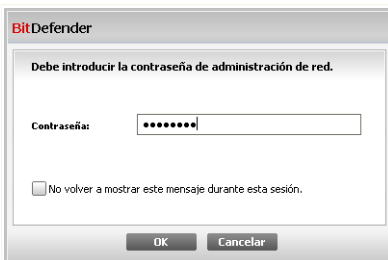
Selección del Tipo de Análisis

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.

BitDefender

Debe introducir la contraseña de administración de red.

Contraseña:

No volver a mostrar este mensaje durante esta sesión.

OK Cancelar

**Introducir Contraseña**

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

BitDefender

Registrar el equipo - mscarlat

Introduzca el número de licencia con el que desea registrarlo

Número de licencia:

Ejecutar esta tarea en todos los equipos

OK Cancelar

**Registrar Todos**

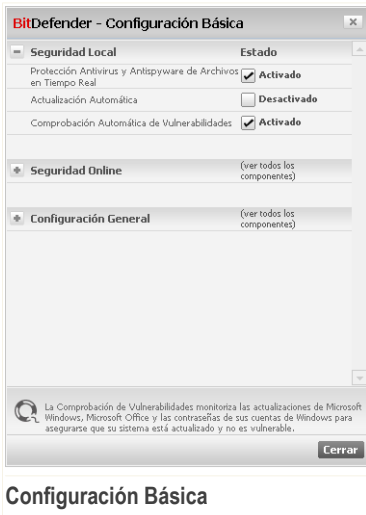
3. Haga clic en **Aceptar**.



## 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
<b>Seguridad Local</b>	Desde aquí puede activar / desactivar la protección de archivos en tiempo real o la actualización automática.
<b>Seguridad Online</b>	Desde aquí puede activar / desactivar la protección en tiempo real del correo y web.
<b>Configuración General</b>	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.

<b>Módulo seguridad</b>	<b>de</b>	<b>Descripción</b>
<b>Protección Antivirus y Antispyware de Archivos en Tiempo Real</b>		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.
<b>Actualización Automática</b>		La Actualización Automática asegura que los archivos y firmas de virus más recientes de BitDefender se descarguen e instalen automáticamente de forma regular.
<b>Comprobación Automática de Vulnerabilidades</b>		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.

<b>Módulo seguridad</b>	<b>de</b>	<b>Descripción</b>
<b>Protección Antiphishing Web en Tiempo Real</b>		La Protección Antiphishing Web en Tiempo Real analiza todos los archivos descargados vía HTTP en busca de tentativas de phishing.
<b>Control de Identidad</b>		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.
<b>Cifrado de IM</b>		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 General

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

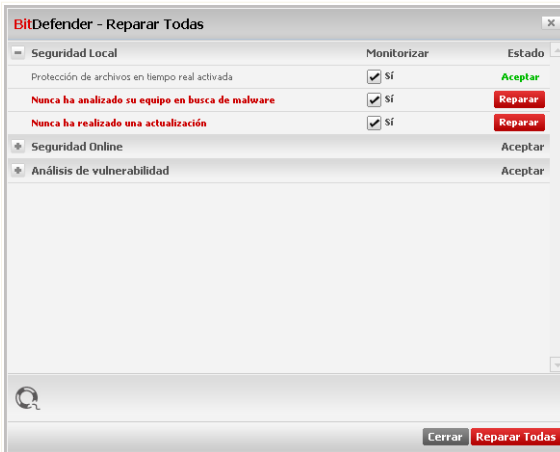
<b>Elemento</b>	<b>Descripción</b>
<b>Modo Trabajo</b>	El Modo Trabajo modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
<b>Modo Portátil</b>	El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.
<b>Contraseña de la Configuración</b>	Al activar esta opción, protegerá la configuración de BitDefender de modo que sólo pueda modificarla la persona que conozca la contraseña.
<b>BitDefender News</b>	Active esta opción si desea recibir noticias importantes sobre BitDefender, las actualizaciones del producto y las nuevas amenazas de seguridad.
<b>Alertas de Notificación del Producto</b>	Al activar esta opción, recibirá alertas de información sobre la actividad del producto.
<b>Barra de Actividad del Análisis</b>	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.
<b>Cargar BitDefender al iniciar Windows</b>	Al activar esta opción, la interfaz de BitDefender se cargará al iniciar el sistema. Esta opción no afecta al nivel de protección.
<b>Enviar Informes de Virus</b>	Al activar esta opción, enviará informes de análisis virus 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.
<b>Detección de Epidemias</b>	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 Antivirus 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 Antivirus 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 Antivirus 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**.

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

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**.



<b><i>Incidencia</i></b>	<b><i>Descripción</i></b>
<b>Cifrado de conversaciones de IM activado</b>	Si sus contactos de mensajería tienen instalado BitDefender 2009, se cifrarán todas las conversaciones de Yahoo! Messenger y Windows Live Messenger. Recomendamos mantener activado el Cifrado de conversaciones de IM para asegurarse la privacidad de sus conversaciones por mensajería.
<b>Antiphishing activado para Mozilla Firefox</b>	BitDefender le protege contra los intentos de phishing mientras navega por Internet.
<b>Antiphishing activado para Internet Explorer</b>	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. 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**.

<b><i>Incidencia</i></b>	<b><i>Descripción</i></b>
<b>Comprobación de Vulnerabilidades activada</b>	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.



<i><b>Incidencia</b></i>	<i><b>Descripción</b></i>
<b>Actualizaciones Críticas de Microsoft</b>	Instala las actualizaciones críticas de Microsoft disponibles.
<b>Otras actualizaciones de Microsoft</b>	Instala las actualizaciones no-críticas de Microsoft disponibles.
<b>Actualizaciones Automáticas de Windows activadas</b>	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.
<b>Admin (Contraseña Segura)</b>	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 Antivirus 2009 incluye un periodo de evaluación de 30 días. Si desea registrar BitDefender Antivirus 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 Antivirus 2009

**BitDefender Antivirus 2009**

Asistente de Registro

Paso 1

Por favor, siga las instrucciones para registrar su producto BitDefender:

El estado de su licencia de BitDefender es: **Evaluación**  
Su número de licencia de BitDefender es: **704BE277EF7785580DF8**  
Este número de licencia caducará en: **30 días**

**Opciones de Registro**  
Para conservar la licencia existente, seleccione la primera opción. Para añadir una nueva licencia, seleccione la segunda opción e introduzca el número de licencia.

Seguir utilizando la licencia actual  
 Quiero registrar el producto con un nuevo número de licencia  
Introduzca un nuevo número de licencia:

**Comprar un número de licencia**  
Si desea comprar una licencia BitDefender, visite nuestra tienda online en:  
**Renueve su número de licencia de BitDefender**

**Puede encontrar su número de licencia en:**

- 1) La etiqueta del CD-Rom
- 2) La tarjeta de licencia del producto
- 3) El correo de confirmación de compra online

Finalizar Cancelar

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 Antivirus 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.

Nombre acción	Acción Realizada	Fecha y hora
Protección en tiempo real	Activado	8/20/2008 4:17:21 PM
Análisis de Comportamie...	Activado	8/20/2008 4:17:21 PM
Protección en tiempo real	Desactivado	8/20/2008 4:17:12 PM
Protección en tiempo real	Activado	8/20/2008 4:11:57 PM
Protección en tiempo real	Desactivado	8/20/2008 4:07:29 PM
Protección en tiempo real	Activado	8/20/2008 3:57:09 PM
Protección en tiempo real	Desactivado	8/20/2008 3:57:02 PM
Protección en tiempo real	Activado	8/20/2008 3:56:25 PM
Protección en tiempo real	Desactivado	8/20/2008 3:56:16 PM

Nombre acción	Nombre de la tarea	Fecha y hora
Análisis finalizado.	742	8/20/2008 4:09:31 PM
Análisis finalizado.	742	8/20/2008 4:09:04 PM
Análisis finalizado.	742	8/20/2008 4:08:40 PM
Análisis finalizado.	742	8/20/2008 4:08:10 PM
Análisis cancelado.	Análisis Manual	8/20/2008 4:05:52 PM
Análisis cancelado.	Asistente de Exclusio...	8/20/2008 4:03:00 PM
Análisis cancelado.	Mis Documentos	8/20/2008 4:00:04 PM
Análisis cancelado.	Análisis Rápido del Sis...	8/20/2008 3:59:56 PM
Análisis cancelado.	Análisis Completo	8/20/2008 3:59:49 PM

### Eventos

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

- **Antivirus**
- **Control de Privacidad**
- **Actualización**
- **Red**



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

The screenshot shows the BitDefender Antivirus 2009 - Evaluación interface. At the top, there is a status bar with a red background indicating "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this, there are tabs for "Visualizador", "Configuración", and "SysInfo". The "Visualizador" tab is active, showing a "General" sidebar on the left with options like "Antivirus", "Control de Privacidad", "Vulnerabilidad", "Cifrado", "Modo Juego/Portátil", "Red", "Actualizar", and "Registro". The main content area is divided into three sections: "Estadísticas" with a table of metrics, "General" with account information, and "Actividad de los Archivos" with a bar chart. The "Estadísticas" table shows 598 files analyzed, 0 disinfectated files, 0 detected viruses, and the last analysis was "Nunca". The "General" section shows the last update was "Nunca", the account is "testare.automata@live.com", and the registration status is "Evaluación" with a green progress bar and a 30-day validity period. The "Actividad de los Archivos" section contains a bar chart with a single bar. At the bottom, there is a footer with the BitDefender logo and navigation links: "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", and "Historial".

Estadísticas	
Archivos analizados:	598
Archivos desinfectados:	0
Virus detectados:	0
Último análisis:	Nunca
Próximo análisis:	Nunca

General	
Última actualización:	Nunca
Mi Cuenta:	testare.automata@live.com
Registro:	Evaluación
Caduca en:	30 días

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.

