

bitdefender



TOTAL SECURITY 2009

Guía de usuario

 **bitdefender**



BitDefender Total Security 2009

Guía de usuario

publicado 2008.08.21

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 Total Security 2009





Tabla de contenidos

LICENCIA DE USO DE SOFTWARE PARA USUARIOS DOMÉSTICOS	xii
Prólogo	xvi
1. Convenciones utilizadas en este libro	xvi
1.1. Convenciones Tipográficas	xvi
1.2. Advertencias	xvii
2. La Estructura del Manual	xvii
3. Petición de Comentarios	xviii
Pasos de la Instalación	1
1. Requisitos del Sistema	2
1.1. Requisitos de Hardware	2
1.2. Requisitos de Software	3
2. Instalando BitDefender	4
2.1. Asistente de Registro	6
2.1.1. Paso 1/2 - Registrar BitDefender Total Security 2009	7
2.1.2. Paso 2/2 - Crear una Cuenta de BitDefender	8
2.2. Asistente de Configuración	10
2.2.1. Paso 1/9 - Intro	11
2.2.2. Paso 2/9 - Seleccione el Modo de Vista	12
2.2.3. Paso 3/9 - Configure la Red de Administración	13
2.2.4. Paso 4/9 - Configure el Control de Identidad	14
2.2.5. Paso 5/9 - Configure el Control Parental	18
2.2.6. Paso 6/9 - Configure el Informe de Virus en Tiempo Real	20
2.2.7. Paso 7/9 - Seleccione la Tarea a Ejecutar	21
2.2.8. Paso 8/9 - Espere a que Finalicen las Tareas	22
2.2.9. Step 9/9 - Finalizar	23
3. Reparar o Desinstalar BitDefender	24
Administración Básica	26
4. Primeros Pasos	27
4.1. Iniciar BitDefender Total Security 2009	27
4.2. Modo de Vista de la Interfaz de Usuario	27
4.2.1. Vista Básica	27
4.2.2. Vista Avanzada	30
4.3. Icono de BitDefender en el Área de Notificación del Sistema	33
4.4. Barra de Actividad del Análisis	33
4.5. Análisis Manual de BitDefender	34



4.6. Modo Juego	35
4.6.1. Usando el Modo Juego	35
4.6.2. Cambiando el Atajo de Teclado del Modo Juego	36
4.7. Integración en Clientes de Correo	36
4.7.1. La barra de herramientas Antispam	37
4.7.2. Asistente de Configuración Antispam	45
4.8. Integración con Navegadores Web	50
4.9. Integración con Programas de Mensajería	52
5. Visualizador	54
5.1. Estadísticas	166
5.2. General	166
5.3. Tareas	57
5.3.1. Analizando con BitDefender	57
5.3.2. Actualizando BitDefender	58
6. Seguridad	60
6.1. Componentes Monitorizados	60
6.1.1. Seguridad local	152
6.1.2. Seguridad online	153
6.1.3. Seguridad de la red	155
6.1.4. Control parental	155
6.1.5. Análisis de Vulnerabilidad	158
6.2. Tareas	66
6.2.1. Analizando con BitDefender	66
6.2.2. Actualizando BitDefender	72
6.2.3. Buscando Vulnerabilidades	74
7. Optimizador	82
7.1. Componentes Monitorizados	83
7.1.1. Optimizador	157
7.2. Tareas	84
7.2.1. Limpiando el Registro	84
7.2.2. Recuperando Claves Eliminadas	89
7.2.3. Eliminando Archivos de Forma Permanente	91
7.2.4. Limpiando los Archivos de Internet	94
7.2.5. Buscar Duplicados	97
7.2.6. Desfragmentando los Discos Duros	102
8. Administrador de Archivos	107
8.1. Componentes Monitorizados	108
8.1.1. Blindaje de archivos	156
8.1.2. Copia de Seguridad	158
8.2. Tareas	110
8.2.1. Realizando Copias de Seguridad Locales	111
8.2.2. Restaurando las Copias de Seguridad Locales	115
8.2.3. Añadiendo Archivos al Blindaje	119



8.2.4. Eliminando Archivos del Blindaje	125
8.2.5. Visualizando los Archivos del Blindaje	130
8.2.6. Bloqueando un Blindaje	134
9. Red	138
9.1. Tareas	139
9.1.1. Unirse a la Red de BitDefender	385
9.1.2. Añadiendo Equipos a la Red de BitDefender	385
9.1.3. Administrando la Red de BitDefender	142
9.1.4. Analizando Todos los Equipos	144
9.1.5. Actualizando Todos los Equipos	145
9.1.6. Registrando Todos los Equipos	146
10. Configuración Básica	147
10.1. Seguridad local	148
10.2. Seguridad online	148
10.3. Configuración del Control Parental	149
10.4. Configuración de la Red	149
10.5. Configuración del Blindaje de Archivos	150
10.6. Configuración General	150
11. Barra de Estado	152
11.1. Seguridad local	152
11.2. Seguridad online	153
11.3. Seguridad de la red	155
11.4. Control parental	155
11.5. Blindaje de archivos	156
11.6. Optimizador	157
11.7. Copia de Seguridad	158
11.8. Análisis de Vulnerabilidad	158
12. Registro	160
12.1. Paso 1/1 - Registrar BitDefender Total Security 2009	160
13. Historial	162
Administración Avanzada	164
14. General	165
14.1. Visualizador	165
14.1.1. Estadísticas	166
14.1.2. General	166
14.2. Configuración	167
14.2.1. Configuración General	168
14.2.2. Configuración del Informe de Virus	170
14.3. Información del Sistema	170



15. Antivirus	172
15.1. Protección en Tiempo Real	172
15.1.1. Configurando el Nivel de Protección	173
15.1.2. Personalizando el Nivel de Protección	174
15.1.3. Configurando el Análisis de Comportamiento	178
15.1.4. Desactivando la Protección en Tiempo Real	181
15.1.5. Configurando la Protección Antiphishing	181
15.2. Análisis Bajo Demanda	182
15.2.1. Tareas de Análisis	184
15.2.2. Utilizando el Menú Contextual	186
15.2.3. Creando tareas de análisis	187
15.2.4. Configurando una Tarea de Análisis	187
15.2.5. Analizando Objetos	200
15.2.6. Viendo los Informes del Análisis	206
15.3. Objetos Excluidos del Análisis	208
15.3.1. Excluyendo Rutas del Análisis	210
15.3.2. Excluyendo Extensiones del Análisis	214
15.4. Área de Cuarentena	218
15.4.1. Administrando los Archivos en Cuarentena	219
15.4.2. Configurando las Opciones de Cuarentena	220
16. Antispam	222
16.1. Comprensión del Antispam	222
16.1.1. Los Filtros Antispam	222
16.1.2. Funcionamiento del Antispam	225
16.2. Estado	226
16.2.1. Estableciendo el Nivel de Protección	227
16.2.2. Configurando la Lista de Amigos	229
16.2.3. Configurando la Lista de Spammers	230
16.3. Configuración	232
16.3.1. Configuración Antispam	234
16.3.2. Filtros Antispam Básicos	234
16.3.3. Filtros Antispam Avanzados	234
17. Control Parental	236
17.1. Estado de la Configuración por Usuario	237
17.1.1. Protegiendo la Configuración del Control Parental	239
17.1.2. Configurando el Filtrado Heurístico de Webs	241
17.2. Control Web	241
17.2.1. Asistente de Configuración	243
17.2.2. Especificar Excepciones	244
17.2.3. Lista Negra de Webs de BitDefender	245
17.3. Control de Aplicaciones	245
17.3.1. Asistente de Configuración	246
17.4. Filtro de Palabras Clave	247
17.4.1. Ventana de Configuración	248



17.5. Control de Mensajería Instantánea (IM)	249
17.5.1. Ventana de Configuración	250
17.6. Limitador de Tiempo Web	251
18. Control de Privacidad	253
18.1. Estado del Control de Privacidad	253
18.1.1. Configurando el Nivel de Protección	254
18.2. Control de Identidad	255
18.2.1. Creando Reglas de Identidad	257
18.2.2. Definiendo las Excepciones	261
18.2.3. Administrando Reglas	262
18.3. Control del registro	263
18.4. Control de las Cookies	265
18.4.1. Ventana de Configuración	267
18.5. Control de Scripts	269
18.5.1. Ventana de Configuración	270
19. Cortafuego	272
19.1. Configuración	272
19.1.1. Estableciendo la Acción Predeterminada	274
19.1.2. Modificando las Opciones Avanzadas del Cortafuego	275
19.2. Red	277
19.2.1. Cambiando el Nivel de Confianza	278
19.2.2. Configurando el Modo Oculto	279
19.2.3. Modificando la Configuración Genérica	279
19.2.4. Zonas de Red	279
19.3. Reglas	280
19.3.1. Añadir Reglas Automáticamente	283
19.3.2. Eliminando Reglas	283
19.3.3. Creando y Modificando Reglas	283
19.3.4. Configuración Avanzada de las Reglas	287
19.4. Control de Conexiones	289
20. Tareas de Copia	291
20.1. Realizando Copias de Seguridad Locales	292
20.1.1. Paso 1/5 - Ventana de Bienvenida	292
20.1.2. Paso 2/5 - Seleccionar los datos a Copiar	292
20.1.3. Paso 3/5 - Seleccionar donde hacer Copia	293
20.1.4. Paso 4/5 - Seleccionar cuando realizar la Copia	294
20.1.5. Paso 5/5 - Resumen	295
20.2. Restaurando las Copias de Seguridad Locales	296
20.2.1. Paso 1/4 - Ventana de Bienvenida	296
20.2.2. Paso 2/4 - Selecciona la Copia a restaurar	297
20.2.3. Paso 3/4 - Seleccionar la Ubicación de Restauración y los Archivos ...	298
20.2.4. Paso 4/4 - Resumen	299
20.3. Copias de Seguridad Avanzadas	300