### 14.1.1. Estadísticas

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

<i>Elemento</i>	<i>Descripción</i>
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.

### 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.

<i>Elemento</i>	<i>Descripción</i>
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.



Elemento	Descripción
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** - permite 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.



### Importante

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

- **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.

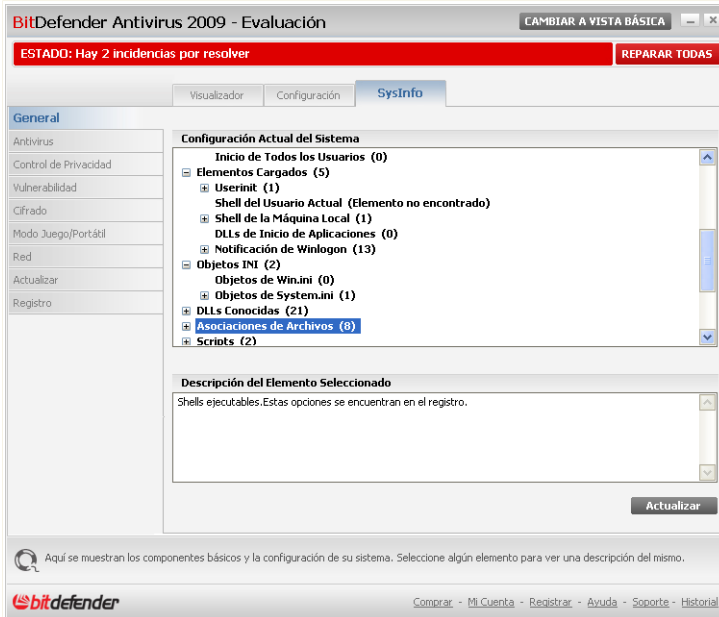
- **Activar la Detección de Epidemias** - envía informes acerca de las posibles epidemias de virus a los Laboratorios de BitDefender.

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:



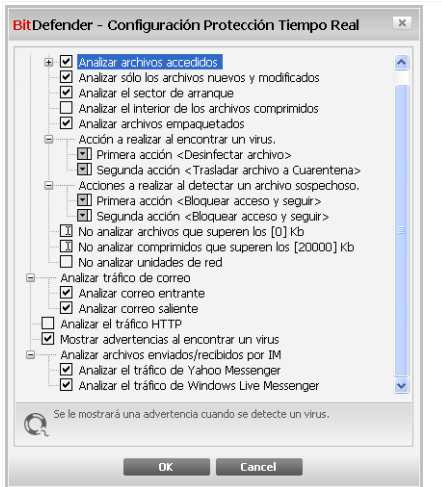
<b>Nivel de Protección</b>	<b>Descripción</b>
<b>Tolerante</b>	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo.  Los programas y mensajes entrantes se analizan sólo en busca de virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se detectan archivos infectados son las siguientes: desinfectar archivo/bloquear acceso.
<b>Por Defecto</b>	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.
<b>Agresivo</b>	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	<b>Analizar todos los archivos</b>	Se analizarán todos los archivos, independientemente de su tipo.
	<b>Analizar sólo programas</b>	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.
<b>Analizar extensiones definidas</b>	Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ",".
<b>Analizar en busca de software de riesgo</b>	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 <b>Omitir dialers y aplicaciones en el análisis</b> si quiere excluir este tipo de archivos del análisis.
<b>Analizar el sector de arranque</b>	Para analizar el sector de arranque del sistema.
<b>Analizar el interior de los archivos comprimidos</b>	Para analizar el contenido de los archivos comprimidos. Con esta opción activada su ordenador puede ralentizarse un poco.
<b>Analizar archivos empaquetados</b>	Para analizar todos los archivos empaquetados.
<b>Primera acción</b>	En el menú desplegable, seleccione la primera acción que desea realizar al encontrar archivos infectados o sospechosos.
<b>Bloquear acceso y seguir</b>	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
<b>Desinfectar archivo</b>	Desinfecta los archivos infectados.



Opción	Descripción
<b>Eliminar archivo</b>	Elimina los archivos infectados inmediatamente y sin previa advertencia.
<b>Mover archivo a la cuarentena</b>	Para trasladar los archivos infectados a la cuarentena.
<b>Segunda acción</b>	En el menú desplegable, seleccione la segunda acción que desea realizar al encontrar archivos infectados o sospechosos, en caso que falle la primera acción.
<b>Bloquear acceso y seguir</b>	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
<b>Eliminar archivo</b>	Elimina los archivos infectados inmediatamente y sin previa advertencia.
<b>Mover archivo a la cuarentena</b>	Para trasladar los archivos infectados a la cuarentena.
<b>No analizar archivos que superen los [x] Kb</b>	Introduzca el tamaño máximo de los archivos a analizar. Si el tamaño es 0 Kb, se analizarán todos los archivos, independientemente de su tamaño.
<b>No analizar comprimidos que superen los [20000] Kb</b>	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.
<b>No analizar unidades de red</b>	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.

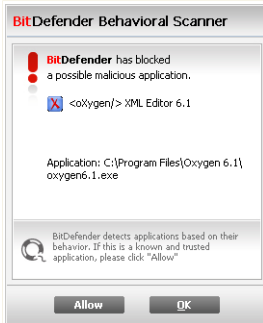
- **Analizar archivos enviados/recibidos por IM.** Para analizar los archivos que reciba o envíe a través de Yahoo Messenger o Windows Live Messenger, seleccione la casilla correspondiente.

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.

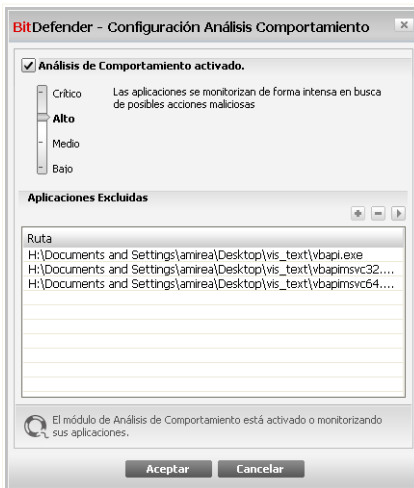


## Alerta del Análisis de Comportamiento

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
<b>Crítico</b>	Las aplicaciones se monitorizan de forma muy estricta en busca de posibles acciones maliciosas.
<b>Alto</b>	Las aplicaciones se monitorizan de forma intensa en busca de posibles acciones maliciosas.
<b>Mediana</b>	Las aplicaciones se monitorizan de forma moderada en busca de posibles acciones maliciosas.
<b>Bajo</b>	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:

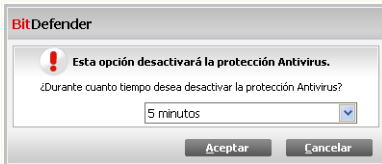
- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.



-  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, dirjase al apartado **Antivirus > Análisis** en la Vista Avanzada.

BitDefender Antivirus 2009 - Evaluación

ESTADO: Hay 2 incidencias por resolver

REPARAR TODAS

Resistente **Análisis** Exclusiones Cuarentena

General

**Antivirus**

Control de Privacidad

Vulnerabilidad

Cifrado

Modo Juego/Portátil

Red

Actualizar

Registro

**Tareas del sistema**

- Análisis en Profundidad**  
Última Ejecución: 8/20/2008 3:57:11 PM
- Análisis Completo**  
Última Ejecución: Nunca
- Análisis Rápido del Sistema**  
Última Ejecución: Nunca
- Análisis del Autologon**  
Última Ejecución: 5/9/2008 7:16:42 PM

**Tareas del usuario**

- Mis Documentos**  
Última Ejecución: Nunca

**Otras tareas**

- Análisis Contextual**
- Detección de Dispositivos**

Nueva Tarea Ejecutar Tareas

Haga clic para crear una nueva tarea, acorde con sus necesidades.

bitdefender

Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial

## 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. 116).

Existen 3 tipos de tareas de análisis:

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

<b>Tarea Predeterminada</b>	<b>Descripción</b>
<b>Análisis en Profundidad</b>	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.
<b>Análisis Completo de Sistema</b>	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.
<b>Análisis Rápido del Sistema</b>	Analiza las carpetas <code>Windows</code> , <code>Archivos de Programa</code> y <code>All Users</code> . 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.
<b>Análisis del Autologon</b>	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

The screenshot shows the BitDefender Antivirus 2009 interface. At the top, it says "BitDefender Antivirus 2009 - Evaluación" and "ESTADO: Hay 2 incidencias por resolver". The main area is divided into "Tareas del sistema" and "Tareas del usuario". Under "Tareas del sistema", there are four tasks: "Análisis en Profundidad", "Análisis Completo", "Análisis Rápido del Sistema", and "Análisis del Autologon". Under "Tareas del usuario", there is "Mis Documentos". A context menu is open over the "Análisis en Profundidad" task, showing options: "Analizar", "Rutas", "Programador", "Logs", "Clonar", "Eliminar", and "Abrir".

**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**).



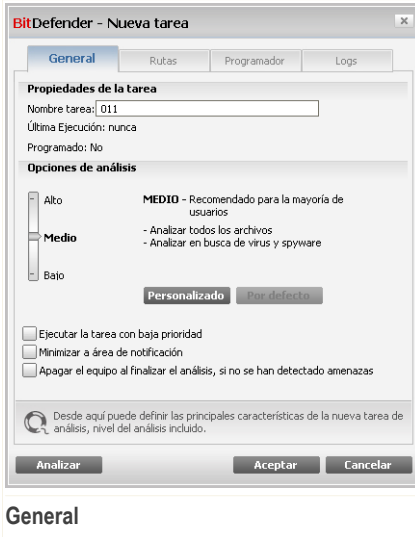
**Nota**

Para más detalles acerca del módulo **Informes**, consulte "**Viendo los Informes del Análisis**" (p. 135).