20.3.1. Barra de Menú	301
20.3.2. Barra de Navegación	303
21. Cifrado	336
21.1. Cifrado de Mensajería Instantánea (IM)	336
21.1.1. Desactivando el Cifrado para Usuarios Específicos	338
21.2. Blindaje de Archivos	338
21.2.1. Creando un Blindaje	339
21.2.2. Abriendo un Blindaje	341
21.2.3. Bloqueando un Blindaje	341
21.2.4. Cambiando la Contraseña del Blindaje	342
21.2.5. Añadiendo Archivos a un Blindaje	343
21.2.6. Eliminando Archivos de un Blindaje	343
22. Vulnerabilidad	344
22.1. Estado	344
22.1.1. Comprobando Vulnerabilidades	345
22.2. Configuración	351
23. Optimizador	353
23.1. Desfragmentando los Discos Duros	354
23.1.1. Paso 1/3 - Analizando... ..	355
23.1.2. Paso 2/3 - Ver Informe del Análisis	356
23.1.3. Paso 3/3 - Ver Informe de la Desfragmentación	357
23.2. Limpiando su PC	358
23.2.1. Paso 1/3 – Iniciar Eliminación	359
23.2.2. Paso 2/3 - Eliminando Archivos... ..	360
23.2.3. Paso 3/3 - Ver Resumen de Resultados	360
23.3. Eliminando Archivos de Forma Permanente	361
23.3.1. Paso 1/3 - Seleccionar Objetivo	362
23.3.2. Paso 2/3 - Eliminando Archivos... ..	363
23.3.3. Paso 3/3 - Ver Resumen de Resultados	363
23.4. Limpiando el Registro de Windows	364
23.4.1. Paso 1/4 - Iniciar Análisis	365
23.4.2. Paso 2/4 - Analizando... ..	365
23.4.3. Paso 3/4 – Seleccione la acción	366
23.4.4. Paso 4/4 - Ver Resumen de Resultados	368
23.5. Recuperando Claves Eliminadas	369
23.5.1. Paso 1/2 - Iniciar Recuperador del Registro	370
23.5.2. Paso 2/2 - Ver Resultados	371
23.6. Buscar Duplicados	371
23.6.1. Paso 1/4 – Seleccione el Objetivo de Búsqueda	372
23.6.2. Paso 2/4 - Buscando... ..	373
23.6.3. Paso 3/4 – Seleccione la acción	373
23.6.4. Paso 4/4 - Ver Resumen de Resultados	375
24. Modo Juego / Portátil	376



24.1. Modo Juego	376
24.1.1. Configurando el Modo Juego Automático	377
24.1.2. Administrando la Lista de Juegos	378
24.1.3. Modificando la Configuración del Modo Juego	380
24.1.4. Cambiando el Atajo de Teclado del Modo Juego	381
24.2. Modo Portátil	382
24.2.1. Configurando las Opciones del Modo Portátil	383
25. Red	384
25.1. Unirse a la Red de BitDefender	385
25.2. Añadiendo Equipos a la Red de BitDefender	385
25.3. Administrando la Red de BitDefender	387
26. Actualización	390
26.1. Actualización automática	390
26.1.1. Solicitando una Actualización	392
26.1.2. Desactivando la Actualización Automática	392
26.2. Configuración de la Actualización	393
26.2.1. Configuración de la Ubicaciones de las Actualizaciones	394
26.2.2. Configurando la Actualización Automática	394
26.2.3. Configurando la Actualización Manual	395
26.2.4. Modificando las Opciones Avanzadas	395
26.2.5. Administrando los Proxies	395
27. Registro	398
27.1. Registrando BitDefender Total Security 2009	398
27.2. Creando una Cuenta de BitDefender	400
Conseguir Ayuda	403
28. Soporte	404
28.1. BitDefender Knowledge Base	404
28.2. Solicitando Ayuda	405
28.2.1. Ir a la Web de Ayuda On-Line	405
28.2.2. Abrir un ticket de soporte	405
28.3. Información de Contacto	406
28.3.1. Direcciones Web	406
28.3.2. Filiales	406
CD de Rescate de BitDefender	409
29. General	410
29.1. Requisitos del Sistema	410
29.2. Software Incluido	411
30. Cómo Utilizar el CD de Rescate de BitDefender	414
30.1. Iniciar el CD de Rescate de BitDefender	414



30.2. Detener el CD de Rescate de BitDefender	415
30.3. ¿Cómo realizo un análisis antivirus?	416
30.4. ¿Cómo puedo configurar la conexión a Internet?	417
30.5. ¿Cómo puedo actualizar BitDefender?	418
30.5.1. ¿Cómo puedo actualizar BitDefender a través de un servidor proxy? ...	419
30.6. Cómo guardar mis datos?	420
Glosario	423



LICENCIA DE USO DE SOFTWARE PARA USUARIOS DOMÉSTICOS

Queda expresamente excluido del ámbito de esta Licencia el uso del software por parte de Empresas



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 física) y BITDEFENDER S.R.L., en relación al uso del software BitDefender por usuarios en el ámbito doméstico. 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, y únicamente al mismo (en adelante referido como el Usuario, que necesariamente debe ser persona física), la facultad no exclusiva, limitada y no transferible de usar BitDefender en los terminos y condiciones del Contrato. Al efecto, el Usuario sólo queda autorizado para instalar y usar BitDefender en un máximo de cuatro equipos o dispositivos (ordenador, PDA, o cualquier otro



dispositivo idóneo), y sólo en un ámbito doméstico. 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, el número de los equipos o dispositivos en los que esté instalado BitDefender y/o su actualización no podrá superar en total el citado límite máximo de 4 equipos o dispositivos.

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

Este manual le describirá el uso de **BitDefender Total Security 2009**, la compañía y el equipo que lo ha desarrollado le guiarán a través del proceso de instalación y le enseñarán a configurarlo. Descubrirá cómo utilizar **BitDefender Total Security 2009**, cómo actualizarlo, evaluarlo y personalizar la configuración. En resumen, aprenderá a sacarle el máximo provecho a BitDefender.

Le deseamos una provechosa y agradable lectura.

1. Convenciones utilizadas en este libro

1.1. Convenciones Tipográficas

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

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



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 Total Security 2009**. Empezando por los pre-requisitos para una instalación exitosa, se le conducirá a través del proceso de instalación por completo. Finalmente, también se describirá el proceso de 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 ha enseñado a configurar y utilizar todos los módulos de



BitDefender para proteger a su equipo eficazmente contra toda clase de amenazas (malware, spam, hackers, contenido inapropiado y otros).

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

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

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

3. Petición de Comentarios

Le invitamos a ayudarnos a mejorar este manual. Hemos comprobado y verificado toda la información contenida en este documento de la mejor forma posible. Por favor, escríbanos para comentarnos cualquier error que encuentre en este manual así como sugerencias para mejorarlo y ayudarnos a ofrecerle la mejor documentación posible.

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



Importante

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



Pasos de la Instalación



1. Requisitos del Sistema

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

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

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



Nota

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

1.1. Requisitos de Hardware

Para Windows XP

- Procesador de 800 MHz o superior
- 256 MB de Memoria RAM (1 GB recomendado)
- 210 MB de espacio libre en disco (250 MB recomendado)

Para Windows Vista

- Procesador de 800 MHz o superior
- 512 MB de Memoria RAM (1 GB recomendado)
- 210 MB de espacio libre en disco (250 MB recomendado)

Para Windows Home Server

- Procesador de 800 MHz o superior
- 512 MB de Memoria RAM (1 GB recomendado)
- 210 MB de espacio libre en disco (250 MB recomendado)



1.2. Requisitos de Software

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

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

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

Protección Antiphishing disponible sólo para:

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

Cifrado de Mensajería Instantánea (IM) disponible sólo para:

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



2. Instalando BitDefender

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

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

1 Bienvenido al Instalador de BitDefender 2009! Bienvenido al Instalador de BitDefender Total Security 2009! BitDefender Total Security 2009 ofrece protección de última generación frente a amenazas de robo de datos. Haga clic en "Siguiente" o "Cancelar" para abandonar la instalación.

2 Recomendaciones: Desinstale o desactive otros productos de seguridad. BitDefender ofrece protección de última generación frente a amenazas de robo de datos, certificados por McAfee, Trend Micro, Symantec, Kaspersky Lab, Avast, AVG, Avira, Sophos, Comodo, Panda, ESET, Ikarus, Avast, AVG, Avira, Sophos, Comodo, Panda, ESET, Ikarus. Si ya tiene instalado un programa antivirus, debe eliminarlo antes de instalar BitDefender. Tener instalados dos programas antivirus puede dañar el sistema. Haga clic en "Siguiente" para comenzar la instalación. Para "Cancelar", haga clic en "Cancelar".