## 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:



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.



<b>Nivel de Protección</b>	<b>Descripción</b>
	Sólo los programas se analizan en busca de virus. Además del clásico análisis basado en firmas de virus, se usa también el análisis heurístico.
<b>Mediana</b>	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 firmas de virus, se usa también el análisis heurístico.
<b>Alto</b>	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 firmas de virus, se usa también el análisis heurístico.

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

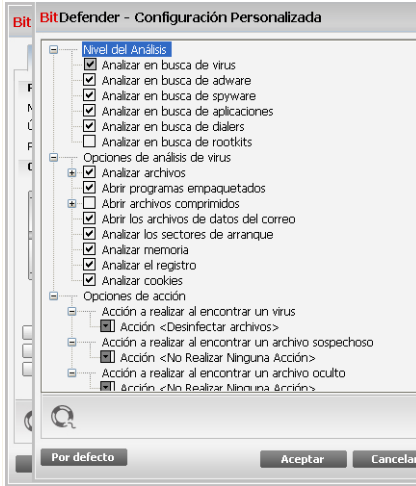
- **Ejecutar el análisis con prioridad baja.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
- **Minimizar ventana de análisis a la barra de tareas.** Minimiza la ventana de análisis 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
<b>Analizar en busca de virus</b>	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.
<b>Analizar en busca de adware</b>	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
<b>Analizar en busca de spyware</b>	Analiza en busca de spyware. Estos archivos se tratarán como si fuesen archivos infectados.
<b>Analizar en busca de aplicaciones</b>	Analiza en busca de aplicaciones legítimas que pueden utilizarse como herramientas de espionaje, para ocultar aplicaciones maliciosas u otros fines maliciosos.
<b>Analizar en busca de dialers</b>	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.
<b>Analizar en busca de Rootkits</b>	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
<b>Analizar archivos</b>	<b>Analizar todos los archivos</b> Se analizarán todos los archivos, independientemente de su tipo.
	<b>Analizar sólo programas</b> 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.
	<b>A n a l i z a r extensiones definidas</b> Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ",".
<b>Abrir programas empaquetados</b>	Para analizar el interior de los archivos empaquetados.



Opción	Descripción
<b>Abrir archivos comprimidos</b>	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 <b>Límite de tamaño de comprimidos</b> e introduzca el tamaño máximo de los archivos comprimidos a analizar, en kilobytes (KB).
<b>Abrir los archivos comprimidos adjuntos en el correo</b>	Para analizar el interior de los archivos comprimidos del correo electrónico.
<b>Analizar los sectores de arranque</b>	Para analizar el sector de arranque del sistema.
<b>Analizar memoria</b>	Analiza la memoria en busca de virus y otros tipos de malware.
<b>Analizar registro</b>	Analiza las entradas del registro.
<b>Analizar cookies</b>	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**.

**1** *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
<b>Ninguno(mostrar objetos)</b>	No se realizará ninguna acción con los archivos infectados. Estos archivos aparecerán en el informe de análisis.
<b>Desinfectar archivos</b>	Elimina el código de malware de los archivos infectados detectados.



<b>Acción</b>	<b>Descripción</b>
<b>Eliminar archivos</b>	Elimina los archivos infectados inmediatamente y sin previa advertencia.
<b>Mover a la Cuarentena</b>	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:

<b>Acción</b>	<b>Descripción</b>
<b>Ninguno(mostrar objetos)</b>	No se realizará ninguna acción con los archivos sospechosos. Estos archivos aparecerán en el informe de análisis.
<b>Eliminar archivos</b>	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
<b>Mover a la Cuarentena</b>	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:

<b>Acción</b>	<b>Descripción</b>
<b>Ninguno(mostrar objetos)</b>	No se realizará ninguna acción con los archivos ocultos. Estos archivos aparecerán en el informe de análisis.
<b>Mover a la Cuarentena</b>	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.
<b>Hacer visible</b>	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
<b>No Realizar Ninguna Acción</b>	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.
<b>Desinfectar archivos</b>	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.
<b>Eliminar archivos</b>	Elimina de forma inmediata los archivos infectados, sin mostrar advertencia alguna.
<b>Mover a la Cuarentena</b>	Traslada los archivos infectados de su ubicación original a la <b>carpeta de la cuarentena</b> . 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:



<b>Acción</b>	<b>Descripción</b>
<b>No Realizar Ninguna Acción</b>	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.
<b>Eliminar archivos</b>	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
<b>Mover a la Cuarentena</b>	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:

<b>Acción</b>	<b>Descripción</b>
<b>Registrar como no analizado</b>	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.
<b>Solicitar contraseña</b>	Al detectar un archivo comprimido protegido con contraseña, solicitará la contraseña al usuario para poder analizar el contenido del archivo.



**Nota**

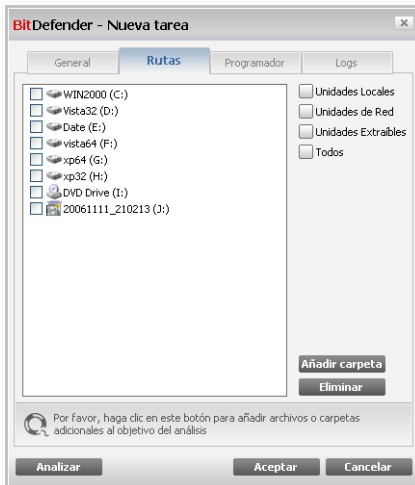
Si decide ignorar los archivos infectados o la acción elegida falla, debería elegir una nueva acción en el Asistente de Análisis.

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 extraíbles, 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**

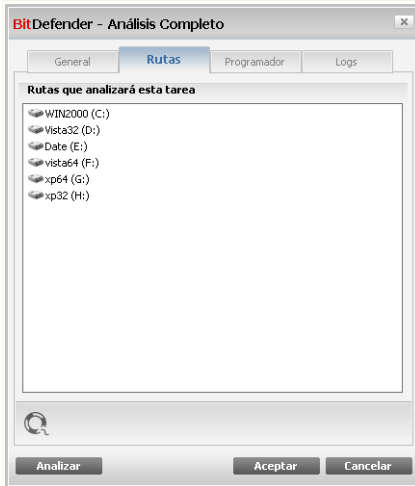
Si desea analizar todo el sistema en busca de virus, seleccione la casilla correspondiente a **Todas las unidades**.

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

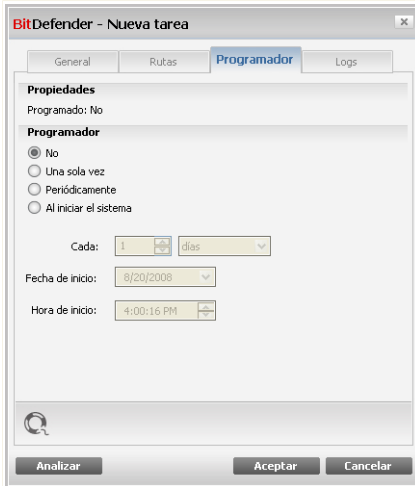
Las tareas **Análisis Completo** y **Análisis en Profundidad** analizarán todas las unidades locales, mientras que la tarea **Análisis Rápido del Sistema** sólo analizará las carpetas **Windows** y **Archivos de Programa**.

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 tipos 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 inmediato.

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. 131).



## 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

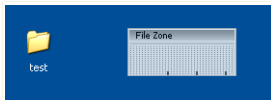
Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **BitDefender Antivirus 2009**.

Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado *“Analizador de BitDefender”* (p. 131).

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. 131).



## Análisis Manual

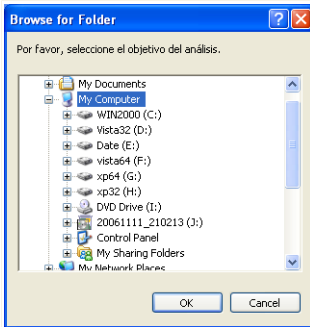
El análisis manual consiste en seleccionar directamente los objetos a analizar con la opción de Análisis Manual de BitDefender desde la carpeta de BitDefender en el menú Inicio.



### 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. 131).

## 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.



**BitDefender 2009 - Análisis en Profundidad**

Análisis Antivirus - Paso 1 de 3

Paso 1 | Paso 2 | Paso 3

**Estado del Análisis**

**Analizando Elemento:** =>HKEY\_LOCAL\_MACHINE\SYSTEM\CURRE...FENDER\BITDEFENDER\_FIREWALL\BDFIREWALL.TXT

**Tiempo Transcurrido:** 00:00:01

**Archivos/Segundo:** 30

**Estadísticas del Análisis**

<b>Elementos Analizados:</b>	30
<b>Elementos No Analizados:</b>	0
<b>Elementos Infectados:</b>	0
<b>Elementos Sospechosos:</b>	0
<b>Elementos Ocultos:</b>	0
<b>Procesos Ocultos:</b>	0

Análisis de virus en curso. En el apartado superior se indica el progreso y estadísticas del análisis. BitDefender intentará desinfectar los elementos infectados de forma predeterminada.

**bitdefender** [Pausa] [Parar] [Cancelar]

**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 complejidad 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.



BitDefender 2009 - 742

Análisis Antivirus - Paso 2 de 3

Paso 1 Paso 2 Paso 3

Resumen de los Resultados

1 amenaza(s) que afecta(n) 1 objeto(s) requiere(n) su atención [No realizar ninguna a](#)

EICAR-Test-File (not a virus) 1 incidencia restante (desinfección fallida) [No realizar ninguna a](#)

Contador de incidencias resueltas: 1

Ruta del archivo	Nombre de la amenaza	Resultado de la acción
H:\Documents and Settings(a...rea)\Desktop\av_testbed\3.vir	Win32.Parite.C	desinfectado

Esta es la acción que BitDefender ha realizado con la amenaza detectada

[Continuar](#)

**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
<b>Ninguna Acción</b>	No se realizará ninguna acción sobre los archivos detectados.
<b>Desinfectar</b>	Desinfecta los archivos infectados.
<b>Eliminar</b>	Elimina los archivos detectados.
<b>Hacer visible</b>	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.

BitDefender 2009 - 742

Análisis Antivirus - Paso 3 de 3

	Paso1	Paso2	Paso3
<b>Resumen de los Resultados</b>			
Elementos Resueltos:	1		
Elementos No Resueltos:	1		
Elem. con Contraseña:	0		
Elementos Omitidos:	0		
Elementos Fallidos:	1		

1 archivo no ha podido desinfectarse, su sistema NO está libre de virus. Más detalles en: [www.bitdefender.es](http://www.bitdefender.es)

El número de elementos cuyo análisis no ha podido completarse

bitdefender

Mostrar Informe Cerrar

### 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](http://www.bitdefender.es). Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

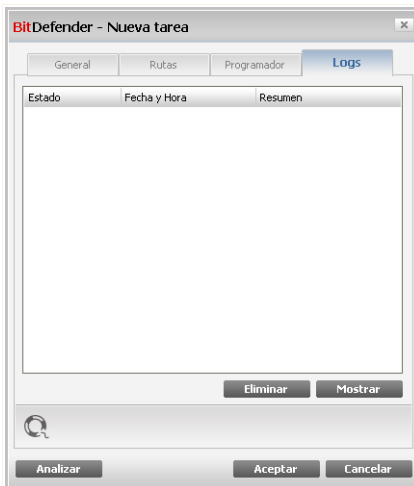
## Objetos Sospechosos Detectados por BitDefender

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.



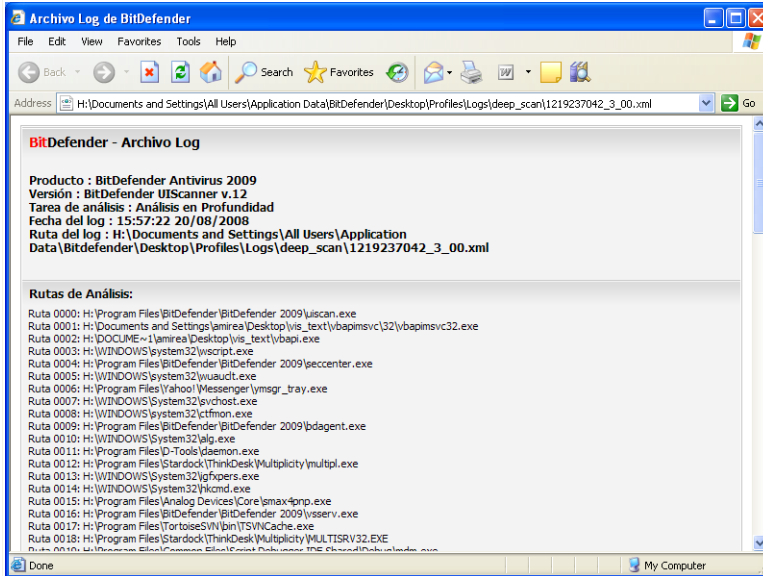
### **Nota**

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, dirijase al apartado **Antivirus > Excepciones** en la Vista Avanzada.

BitDefender Antivirus 2009 - Evaluación CAMBIAR A VISTA BÁSICA

**ESTADO: Hay 2 incidencias por resolver** REPARAR TODAS

Residente    Análisis    **Excepciones**    Cuarentena

General

**Antivirus**

Control de Privacidad

Vulnerabilidad

Cifrado

Modo Juego/Portátil

Red

Actualizar

Registro

**Excepciones activadas**

Elementos excluidos del análisis	Tiempo Real	Bajo Demanda
Archivos y carpetas		
c:\	Sí	Sí
Extensiones		
*.zip (Archivo Comprimido)	Sí	Sí

Aplicar    Descartar

Haga clic aquí para aplicar los últimos cambios

**bitdefender** Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial

## 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

**BitDefender Total Security 2009**

Asistente de Exclusiones - Paso 2 de 4

Excluir rutas

Por favor, introduzca la ruta a omitir del análisis

Explorar Añadir

Rutas seleccionadas

c:\

Arriba puede seleccionar las rutas que desee excluir del análisis. Recuerde que debe hacer clic en Añadir tras seleccionar la ruta (archivo o carpeta). Puede añadir múltiples elementos a la lista.

Por favor, seleccione las excepciones del proceso de análisis con cuidado y recuerde que para asegurarse que su sistema está totalmente protegido, no es recomendable crear excepciones

bitdefender Atrás Siguiente Cancelar

**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

**BitDefender Total Security 2009**

Asistente de Exclusiones - Paso 3 de 4

Paso 1	Paso 2	Paso 3	Paso 4
--------	--------	--------	--------

**Cuando aplicar**

Por favor, elija el tipo de análisis que desea aplicar a las excepciones seleccionadas: bajo demanda, en tiempo real o ambos. Haga clic en el texto situado en la columna de la derecha, junto a cada celda, y seleccione la opción que mejor se adapte a sus necesidades.

Objetos seleccionados	Cuando aplicar
c:\	Ambos

Por favor, seleccione las excepciones del proceso de análisis con cuidado y recuerde que para asegurarse que su sistema está totalmente protegido, no es recomendable crear excepciones

**bitdefender**      Atrás      Siguiente      Cancelar

**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**.

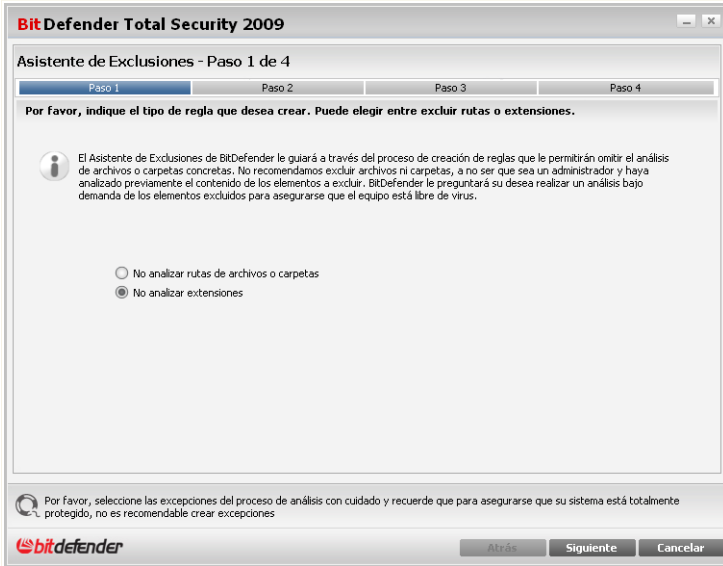
Haga clic en **Aplicar** para guardar los cambios.

## 15.3.2. Excluyendo Extensiones del Análisis

Para excluir extensiones del análisis, 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

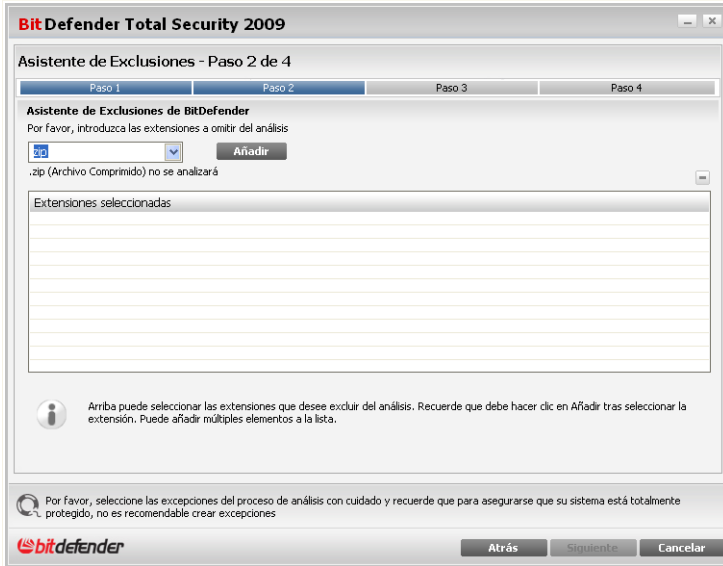


### Tipo de Objeto

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**.

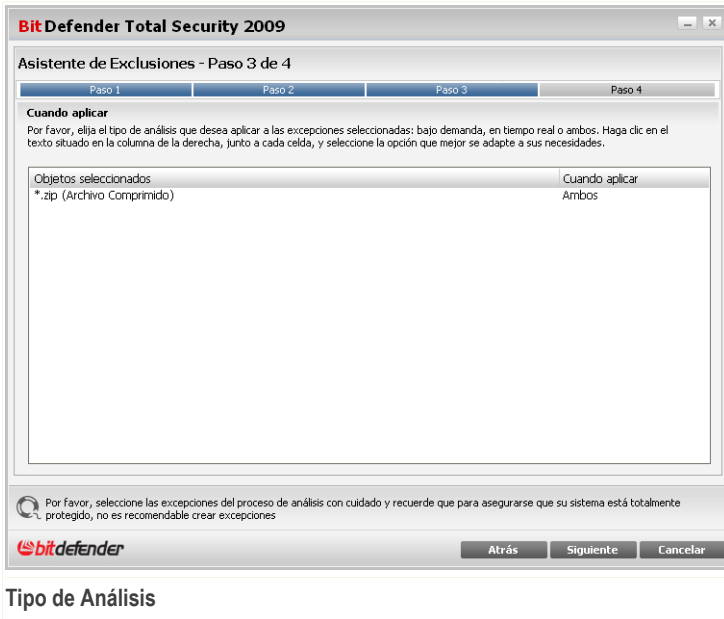
Las extensiones aparecerán en la tabla a medida que las vaya añadiendo. Puede añadir tantas extensiones como desee.