3 Contrato de licencia: Por favor lea con atención el contrato de licencia. 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

4 Seleccione la ubicación de la instalación: Seleccione la ubicación dónde desea almacenar los archivos. Haga clic en Explorador para elegir una nueva ubicación o BitDefender Total Security 2009. Basándose en su sitio espacio necesario y determinará si hay espacio suficiente. Ubicación: D:\Program Files\BitDefender\ Haga clic en Siguiente para continuar la instalación. Haga clic en "Cancelar" para abandonar la instalación.

5 Por favor, seleccione las opciones de instalación: Abre fichero Inicio Crear acceso directo Desactivar Firewall de Windows desde el momento de la instalación de BitDefender ya si está instalado. Haga clic en "Instalar" para comenzar la instalación. Haga clic en "Cancelar" para abandonar la instalación.

6 Finalizando la instalación del programa BitDefender Total Security 2009: Haga clic en el botón "Finalizar" para terminar la instalación.

Pasos de la Instalación



Siga estos pasos para instalar BitDefender Total Security 2009:

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

BitDefender Total Security 2009 le avisará si tiene otros productos antivirus instalados en su ordenador. Haga clic en **Desinstalar** para eliminar el producto correspondiente. Si desea continuar sin desinstalar los productos detectados, haga clic en **Siguiente**.



Aviso

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

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



Importante

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

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

Haga clic en **Siguiente**.

5. Seleccione las opciones relativas al proceso de instalación. Algunas opciones están seleccionadas por defecto:
 - **Abrir fichero léame** - para abrir el fichero léame al final de la instalación.
 - **Crear acceso directo en el Escritorio** - para situar un acceso directo de BitDefender Total Security 2009 en el Escritorio al finalizar la instalación.
 - **Expulsar el CD al completar la instalación** - para expulsar el CD cuando finalice la instalación; esta opción aparece cuando instala el producto desde un CD.
 - **Desactivar el cortafuego de Windows** - para desactivar el Firewall de Windows.



Importante

Recomendamos desactivar el Firewall de Windows puesto que BitDefender Total Security 2009 ya incluye un cortafuego avanzado. Ejecutar dos cortafuegos en el mismo equipo puede causar problemas.

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

Haga clic en **Instalar** para iniciar la instalación del producto. En caso de no disponer de .NET Framework 1.1, BitDefender empezará con la instalación de este componente.

Espere hasta que la instalación se complete.

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



Importante

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

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

2.1. Asistente de Registro

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

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

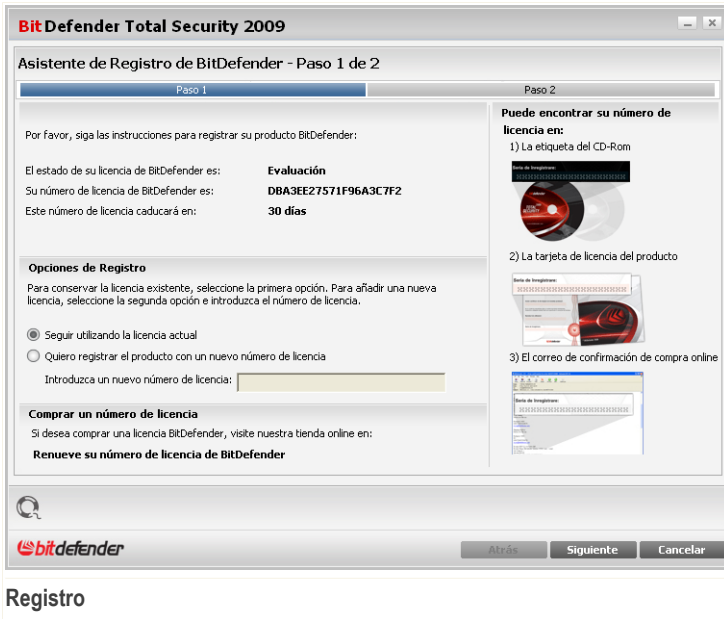


Nota

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



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



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

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

Para registrar BitDefender Internet Total 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 Total Security 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?](#)

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

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 Total Security 2009 esté instalado.

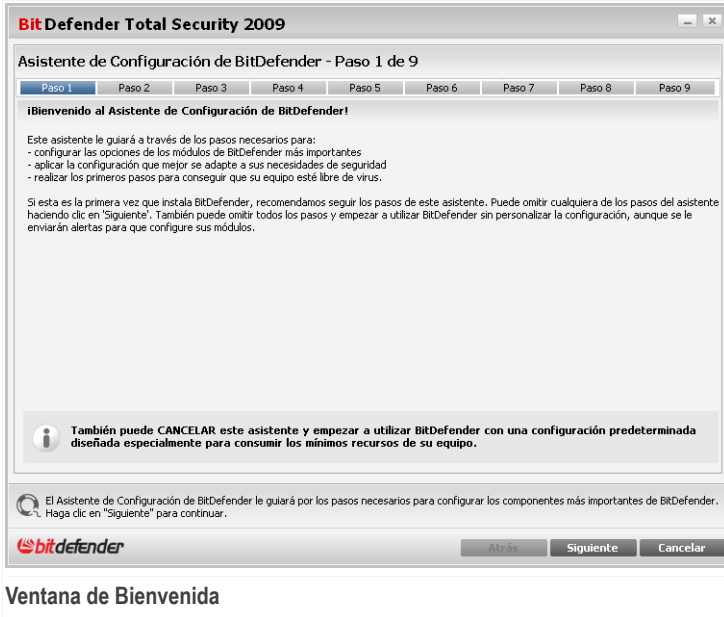


Nota

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



2.2.1. Paso 1/9 - Intro

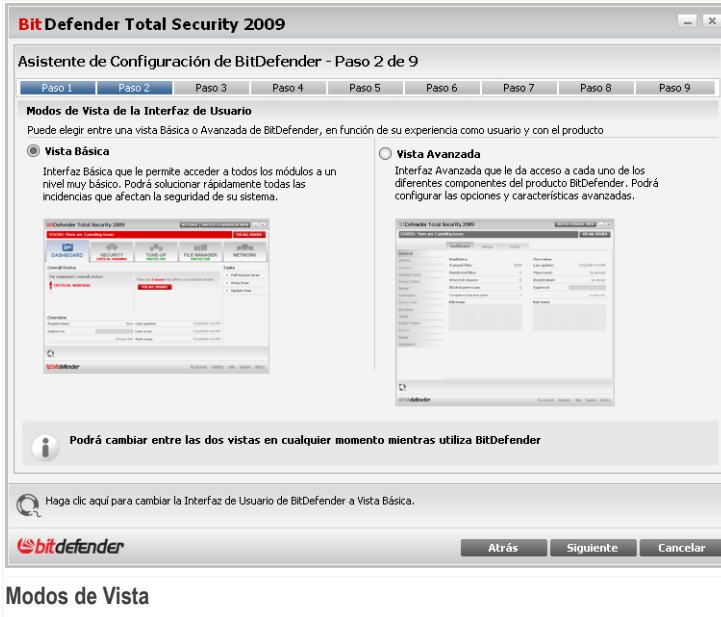


Ventana de Bienvenida

Haga clic en **Siguiente** para continuar.



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



Modos de Vista

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

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

Haga clic en **Siguiente** para continuar.



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

BitDefender Total Security 2009

Asistente de Configuración de BitDefender - Paso 3 de 9

Paso 1 Paso 2 **Paso 3** Paso 4 Paso 5 Paso 6 Paso 7 Paso 8 Paso 9

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 este área.

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.



Haga clic en **Siguiente** para continuar.

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

BitDefender Total Security 2009

Asistente de Configuración de BitDefender - Paso 4 de 9

Página de Administración de Regla de Identidad

El módulo Control de Identidad de BitDefender protege sus datos confidenciales frente a tentativas de robo de información privada, como el número de tarjeta de crédito, dirección de e-mail, etc.

También le ayuda a mantener la confidencialidad de sus datos al analizar el tráfico de correo y web en busca de determinadas cadenas de texto. Para utilizar este módulo, debe activarlo y configurarlo. Toda información introducida será cifrada bajo las credenciales de su cuenta.

I want to configure it now

Añadir **Quitar**

Nombre de la ...	Tipo de Regla	HTTP	SMTP	IM	Palabras co...	Mayúsculas y ...	Descripción
1	Tarjeta de cr...	SI	SI	NO	SI	NO	

Excepciones

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

Configuración del Control de Identidad

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

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

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



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

Haga clic en **Siguiente** para continuar.

Creando Reglas del Control de Identidad

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

Añadir Regla de Identidad

Nombre de la Regla Analizar HTTP

Tipo de Regla 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:

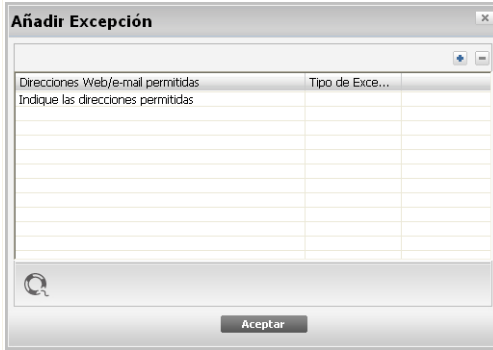
- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (correo) y bloquea los mensajes salientes que coinciden con los datos de la regla.
- **Analizar Mensajería Instantánea** - analiza el 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 5/9 – Configure el Control Parental

Asistente de Configuración de BitDefender - Paso 5 de 9

Control Parental de BitDefender

El Control Parental de BitDefender le permite controlar el acceso a Internet y a determinadas aplicaciones de cada una de las Cuentas de Usuario de Windows del sistema. Para utilizar este módulo debe activarlo y configurarlo.

Haga clic derecho sobre un nombre de usuario para configurar su opciones del Control Parental.

Quiero usar el Control Parental

Lista de Usuarios	Estado
Administrador	Adolescente

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 Control Parental

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

Si desea usar el Control Parental, siga estos pasos:

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

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



Perfil	Descripción
Adolescente	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios entre 14 y 18 años. Se bloqueará el acceso a las páginas web con contenido sexual, pornográfico o adulto.
Adulto	Ofrece un acceso sin restricción a todas las páginas web, independientemente de su contenido.



Nota

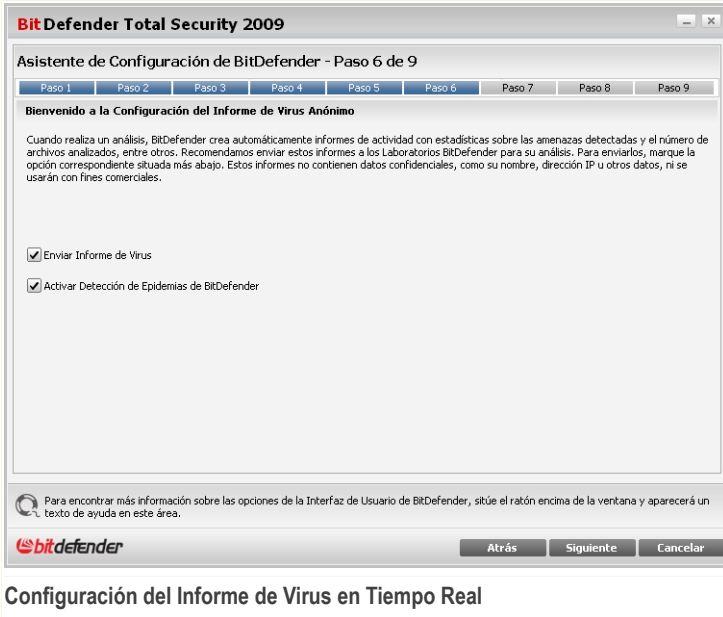
Para configurar por completo el Control Parental o desactivarlo en determinadas cuentas de Windows, abra BitDefender, cambie a la Vista Avanzada y diríjase al apartado **Control Parental**. Puede configurar Control Parental para que bloquee:

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

Haga clic en **Siguiente** para continuar.



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



Configuración del Informe de Virus en Tiempo Real

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

Puede configurar las siguientes opciones:

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



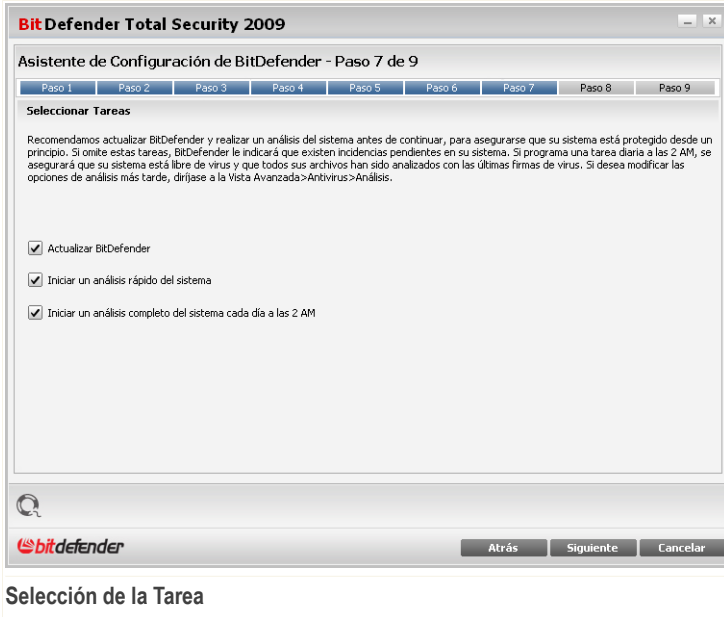
Nota

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

Haga clic en **Siguiente** para continuar.



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



Selección de la Tarea

Configure BitDefender Total Security 2009 para que realice tareas importantes para la seguridad de su sistema. Dispone de las siguientes opciones:

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



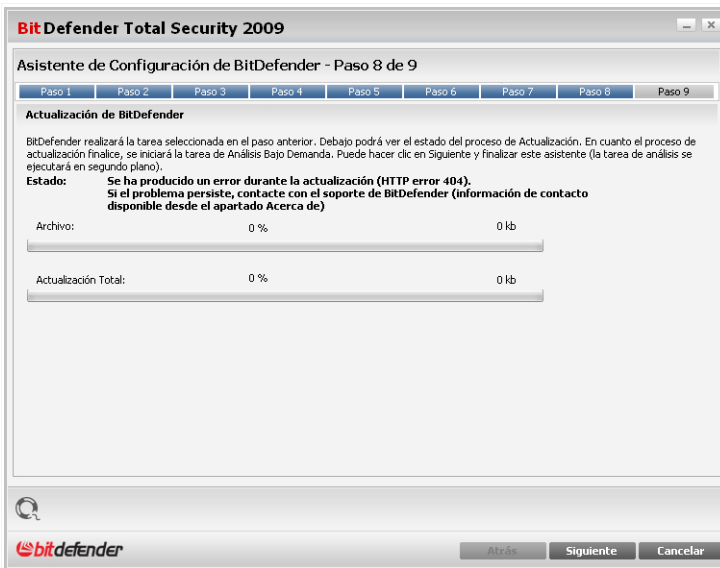
Importante

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

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

Haga clic en **Siguiente** para continuar.

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



Estado de la Tarea

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

Haga clic en **Siguiente** para continuar.



2.2.9. Step 9/9 - Finalizar



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 Total Security 2009**, siga estos pasos en el menú Inicio de Windows: **Inicio** → **Programas** → **BitDefender 2009** → **Reparar o Desinstalar**.

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

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

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

Reinicie el ordenador cuando se le indique, y a continuación haga clic en **Instalar** para reinstalar BitDefender Total Security 2009.

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

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



Nota

Recomendamos seleccionar la opción **Desinstalar** para realizar una reinstalación limpia.

Si decide desinstalar BitDefender, aparecerá una nueva ventana.



Importante

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

Haga clic en **Desinstalar** para iniciar la desinstalación de BitDefender Total Security 2009 en su equipo.

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

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



Nota

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

Error durante la desinstalación de BitDefender

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



Administración Básica




4. Primeros Pasos

Una vez tenga BitDefender instalado, su equipo estará protegido.

4.1. Iniciar BitDefender Total Security 2009

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

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

4.2. Modo de Vista de la Interfaz de Usuario

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

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



Nota

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

4.2.1. Vista Básica

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



Vista Básica

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

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

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



Pestaña	Descripción
Visualizador	Muestra estadísticas representativas sobre la actividad del producto, el estado de su registro y enlaces a las tareas bajo demanda más importantes.
Seguridad	Muestra el estado de los módulos de seguridad (antivirus, antiphishing, cortafuego, antispam, cifrado de IM, privacidad, comprobación de vulnerabilidades y actualización) junto con enlaces a tareas antivirus, actualización y comprobación de vulnerabilidades.
Optimizador	Muestra el estado de las características de BitDefender diseñadas para mejorar el rendimiento de su equipo, así como enlaces a tareas de optimización.
Administrador de Archivos	Muestra el estado de los módulos blindaje de archivos y copia de seguridad, así como enlaces a tareas de relacionadas con éstos.
Red	Muestra la estructura de la red de administración.

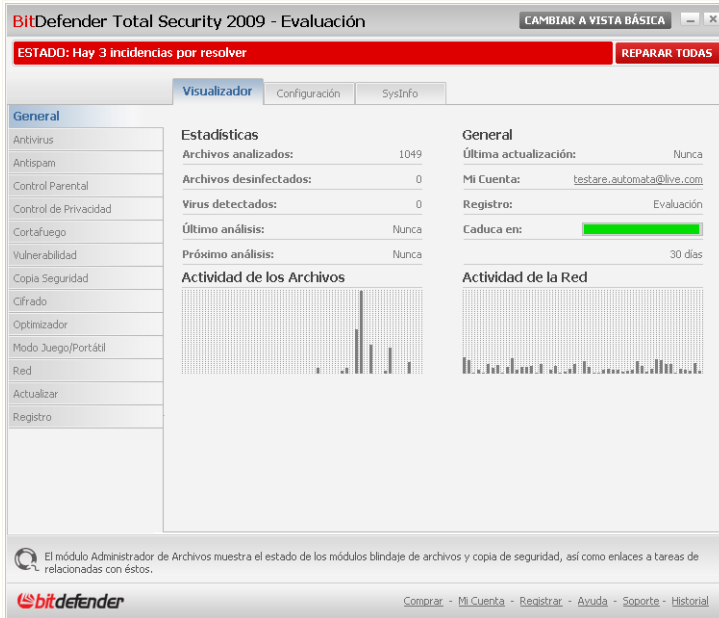
- Además, la ventana de Vista Básica contiene algunos accesos directos que pueden resultarle útiles.