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



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 Cuarentena

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.

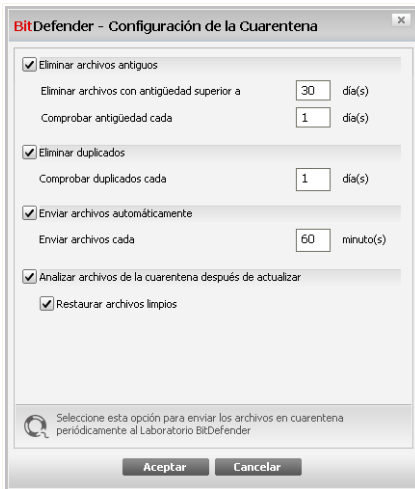




**Menú contextual.** A través del menú contextual podrá gestionar los archivos de la cuarentena fácilmente. También puede seleccionar **Actualizar** para actualizar el apartado de Cuarentena.

## 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. 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 envíen información personal (como números de tarjetas de crédito) desde su equipo hacia el hacker.

### 16.1. 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.

The screenshot shows the BitDefender Antivirus 2009 - Evaluación interface. At the top, there is a red status bar that reads "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this, there are tabs for "Estado", "Identidad", "Registro", "Cookie", and "Script". The "Estado" tab is selected, showing a section for "Control de privacidad general" with a checked box for "Control de privacidad activado" and "Control de Identidad desactivado". Underneath, there is a "Nivel de protección" section with a slider set to "Tolerante" and a list of settings: "Identidad control desactivado", "Registro control desactivado", "Cookie control desactivado", and "Script control desactivado". There are buttons for "Personalizado" and "Por Defecto". At the bottom, there is a section for "Estadísticas del Control de Privacidad" with a table showing 0 for all categories: "Información privada bloqueada", "Registro bloqueados", "Cookies bloqueadas", and "Scripts bloqueados". A footer note states that the Privacy Protection module is disabled and provides instructions to activate it. The BitDefender logo and navigation links are at the bottom.

Estadísticas del Control de Privacidad	
Información privada bloqueada:	0
Registro bloqueados:	0
Cookies bloqueadas:	0
Scripts bloqueados:	0



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**.

### 16.1.1. 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:

<b>Nivel de Protección</b>	<b>Descripción</b>
<b>Tolerante</b>	Sólo el <b>Control del Registro</b> está activado.
<b>Por Defecto</b>	El <b>Control del Registro</b> y <b>Control de Identidad</b> están activados.
<b>Agresivo</b>	El <b>Control del Registro</b> , el <b>Control de Identidad</b> y el <b>Control de Scripts</b> 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.

## 16.2. 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.

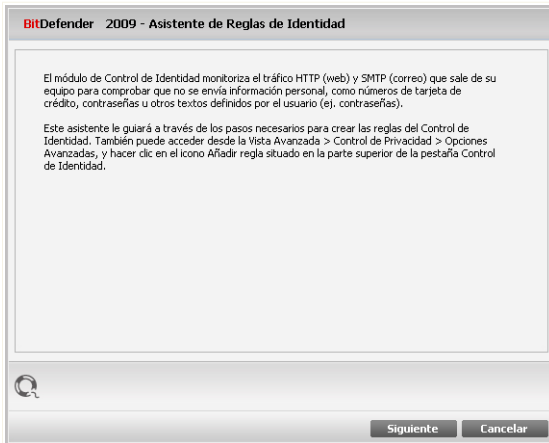
Si configura las reglas de protección de la identidad adecuadas, no podrá enviar información personal (como el número de su tarjeta de crédito) a través de una página web, a menos que la haya definido explícitamente como excepción a las reglas.

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





## Paso 1/4 - Ventana de Bienvenida



### Ventana de Bienvenida

Haga clic en **Siguiente**.



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

BitDefender 2009 - Asistente de Reglas de Identidad

Nombre de la Regla

Tipo de Regla

Datos de la Regla

La información personal está cifrada y nadie, excepto usted, podrá utilizarla. Para mayor seguridad, por favor, introduzca sólo parte de la información que debemos proteger (Ejemplo: si desea filtrar el tráfico para la dirección john.doe@example.com, incluya sólo en la cadena de texto.)

Introduzca el nombre de la regla aquí

Atrás Siguiente Cancelar

### 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

**BitDefender 2009 - Asistente de Reglas de Identidad**

Analizar HTTP  
 Analizar SMTP  
 Analizar Mensajería Instantánea  
 Coincidir sólo palabras completas  
 Mayúsculas y Minúsculas

Tráfico HTTP (web) y Tráfico IM (messenger) que contenga su información personal será bloqueado.

Marque esta casilla para activar el análisis del tráfico HTTP

Atrás   Siguiente   Cancelar

### 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

BitDefender 2009 - Asistente de Reglas de Identidad

Descripción de la regla

Introduzca una descripción para esta regla. La descripción debería ayudarle a vd. o a otros administradores a identificar más fácilmente que información se ha bloqueado.

Introduzca la descripción de la regla aquí

Atrás Finalizar Cancelar

### Describa la regla

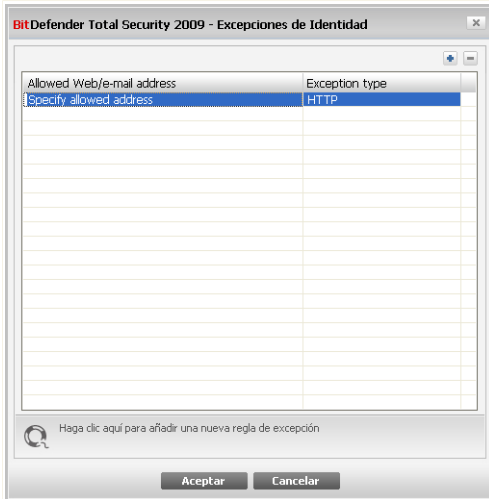
Introduzca una breve descripción de la regla en el campo editable. Como los datos bloqueados (las cadena de texto) no se muestran en texto plano cuando accede a la regla, es importante introducir una breve descripción que le ayude a identificar fácilmente los datos que protege.

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

## 16.2.2. 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.

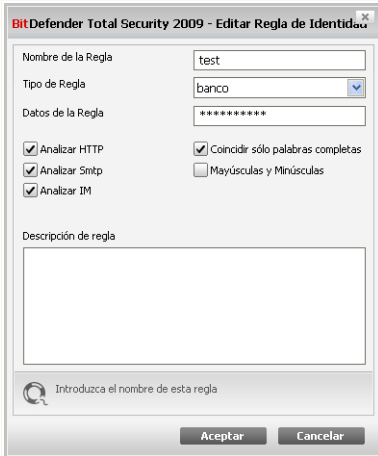
## 16.2.3. Administrando Reglas

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

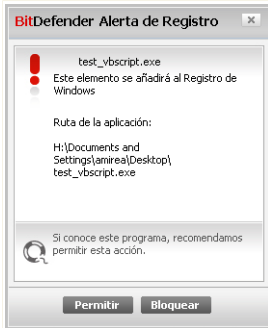
Aquí puede cambiar el nombre, la descripción y los parámetros de la regla (tipo, datos y tráfico). Haga clic en **Aceptar** para guardar los cambios.

## 16.3. 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

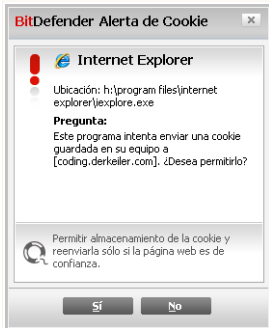
Generalmente, BitDefender le mostrará alertas cuando instale nuevos programas que necesitan iniciarse la próxima vez que reinicie el equipo. En la mayoría de los casos, estos programas son legítimos y de confianza.

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





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 **Sí** 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.

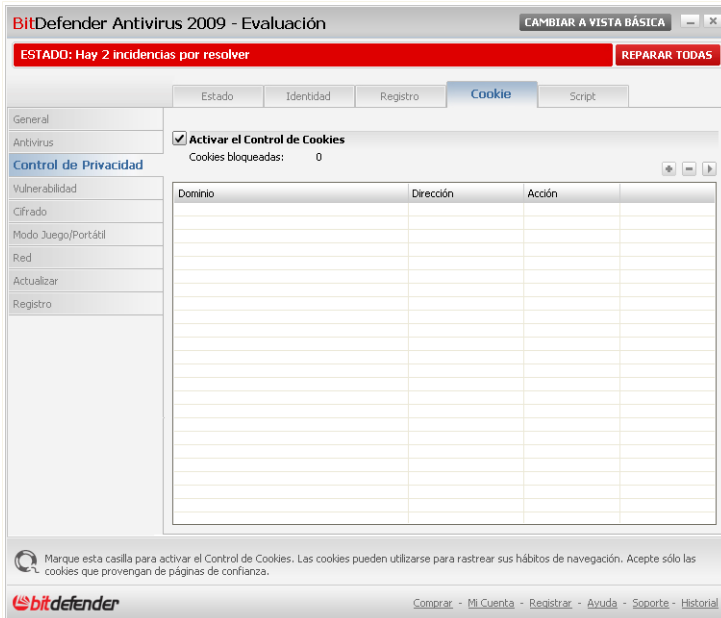
Esto le ayudará a decidir cuáles son los sitios web de confianza y cuáles no.



### 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.

## 16.4.1. 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.

<i>Acción</i>	<i>Descripción</i>
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

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

<i>Tipo</i>	<i>Descripción</i>
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**.