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



4.2.2. Vista Avanzada

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



Vista Avanzada

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

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



<i>Elemento</i>	<i>Descripción</i>
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.

<i>Módulo</i>	<i>Descripción</i>
General	Le permite acceder a la configuración general o ver el visualizador e información del sistema.
Antivirus	Le permite configurar la protección antivirus en tiempo real y operaciones de análisis, establecer excepciones y configurar el módulo cuarentena.
Antispam	Le permite configurar en detalle el módulo antispam y así mantener su bandeja de entrada libre de Spam.
Cortafuego	Le permite proteger su sistema frente a los intentos de conexión externos o internos no autorizados. Algo parecido a tener un guardia en su puerta – vigilará su conexión a Internet y monitorizará todas las conexiones que decida autorizar o bloquear.
Control de Privacidad	Le ayuda a impedir el robo de datos de su equipo y protege su privacidad mientras está conectado a Internet.
Control Parental	Le permite impedir el acceso a contenido inapropiado a través de reglas de acceso personalizadas.
Tareas de Copia	Le permite realizar copias de seguridad de sus datos en el equipo, discos extraíbles, ubicaciones de la red, así como restaurarlos cuando sea necesario.
Cifrado	Le permite cifrar las conversaciones de Yahoo y Windows Live (MSN) Messenger, así como cifrar sus archivos, carpetas o particiones críticos.
Vulnerabilidad	Le permite tener actualizado el software crucial de su PC.
Optimizador	Le ayuda a mejorar el rendimiento de su equipo realizando desfragmentaciones del disco y limpiado el registro, archivos duplicados, etc.



Módulo	Descripción
Modo Juego/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 Total Security 2009, cambiar el número de licencia o crear una cuenta de BitDefender.

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

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

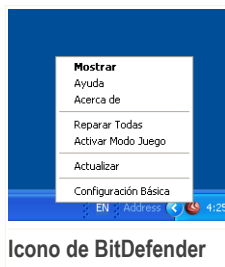


4.3. Icono de BitDefender en el Área de Notificación del Sistema

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

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

- **Mostrar** - abre BitDefender.
- **Ayuda** - abre el archivo de ayuda en el que se explica el funcionamiento y uso de BitDefender Total Security 2009.
- **Acerca de** - abre la ventana de información de BitDefender.
- **Reparar Incidencias** - le ayuda a eliminar las vulnerabilidades de seguridad.
- **Activar / desactivar Modo Juego** - activa o desactiva el **Modo Juego**.
- **Actualizar** - realiza una actualización inmediata. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización.
- **Configuración básica** - le permite activar o desactivar fácilmente los módulos de seguridad más importantes. Aparecerá una nueva ventana desde la que podrá activar / desactivar los módulos con un simple clic.



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

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

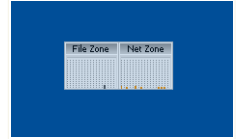
4.4. Barra de Actividad del Análisis

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



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

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



Barra de Actividad



Nota

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

Puede utilizar la opción **Barra de actividad del Análisis** para analizar archivos. Arrastre y suelte los archivos que desea analizar sobre la ventana de actividad BitDefender. Para más información, por favor, consulte el “*Análisis al Arrastrar y Soltar*” (p. 201) de esta guía de usuario.

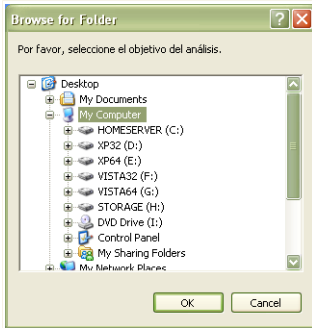
Para ocultar la barra de actividad haga clic derecho encima y seleccione **Ocultar**. Para ocultar completamente esta ventana, siga estos pasos:

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 Juego

El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento del sistema. Cuando activa el Modo Juego, 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 Juego está activado, podrá ver la letra **G** encima del icono de BitDefender.

4.6.1. Usando el Modo Juego

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 Juego**.
- Pulse **Ctrl+Shift+Alt+G** (el atajo de teclado predeterminado).



Importante

No olvide desactivar el Modo Juego 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 Juego

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 Juego/Portátil** del menú de la izquierda.
3. Haga clic en la pestaña **Modo Juego**.
4. Haga clic en el botón **Opciones Avanzadas**.
5. Debajo de la opción **Usar Atajos de Teclado**, configure la combinación de teclas deseada:

- Elija las teclas que desea utilizar seleccionado alguna de las siguientes: Control (Ctrl), Shift (Shift) o Alternate (Alt).
- En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

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



Nota

Si desmarca la casilla correspondiente a **Usar Atajos de Teclado**, desactivará la combinación de teclas.

4.7. Integración en Clientes de Correo

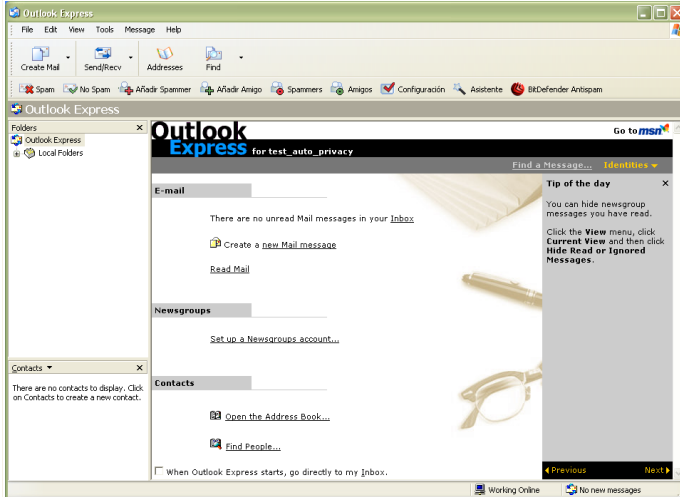
BitDefender se integra a través de una barra de herramientas muy intuitiva y fácil de usar en los siguientes clientes de correo:

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



4.7.1. La barra de herramientas Antispam

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



La barra de herramientas Antispam




Importante

La diferencia principal entre BitDefender Antispam para Microsoft Outlook y Outlook Express / Windows Mail, es que los mensajes SPAM son trasladados a la carpeta **Spam** en Microsoft Outlook, y a la carpeta **Elementos Eliminados** en Outlook Express. En ambos casos, los mensajes están marcados como SPAM en el asunto del mensaje.

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

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

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



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



Nota

Puede seleccionar un mensaje o todos los mensajes que desee.

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

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



Nota

Puede seleccionar un mensaje o todos los mensajes que desee.



Importante

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

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



Añadir Spammer

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

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

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

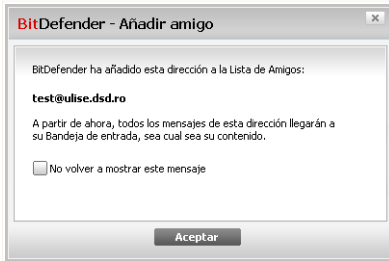


Nota

Puede seleccionar un remitente o todos los remitentes que desee.



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



Añadir Amigo

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

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

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



Nota

Puede seleccionar un remitente o todos los remitentes que desee.

- **Spammers** - abre la **Lista de Spammers** que contiene todas las direcciones de correo electrónico de las cuales no quiere recibir mensajes, independientemente de su contenido.



Nota

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



Lista de Spammers

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

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



Importante

Sintaxis: nombre@dominio.com.

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



Importante

Sintaxis:



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





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

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


En ambos casos, la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las direcciones que desee y haga clic en para añadirlas a la **Lista de Spammers**. Si hace clic en se añadirán todas las direcciones de correo al listado.

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

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

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

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

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




Nota

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



Lista de Amigos


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

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



Importante

Sintaxis: nombre@dominio.com.

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



Importante

Sintaxis:



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





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

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

En ambos casos, la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las direcciones que desee y haga clic en to add them to the **Lista de Amigos**. Si hace clic en se añadirán todas las direcciones de correo al listado.

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

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


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



Nota

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

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

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



Configuración

Dispone de las siguientes opciones:

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

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

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

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



Nota

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



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

4.7.2. Asistente de Configuración Antispam

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



Nota

Puede iniciar el asistente cuando quiera, haciendo clic en el botón **Asistente** de la **Barra de Herramientas Antispam**.

Paso 1/6 - Ventana de bienvenida



Ventana de Bienvenida

Haga clic en **Siguiente**.



Paso 2/6 - Completar la Lista de Amigos



Completar la Lista de Amigos

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

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

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



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



Eliminar la base de datos del filtro Bayesiano

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

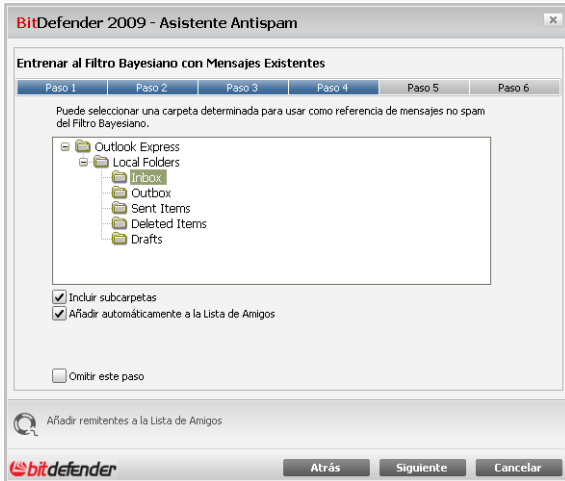
Seleccione la opción **Limpiar la base de datos del filtro Antispam** si desea reiniciar la base de datos del filtro Bayesiano.

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

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



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



Entrenar el Motor de Aprendizaje con Mensajes Legítimos

Por favor, seleccione una carpeta que contenga mensajes legítimos. Estos mensajes serán utilizados para entrenar el filtro antispam.

Existen dos opciones debajo de la lista de carpetas:

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

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



Paso 5/6 - Entrenar el Filtro Bayesiano con Spam



Entrenar el Filtro Bayesiano con Spam

Por favor, seleccione una carpeta que contenga mensajes de Spam. Estos mensajes serán utilizados para entrenar el filtro antispam.



Importante

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

Existen dos opciones debajo de la lista de carpetas:

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

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



Paso 6/6 - Epílogo



Resumen

En esta ventana se muestran todas las opciones del Asistente de Configuración. Puede hacer cualquier modificación que considere oportuna, volviendo al paso anterior (clic en **Atrás**).

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

4.8. Integración con Navegadores Web


BitDefender le protege contra los intentos de phishing mientras navega por Internet. Analiza las páginas web a las que accede y le alerta si detecta alguna amenaza de phishing. Puede configurar la Lista Blanca de páginas web que no serán analizadas por BitDefender.

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

- Internet Explorer
- Mozilla Firefox



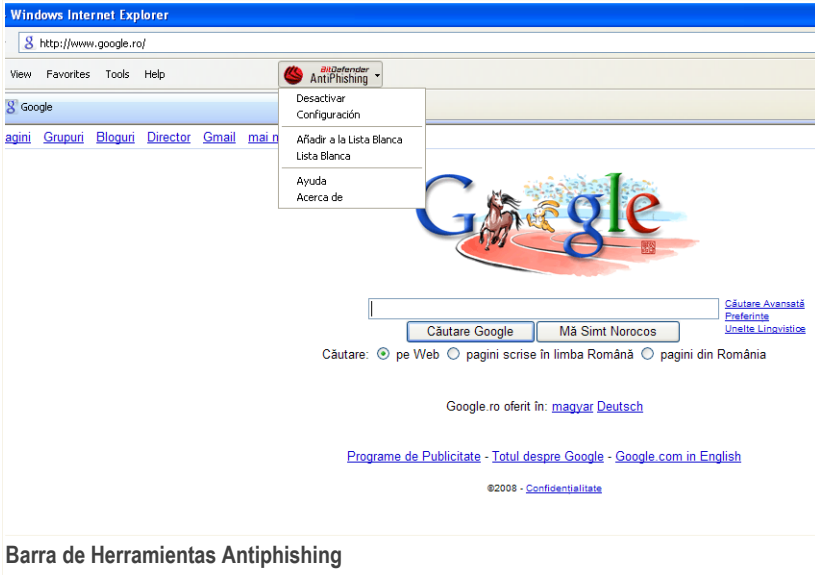
Puede administrar la protección antiphishing y la Lista Blanca fácilmente a través de la barra de herramientas de BitDefender Antiphishing, integrada en los navegadores citados anteriormente.

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



Nota

Si no puede ver la barra de herramientas, abra el menú **Ver**, diríjase a la opción **Barras de herramientas** y marque la opción **BitDefender Toolbar**.



Windows Internet Explorer

http://www.google.ro/

View Favorites Tools Help

Google

agini Grupuri Bloguri Director 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.

4.9. Integración con Programas de Mensajería

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

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

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



Importante

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

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

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

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

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 Total Security 2009 - Evaluación

CONFIGURACIÓN CAMBIAR A VISTA AVANZADA

ESTADO: Hay 4 incidencias por resolver REPARAR TODAS

VISUALIZADOR SEGURIDAD ADVERTENCIA CRÍTICA OPTIMIZADOR OPTIMIZADO ADMIN. ARCHIVOS ASEGURADO RED

Estado

Tareas

Estado global de Mi PC:
ADVERTENCIA CRÍTICA

Hay 4 incidencias que afectan a la seguridad de su sistema.
REPARAR TODAS

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

El Visualizador consta de varios apartados:

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



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

5.1. Estadísticas

Si desea tener controlada la actividad de BitDefender, puede empezar por el apartado Estadísticas:

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

5.2. General

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

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



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

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

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

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



Nota

Los datos que introduzca aquí serán confidenciales.

Para registrar BitDefender Total Security 2009, siga estos pasos:

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

Para comprar una nueva licencia, siga esto pasos:

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



3. Haga clic en el botón **Comprar**.

5.3. 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.

5.3.1. Analizando con BitDefender

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

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



Nota

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

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

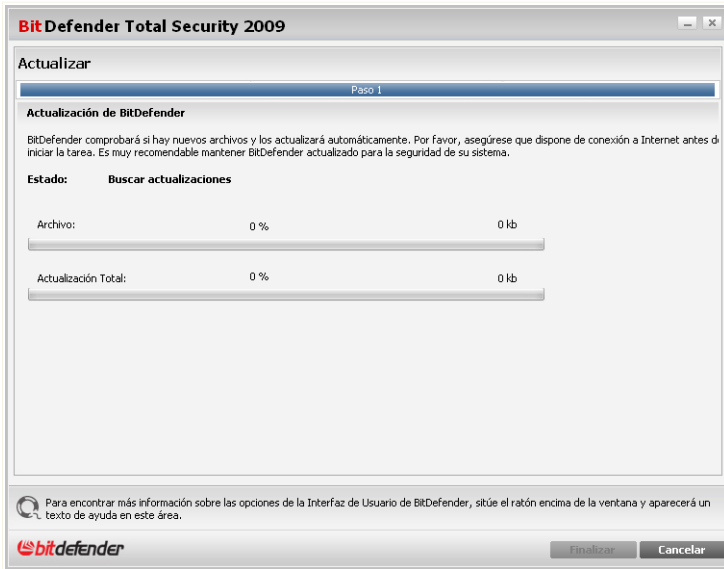


Siga el proceso guiado de tres pasos para completar el proceso de análisis.

5.3.2. Actualizando BitDefender

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

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



Actualizando BitDefender

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

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

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



Nota

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

Reinicie el equipo si así se le solicita. Cuando se produzca una actualización importante, se le solicitará reiniciar el equipo.

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

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



6. Seguridad

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

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

The screenshot shows the BitDefender Total Security 2009 - Evaluación interface. At the top, there's a navigation bar with 'CONFIGURACIÓN' and 'CAMBIAR A VISTA AVANZADA'. Below that, a red banner indicates 'ESTADO: Hay 4 incidencias por resolver' and a 'REPARAR TODAS' button. The main area has five tabs: 'VISUALIZADOR', 'SEGURIDAD ADVERTENCIA CRÍTICA', 'OPTIMIZADOR OPTIMIZADO', 'ADMIN. ARCHIVOS ASEGURADO', and 'RED'. The 'SEGURIDAD' tab is active, showing a table of 'Componentes Monitorizados' and a 'Tareas' sidebar.

Componentes Monitorizados	Monitorizar	Estado
Seguridad Local		
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
Cortafuego desactivado	<input checked="" type="checkbox"/> Sí	Reparar
Seguridad Online		1 incidencia por resolver
Control Parental		Aceptar
Análisis de vulnerabilidad		Aceptar

Tareas

- Actualizar
- Analizar Mis Documentos
- Análisis Completo
- Análisis en Profundidad
- Analizar Vulnerabilidades

El módulo Seguridad muestra el estado de los módulos de seguridad (antivirus, antiphishing, cortafuego, antispam, cifrado de IM, privacidad, comprobación de vulnerabilidades y actualización) así como enlaces a tareas antivirus, actualización y comprobación de vulnerabilidades.

bitdefender [Comprar](#) - [Mi Cuenta](#) - [Registrar](#) - [Ayuda](#) - [Soporte](#) - [Historial](#)

Seguridad

El módulo Seguridad consta de dos apartados:

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

6.1. Componentes Monitorizados

Los componentes monitorizados se agrupan en varias categorías.



Categoría	Descripción
Seguridad Local	Aquí puede comprobar el estado de cada uno de los módulos de seguridad encargados de proteger los objetos almacenados en su equipo (archivos, registro, memoria, etc.).
Seguridad Online	Aquí puede comprobar el estado de cada uno de los módulos de seguridad encargados de proteger sus transacciones online y la actividad de su equipo mientras está conectado a Internet.
Seguridad de la red	Desde aquí puede comprobar el estado del módulo Cortafuego que le protege frente a hackers.
Control parental	Desde aquí puede comprobar el estado del Control Parental, que le permite bloquear el acceso a Internet y a determinadas aplicaciones a sus hijos.
Análisis de Vulnerabilidad	Desde aquí puede comprobar si el software crucial de su PC está actualizado. También se comprueba si las cuentas de Windows cumplen los requisitos de seguridad.