## 16.5. 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:

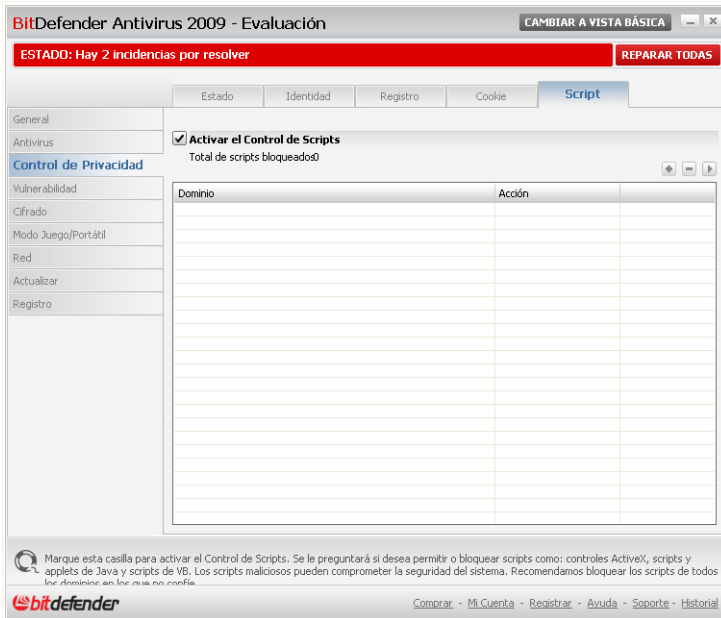


**Alerta de Script**

Puede ver el nombre del recurso.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Sí** 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.

## 16.5.1. 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.

<i>Acción</i>	<i>Descripción</i>
<b>Permitir</b>	La aplicación será permitida.
<b>Bloquear</b>	La aplicación será bloqueada.

Haga clic en **Finalizar**.



## 17. 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, dirijase 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. 35) de esta guía.



The screenshot shows the BitDefender Antivirus 2009 - Evaluación interface. At the top, there is a red status bar indicating 'ESTADO: Hay 2 incidencias por resolver' and a 'REPARAR TODAS' button. The main window title is 'BitDefender Antivirus 2009 - Evaluación' and there is a 'CAMBIAR A VISTA BÁSICA' button. The left sidebar contains a navigation menu with options: General, Antivirus, Control de Privacidad, Vulnerabilidad, Cifrado (selected), Modo Juego/Portátil, Red, Actualizar, and Registro. The main content area is titled 'Cifrado de IM' and contains the following sections:

- Cifrado de IM desactivado.** This section has three checkboxes:
  - Cifrado de IM desactivado.
  - Cifrado de Yahoo Messenger desactivado.
  - Cifrado de Windows Live (MSN) Messenger desactivado.
- Exclusiones del Cifrado** (with expand/collapse buttons): A table with two columns: 'ID de usuario' and 'Programa de IM'. The table is currently empty.
- Conexiones Actuales** (with expand/collapse buttons): A table with three columns: 'ID de usuario', 'Programa de IM', and 'Estado del Cifrado'. The table is currently empty.

At the bottom of the interface, there is a search icon and the text: 'Desde aquí puede configurar detalladamente el componente de Cifrado de IM.' Below that is the BitDefender logo and a footer with links: 'Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial'.

## 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.

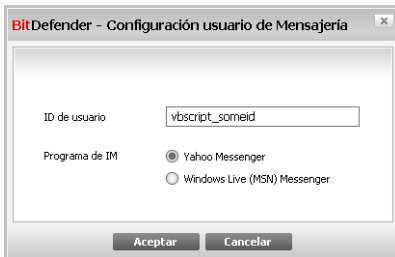


- Su contacto no tiene instalada ninguna versión de BitDefender que soporte el cifrado de IM.

## 17.1. 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**.





**Importante**

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

### 18.1.1. 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

BitDefender Total Security 2009

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6

Seleccionar tareas

Este asistente le guiará a través de las acciones necesarias para identificar aplicaciones no actualizadas y cuentas de Windows con contraseñas inseguras. Por favor, seleccione los elementos a comprobar en busca de vulnerabilidades en la lista de abajo.

- Comprobar Contraseñas de Cuentas de Windows
- Buscar Actualizaciones de Aplicaciones
- Buscar Actualizaciones Críticas de Windows
- Buscar Actualizaciones Opcionales de Windows

Seleccione esta casilla para que BitDefender compruebe las contraseñas de las cuentas de Windows de su equipo. Estas contraseñas deben contener números, letras y símbolos para conseguir una mejor protección de sus cuentas.

bitdefender Siguiente Cancelar

**Vulnerabilidades**

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



## Paso 2/6 - Comprobando Vulnerabilidades



Espere hasta que BitDefender finalice la comprobación de vulnerabilidades.



### Paso 3/6 - Cambie las Contraseñas Inseguras

Usuario	Fortaleza	Estado
Administrator	Strong	Ok
amirea	Strong	Ok

Esta es una lista de las contraseñas de las cuentas de Windows de su equipo y su nivel de protección. Haga clic en el botón 'Reparar' para modificar las contraseñas débiles.

**bitdefender** Siguiente Cancelar

**Contraseñas de los Usuarios**

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

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

**BitDefender**

Choose method to fix:

- Force user to change password at next login
- Change user password

Type password:

Confirm password:

OK Close

**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

BitDefender Total Security 2009

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5 Paso 6

Buscar Actualizaciones de Aplicaciones

Aplicación	Versión Instalada	Última Versión	Estado
Adobe Reader	8.1.2	8.1.2	Actualizado
Yahoo! Messenger	8.1.0.421	8.1.0.241	Actualizado
Firefox	3.0 (en-US)	3.0 (en-US)	Actualizado

Esta es una lista de las aplicaciones soportadas por BitDefender y las actualizaciones disponibles, en caso que existan.

**Siguiente** **Cancelar**

**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

**BitDefender Total Security 2009**

Asistente de Vulnerabilidad de BitDefender

Paso 1 Paso 2 Paso 3 **Paso 4** Paso 5 Paso 6

Actualizaciones de Windows

Buscar Actualizaciones Críticas de Windows

- Security Update for Windows XP (KB901190)
- Security Update for Microsoft XML Core Services 6.0 and Microsoft XML Core Services 6.0 Service Pack 1 (KB933579)
- Microsoft .NET Framework 2.0 Service Pack 1 (KB110906)
- Microsoft .NET Framework 1.1 Service Pack 1
- Security Update for Windows XP (KB950749)
- Update for Windows XP (KB932823)
- Security Update for Windows XP (KB950762)
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB936181)
- Security Update for Windows XP (KB951376)
- Security Update for Windows XP (KB951698)
- Windows XP Service Pack 3 (KB936929)
- Security Update for Windows XP (KB951748)
- Cumulative Security Update for ActiveX Killbits for Windows XP (KB953839)
- Windows Malicious Software Removal Tool - August 2008 (KB890830)
- Security Update for Outlook Express for Windows XP (KB951066)

**Instalar Todas las Actualizaciones del Sistema**

Esta es una lista de las actualizaciones críticas y no críticas de las aplicaciones de Windows

**bitdefender** Siguiente Cancelar

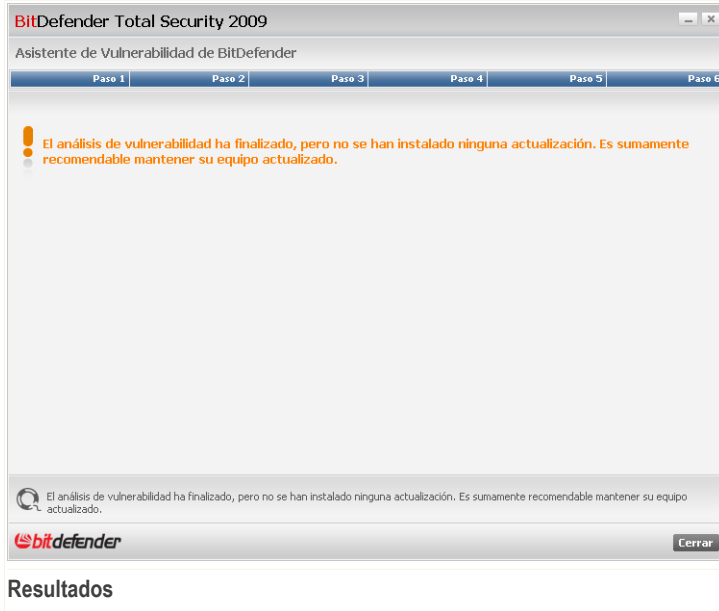
**Actualizaciones de Windows**

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**.



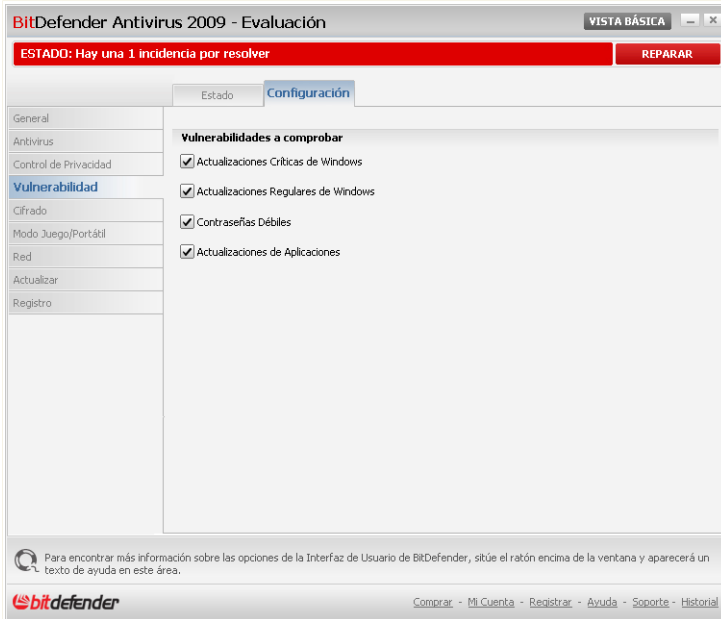
## Paso 6/6 – Ver Resultados



Haga clic en **Cerrar**.