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

6.1.1. Seguridad local

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

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

Incidencia	Descripción
Protección de archivos en tiempo real activada	Asegura el análisis de todos los archivos a los que accede o bien utilizan las aplicaciones que se ejecutan en el sistema.



<i>Incidencia</i>	<i>Descripción</i>
Nunca ha analizado su equipo en busca de malware	Recomendamos encarecidamente iniciar una tarea de análisis bajo demanda cuanto antes, para asegurarse que los archivos almacenados en su equipo están libres de malware.
Actualización automática activada	Mantenga activada la actualización automática para asegurarse que las firmas de malware de su producto BitDefender se actualizan regularmente.
Actualizando	Se está realizando una actualización del producto y firmas de malware.

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

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

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

6.1.2. Seguridad online

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

<i>Incidencia</i>	<i>Descripción</i>
Protección en tiempo real del tráfico web (HTTP) activada	Recomendamos mantener activada la protección web (HTTP) para proteger su equipo frente al malware que se propaga a través de páginas web y la descarga de archivos potencialmente maliciosos.
Protección del tráfico de correo en tiempo real activada	La protección del tráfico de correo le asegura que sus e-mails son analizados en busca de malware y filtrados en busca de spam.



<i>Incidencia</i>	<i>Descripción</i>
Protección del tráfico IM en tiempo real activada	Recomendamos activar la protección IM por completo para proteger su equipo y cifrar sus conversaciones.
Control de Identidad activado	Le ayuda a mantener a salvo su información confidencial, al analizar todo el tráfico web y el correo en busca de determinadas cadenas de texto. Recomendamos activar el Control de Identidad para mantener a salvo sus datos confidenciales (dirección de correo, IDs de usuario, contraseñas, números de tarjetas de crédito, etc) y impedir su robo.
Cifrado de conversaciones de IM activado	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.
Antiphishing activado para Mozilla Firefox	BitDefender le protege contra los intentos de phishing mientras navega por Internet.
Antiphishing activado para Internet Explorer	BitDefender le protege contra los intentos de phishing mientras navega por Internet.

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

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

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



6.1.3. Seguridad de la red

Cuando su equipo forma parte de una red, es necesario protegerse frente a hackers e intentos de conexión no autorizados a su sistema.

Las incidencias relativas a la seguridad de la red 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>
Cortafuego activado	Protege su equipo frente a hackers y ataques externos.

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

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

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

6.1.4. Control parental

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

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

<i>Incidencia</i>	<i>Descripción</i>
Control de Parental no configurado	El módulo Control Parental puede bloquear el acceso a las páginas web que considere inapropiadas, bloquear el acceso a Internet en determinados periodos de tiempo, y filtrar el tráfico



<i>Incidencia</i>	<i>Descripción</i>
	web, de correo y mensajería instantánea en busca de determinadas palabras.

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

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

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

6.1.5. 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>
Comprobación de Vulnerabilidades activada	Monitoriza las Actualizaciones de Microsoft Windows y Microsoft Office, así como las contraseñas de las cuentas de Windows, para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.
Actualizaciones Críticas de Microsoft	Instala las actualizaciones críticas de Microsoft disponibles.
Otras actualizaciones de Microsoft	Instala las actualizaciones no-críticas de Microsoft disponibles.
Actualizaciones Automáticas de Windows activadas	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.



<i>Incidencia</i>	<i>Descripción</i>
Admin (Contraseña Segura)	Indica la fortaleza de la contraseña de determinados usuarios.

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

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

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

6.2. Tareas

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

Dispone de los siguientes botones:

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

6.2.1. Analizando con BitDefender

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



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



Nota

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

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

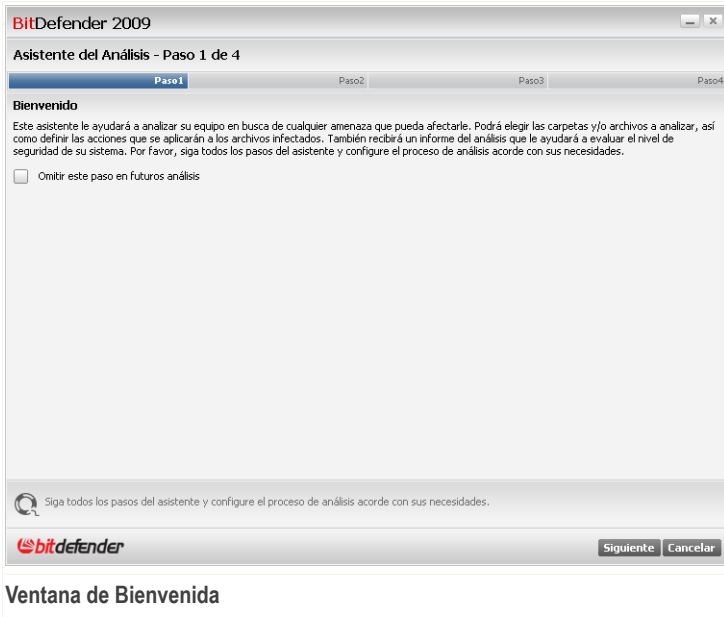
Siga el proceso guiado de tres pasos para completar el proceso de análisis.

Análisis personalizado

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

Paso 1/4 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.



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.



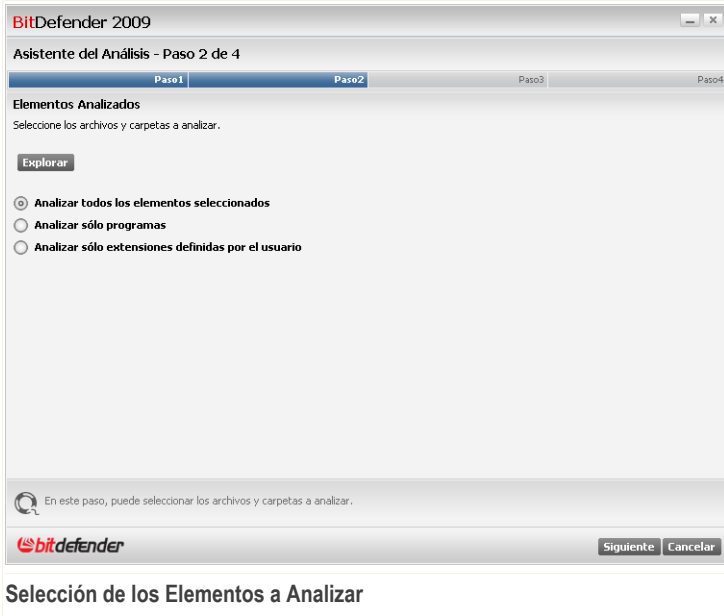
Nota

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.



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

Dispone de las siguientes opciones:

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



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

Paso 3/4 - Seleccione la Acción a Realizar

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

BitDefender 2009

Asistente del Análisis - Paso 3 de 4

Paso 1 | Paso 2 | **Paso 3** | Paso 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:

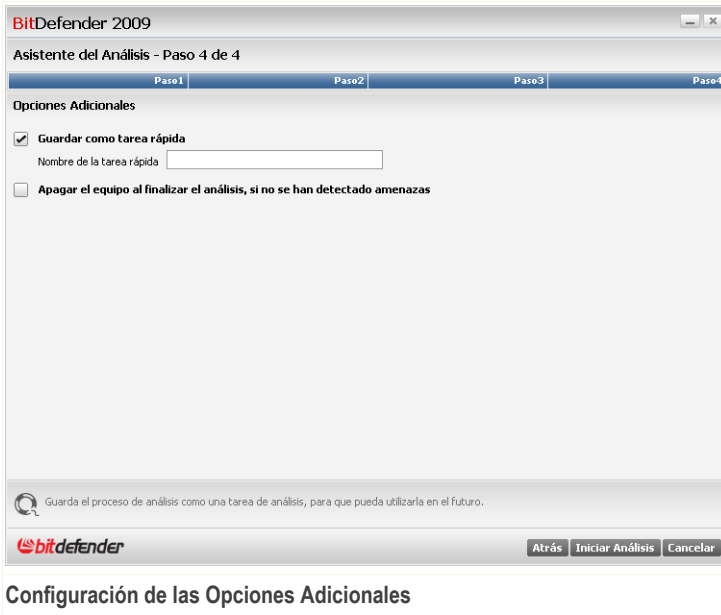


Nivel de Protección	Descripción
Alto	<p>Ofrece un alto nivel de seguridad. El nivel de consumo de recursos es alto.</p> <ul style="list-style-type: none">■ analiza todos los archivos y comprimidos■ analiza en busca de virus y spyware■ analiza en busca de procesos ocultos
Mediana	<p>Ofrece un nivel de seguridad medio. El nivel de consumo de recursos es moderado.</p> <ul style="list-style-type: none">■ analiza todos los archivos■ analiza en busca de virus y spyware
Bajo	<p>Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo.</p> <ul style="list-style-type: none">■ analiza sólo archivos de programas■ analiza en busca de virus
Personalizado	<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.