## 18.2. 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.



## 19. 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.

### 19.1. 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**.
- Por defecto, no se realizarán actualizaciones.



#### Nota


Para modificar esta opción, dirijase 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, dirijase al apartado **Modo Trabajo/Portátil > Modo Trabajo** en la Vista Avanzada.

The screenshot shows the BitDefender Antivirus 2009 - Evaluación interface. At the top, there is a red status bar indicating "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this, the "Modo Juego" configuration window is open, showing the "Modo Portátil" tab. The "Estado actual" section shows "Modo Juego desactivado" with an "Activar Modo Juego" button. The "Modo Juego Automático activado" section has three checked options: "Usar la lista predeterminada de juegos de BitDefender" (with an "Administrar Juegos" button), "Activar modo juego al entrar en modo pantalla completa", and "Preguntar si la aplicación debe añadirse a la lista blanca". The "Configuración" section has "Tarea de Análisis" checked, with radio buttons for "Omitir Tarea" (selected) and "Posponer Tarea". A "Opciones Avanzadas" button is also present. At the bottom, there is a note about the game list and a footer with the BitDefender logo and navigation links: "Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial".

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.

## 19.1.1. 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.

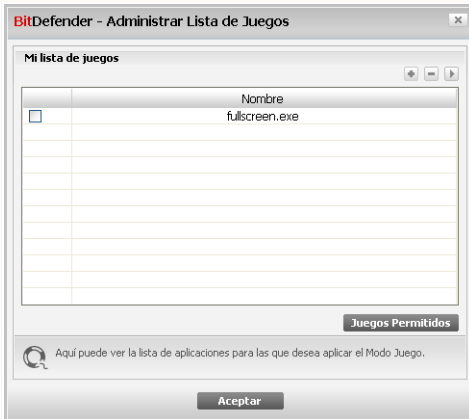


**Nota**

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

### 19.1.2. 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.

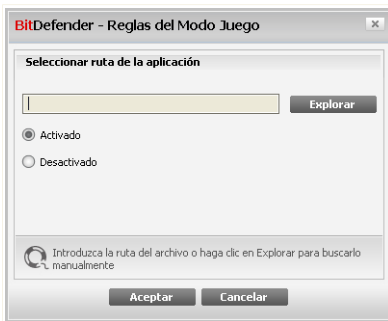
Si desea desactivar el Modo Trabajo Automático para una aplicación concreta de la lista, desmarque su casilla correspondiente. Debe desactivar el Modo Trabajo Automático para aquellas aplicaciones de uso habitual que utilizan el modo pantalla completa, como navegadores web o reproductores de vídeos y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



### 19.1.3. Modificando la Configuración del Modo Trabajo

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

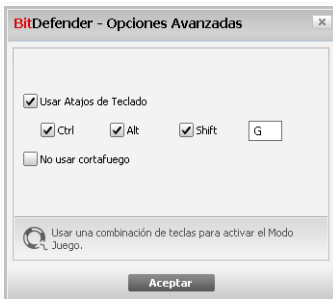
- **Tarea de Análisis** - para impedir que las tareas de análisis programadas se ejecuten mientras el Modo Trabajo está activado. Puede seleccionar una de de las siguientes opciones:

Opción	Descripción
Omitir Tarea	Para no iniciar la tarea programada.
Posponer Tarea	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Trabajo.

### 19.1.4. 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.

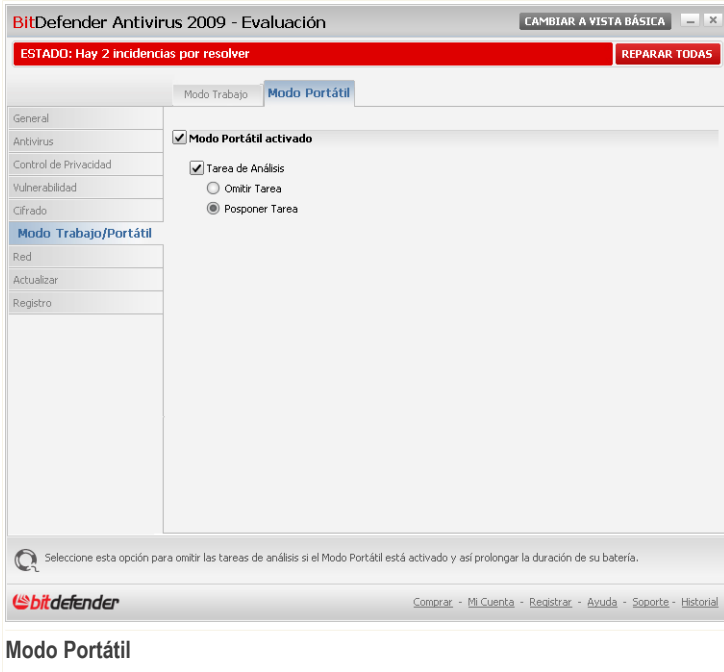
## 19.2. Modo Portátil

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.



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.

### 19.2.1. 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.



<i>Opción</i>	<i>Descripción</i>
<b>Posponer Tarea</b>	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Portátil.



## 20. 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 uno 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.



## 20.1. 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**.

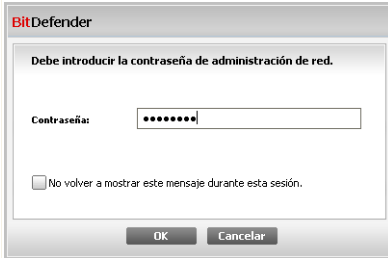
Podrá ver como el nombre del equipo aparece en el mapa de la red.

## 20.2. 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.

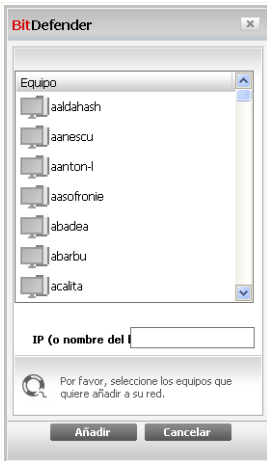
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

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.




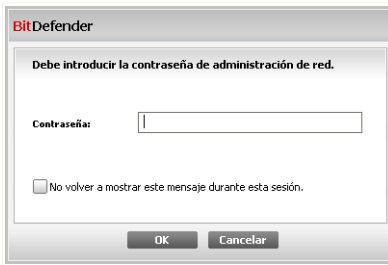
### Añadir Equipo

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.



**Autenticar**

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.

## 20.3. 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.

The screenshot shows a dialog box titled "BitDefender". Inside the dialog, the text reads "Debe introducir la contraseña de administración de red." Below this is a label "Contraseña:" followed by a text input field containing seven dots. At the bottom left, there is a checkbox with the text "No volver a mostrar este mensaje durante esta sesión." At the bottom right, there are two buttons: "OK" and "Cancelar".

**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.



## 21. 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 actualizaciones 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 para los motores antispymware** - se añadirán nuevas firmas de spyware a la base de datos. Esta actualización también es conocida como **Actualización Antispymware**.
- **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**.

### 21.1. Actualización automática

Para ver la información relacionada con las actualizaciones, diríjase al apartado **Actualización > Actualizar** en la Vista Avanzada.



The screenshot shows the BitDefender Antivirus 2009 - Evaluación window. At the top, there is a red status bar that reads "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this, there are tabs for "Actualizar" (selected) and "Configuración". A left sidebar contains various settings categories like "General", "Antivirus", "Control de Privacidad", etc. The main content area is divided into several sections:

- Actualización automática activada:** A checked checkbox. Below it, a table shows "Última comprobación" as "8/20/2008 4:19:35 PM" and "Última actualización" as "Nunca". An "Actualizar" button is to the right.
- Propiedades de las Firmas de Virus:** A table showing "Firmas de Virus" as "1571313" and "Versión del motor" as "7.20597". A "Lista de Virus" button is to the right.
- Estado de la Descarga:** A section titled "Deteniendo actualización" with two progress bars. The first bar is for "Archivo:" at 0% (0 kb). The second bar is for "Total actualización" at 0% (0 kb).

At the bottom, there is a help icon and text: "Para encontrar más información sobre las opciones de la Interfaz de Usuario de BitDefender, sitúe el ratón encima de la ventana y aparecerá un texto de ayuda en este área." Below that is the BitDefender logo and a navigation bar with links: "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", "Historial".

## 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.



### 21.1.1. 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.

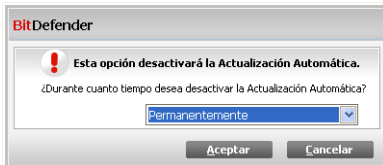


#### Nota

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

### 21.1.2. 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.

## 21.2. 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.

BitDefender Antivirus 2009 - Evaluación

CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver

REPARAR TODAS

Actualizar Configuración

General

Antivirus

Control de Privacidad

Vulnerabilidad

Cifrado

Modo Juego/Portátil

Red

Actualizar

Registro

**Configuración de la Ubicación de las Actualizaciones**

Ubicación primaria   Usar proxy

Ubicación alternativa   Usar proxy

**Configuración de la actualización automática**

Intervalo de tiempo  horas

Confirmar actualización

Actualización Silenciosa

Preguntar antes de descargar actualizaciones

Preguntar antes de instalar actualizaciones

**Configuración de la Actualización Manual**

Actualización Silenciosa

Preguntar antes de descargar actualizaciones

**Opciones avanzadas**

Esperar a que el usuario reinicie, en lugar de preguntar

No actualizar si hay un análisis en curso

No actualizar si el Modo Juego está activado

Aplicar Por defecto Opciones proxy

Para encontrar más información sobre las opciones de la Interfaz de Usuario de BitDefender, sitúe el ratón encima de la ventana y aparecerá un texto de ayuda en este área.

bitdefender

Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial

### 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.



## 21.2.1. 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. 201).

## 21.2.2. 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.



### 21.2.3. 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.

### 21.2.4. 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.

### 21.2.5. 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.



## 22. Registro

Para encontrar más información sobre su producto BitDefender y el estado del registro, diríjase al apartado **Registro** en la Vista Avanzada.

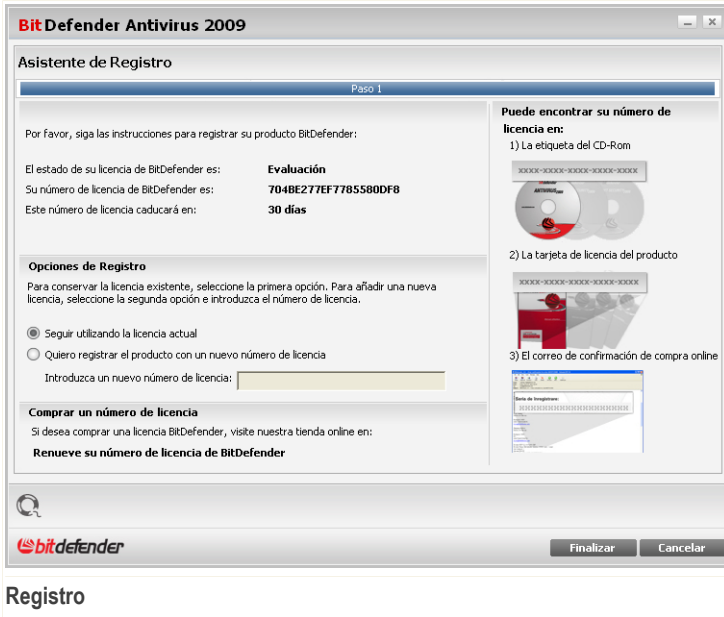
The screenshot shows the BitDefender Antivirus 2009 - Evaluación window. At the top, there is a red status bar that reads "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this is a navigation menu with "Registro" selected. The main content area is divided into three sections: "Información del Producto" (showing "BitDefender Antivirus 2009" and "Versión: 12.0.10"), "Información de Registro" (showing "Registrado por testare.automata@live.com", "Caduca en 30 días", and "Número de licencia: 7046E277EF785580DF8"), and "Acciones" (with buttons for "Crear una cuenta" and "Registrar Ahora"). A footer section contains a help icon and text: "Aquí puede ver información detallada sobre el registro de su producto BitDefender, el tipo de licencia, el periodo de validez y el número de licencia." Below the footer is the BitDefender logo and a navigation bar with links: "Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial".

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.

### 22.1. Registrando BitDefender Antivirus 2009

Haga clic en **Registrar** para abrir la ventana de registro del producto.



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 Antivirus 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**.

## 22.2. 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.

**BitDefender Antivirus 2009**

Crear Cuenta

Paso 1

**Registro en Mi Cuenta**

La Cuenta de BitDefender le da acceso al soporte técnico, así como a ofertas y promociones especiales. En caso de pérdida de su número de licencia de BitDefender, puede recuperarlo iniciando sesión en <http://myaccount.bitdefender.com>. Puede elegir entre iniciar sesión con una Cuenta de BitDefender existente o crear una nueva cuenta.

Iniciar sesión con una Cuenta de BitDefender existente

E-mail:

Contraseña:

[¿Ha olvidado su contraseña?](#)

Crear una Cuenta de BitDefender nueva

E-mail:

Contraseña:

Repetir contraseña:

Nombre:

Apellidos:

País:

Omitir Registro

Enviarme todos los mensajes de BitDefender

Enviarme sólo los mensajes más importantes

No enviarme ningún mensaje

Finalizar Cancelar

**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. 207)



- “Ya tengo una cuenta de BitDefender” (p. 207)

## 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**



## **23. 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](mailto: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.

### **23.1. 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>.



## **23.2. Solicitando Ayuda**

### **23.2.1. 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/>

### **23.2.2. 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/>



## 23.3. 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.

### 23.3.1. Direcciones Web

Departamento Comercial: [comercial@bitdefender.es](mailto:comercial@bitdefender.es)  
Soporte técnico: [soporte@bitdefender.es](mailto:soporte@bitdefender.es)  
Documentación: [documentation@bitdefender.com](mailto:documentation@bitdefender.com)  
Programa de Partners: [partners@bitdefender.es](mailto:partners@bitdefender.es)  
Marketing: [marketing@bitdefender.es](mailto:marketing@bitdefender.es)  
Relaciones con la Prensa: [prensa@bitdefender.es](mailto:prensa@bitdefender.es)  
Oportunidades de Trabajo: [jobs@bitdefender.es](mailto:jobs@bitdefender.es)  
Envío de Virus: [virus@bitdefender.es](mailto:virus@bitdefender.es)  
Envío de Spam: [spam\\_submission@bitdefender.com](mailto:spam_submission@bitdefender.com)  
Notificar abuso: [abuso@bitdefender.es](mailto: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](http://www.bitdefender.com/partner_list)  
BitDefender Knowledge Base: <http://kb.bitdefender.com>

### 23.3.2. 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](mailto: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](mailto: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](mailto:info@bitdefender.com)

Comercial: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Web: <http://www.bitdefender.com>

Soporte Técnico: [support@bitdefender.com](mailto:support@bitdefender.com)

## **Reino Unido e Irlanda**

Business Centre 10 Queen Street

Newcastle, Staffordshire

ST5 1ED

Tel: +44(0)1782664865

Email: [info@bitdefender.com](mailto:info@bitdefender.com)

Comercial: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Web: <http://www.bitdefender.co.uk>

Soporte técnico: [soporte@bitdefender.es](mailto:soporte@bitdefender.es)

## **España**

**BitDefender España, S.L**

C/ Balmes 191, 2ª planta, 08006

Barcelona

Soporte Técnico: [soporte@bitdefender.es](mailto:soporte@bitdefender.es)

Comercial: [comercial@bitdefender.es](mailto: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](mailto:soporte@bitdefender.es)

Comercial: [sales@bitdefender.com](mailto:sales@bitdefender.com)

Tel: +40 21 3001255

Tel: +40 21 3001254

Página del producto: <http://www.bitdefender.es>



*BitDefender Antivirus 2009*

## **CD de Rescate de BitDefender**



## 24. General

**BitDefender Antivirus 2009** incluye 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/](http://download.bitdefender.com/rescue_cd/)

## 24.1. 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 rendimiento. 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.

## 24.2. 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 las 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](#) .



## 25. 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.

### 25.1. 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

## 25.2. Detener el CD de Rescate de BitDefender

Puede apagar su equipo de forma segura seleccionando 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.

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufs) (aufs) (aufs) (aufs)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspend)
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufs) (aufs) (aufs) (aufs)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
d) (khsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Espera este mensaje cuando apaga el equipo

## 25.3. ¿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 complejidad 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**.

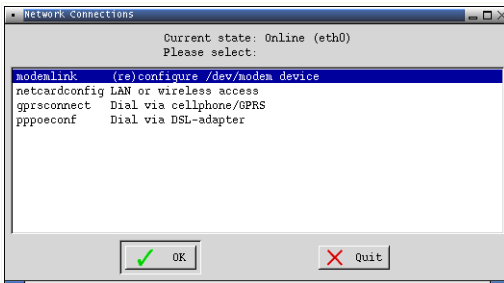
También puede utilizar el siguiente comando estando conectado como root en la terminal. El **Análisis Antivirus de BitDefender** comenzará a analizar los archivos y carpetas seleccionados.

```
# bdscan /path/to/scan/
```

## 25.4. ¿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
<b>modemlink</b>	Seleccione este tipo de conexión cuando utilice un módem y una línea de teléfono para acceder a Internet.
<b>netcardconfig</b>	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.
<b>gprsconnect</b>	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.
<b>pppoeconf</b>	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
```

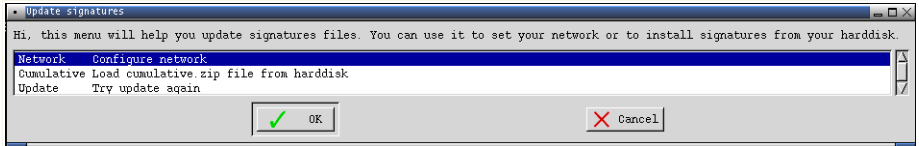
4. Siga las instrucciones que aparecen en pantalla. Si no está seguro de los datos que debe introducir, póngase en contacto con su administrador de sistema o red para más detalles.

## **25.5. ¿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 las 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**.

### 25.5.1. ¿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`.



## 25.6. 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 su equipo. En este tipo de situaciones es donde 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 Emulador 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.



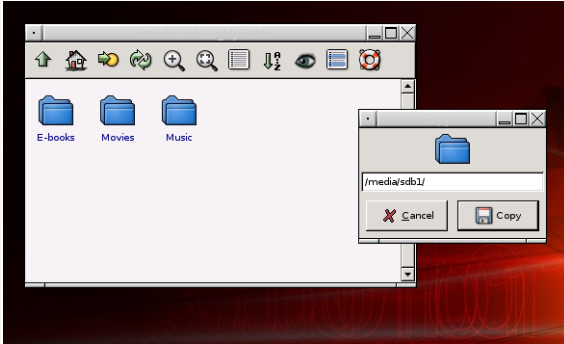
### Importante

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 dominio 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 específicas. 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 las 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 ordenadores con 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-repican; 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.