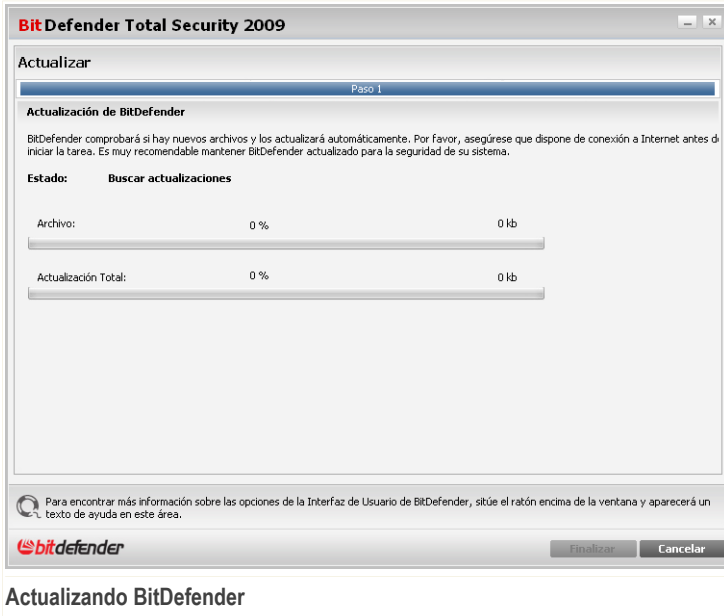
Haga clic en **Iniciar Análisis** y siga el asistente guiado de tres pasos para completar el proceso de análisis.

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:



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

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

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



Nota

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

Reinicie el equipo si así se le solicita. Cuando se produzca una actualización importante, se le solicitará reiniciar el equipo.



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

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

6.2.3. Buscando Vulnerabilidades

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

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

Comprobando Vulnerabilidades

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



Paso 1/6 – Seleccione las Vulnerabilidades a Comprobar

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.

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

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

How do you prefer to solve this issue?

Force user to change password at next logon

Change the password yourself now

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
Yahoo! Messenger	8.1.0.421	8.1.0.241	Actualizado
Firefox	2.0.0.16 (en-US)	3.0 (en-US)	Página de Inicio

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

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

- Microsoft GDI+ Detection Tool (KB873374)
- Windows Genuine Advantage Validation Tool (KB892130)
- Windows Internet Explorer 7 for Windows XP
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB936181)
- Windows XP Service Pack 3 (KB936929)
- 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)
- Security Update for Windows XP (KB946648)
- Security Update for Windows XP (KB952954)
- Cumulative Security Update for Internet Explorer 6 for Windows XP (KB953838)
- Security Update for Windows XP (KB950974)
- Update for Windows XP (KB951072)
- Update for Windows XP (KB952287)

Buscar Actualizaciones Opcionales de Windows

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

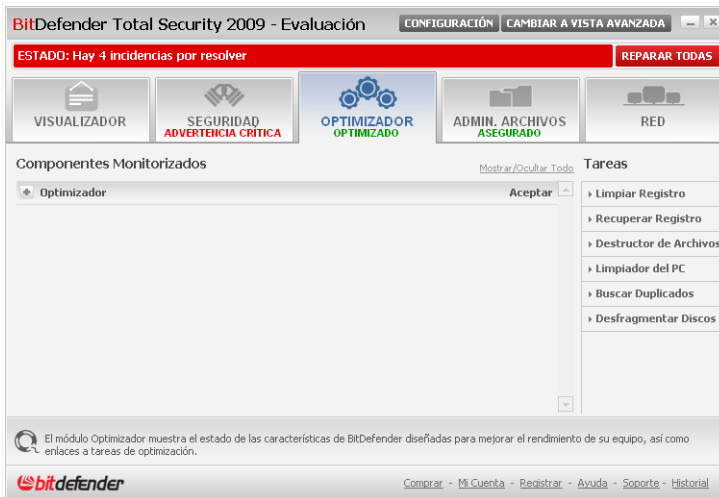
Haga clic en **Cerrar**.



7. Optimizador

BitDefender incluye un módulo Optimizador que le ayudará a mantener la integridad de su sistema. Las herramientas de mantenimiento que se ofrecen son muy importantes para mejorar el rendimiento de su sistema y administrar eficientemente el espacio de los discos duros.

Para realizar operaciones de mantenimiento en su PC, haga clic en la pestaña **Optimizador** y utilice las herramientas incluidas.



Optimizador

El módulo Optimizador consta de dos apartados:

- **Componentes Monitorizados** - Le permite ver la lista completa de las tareas de optimización monitorizadas. Puede elegir los módulos que desea monitorizar.
- **Tareas** - Aquí encontrará enlaces a las tareas de optimización más importantes: limpieza y recuperación del registro, eliminar archivos de forma permanente, limpieza de los archivos temporales de Internet y cookies, eliminar de archivos duplicados, desfragmentar discos locales.



7.1. Componentes Monitorizados

El componente monitorizado es: Optimizador.

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

7.1.1. Optimizador

Las incidencias relativas al rendimiento de su equipo 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>
Nunca ha realizado una limpieza del registro	El Limpiador del Registro analiza el Registro de Windows y elimina las claves inválidas. Realice una limpieza del registro de vez en cuando para mejorar el rendimiento de su equipo.
Nunca ha realizado una limpieza del equipo	Si realiza una limpieza del equipo de vez en cuando, mejorará su rendimiento. Realice una limpieza del equipo en el momento que considere oportuno.
Nunca ha ejecutado el buscador de archivos duplicados	El Buscador de Archivos Duplicados optimiza el espacio de su disco al buscar aquellos archivos duplicados en su sistema. Ejecútelo en el momento que considere oportuno.
Nunca ha realizado una desfragmentación del disco	El Desfragmentador de Disco reorganiza físicamente los datos del disco duro para que los fragmentos que componen cada archivo se almacenen juntos. Realice una desfragmentación del disco en el momento que considere oportuno.

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

Dispone de los siguientes botones:

- **Limpiar Registro** - inicia el asistente que le permitirá limpiar el Registro de Windows.
- **Recuperar Registro** - inicia el asistente que le permitirá recuperar las entradas del registro eliminadas.
- **Destruir Archivos** - inicia el asistente que le permitirá eliminar permanentemente archivos de su equipo.
- **Limpiar Temp. Internet** - inicia el asistente que le permite eliminar los archivos temporales de Internet y las cookies.
- **Buscar Duplicados** - inicia el asistente que le permite encontrar y eliminar archivos duplicados.
- **Desfragmentar Discos** - inicia el asistente que le permitirá desfragmentar los discos locales.

7.2.1. Limpiando el Registro

El Registro de Windows es una parte importante de los sistemas operativos Windows. Se trata de una base de datos que contiene información y configuración del hardware y aplicaciones instaladas, usuarios, preferencias de su equipo, entre otra información

Muchas aplicaciones escriben claves en el Registro de Windows cuando se instalan. Pero al desinstalarse, algunas de las claves asociadas no pueden eliminarse y permanecen en el Registro de Windows, ralentizando su ordenador o incluso causando fallos de estabilidad. Lo mismo ocurre cuando elimina accesos directos a determinados archivos, o si existen controladores corruptos.

Utilice el Limpiador del Registro para limpiar el Registro de Windows y mejorar el rendimiento de su sistema. El Limpiador del Registro analiza el Registro de Windows y elimina las claves inválidas.

Para limpiar el Registro de Windows, haga clic en la pestaña **Limpiar Registro**. Deberá completar un asistente guiado de cuatro pasos.

Paso 1/4 - Iniciar Análisis

Desde aquí puede iniciar el análisis del Registro.

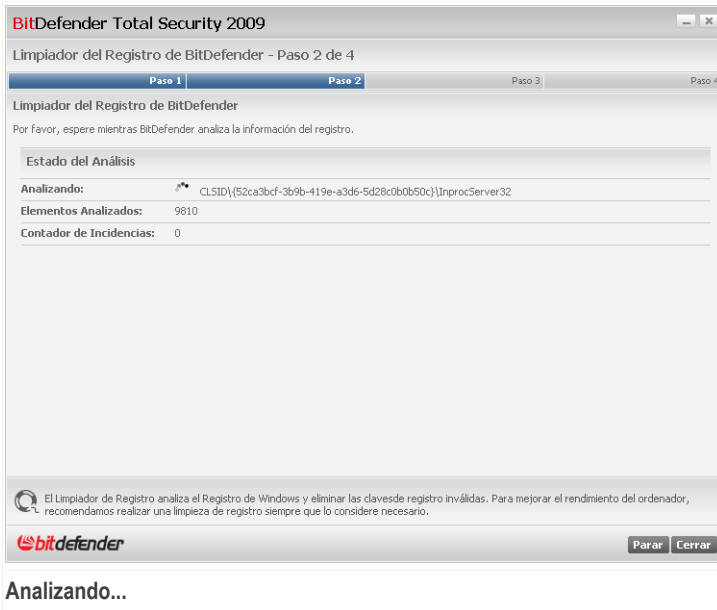


Puede ver cuándo se inició el Limpiador del Registro por última vez y las recomendaciones de BitDefender.

Haga clic en **Siguiente**.

Paso 2/4 - Analizando...

El Limpiador del Registro iniciará el análisis del registro.



Analizando...

Puede ver la última clave del registro analizada y estadísticas relacionadas con el análisis.

Espere a que el Registro de Windows finalice el análisis de claves. Si desea cancelar la operación, haga clic en **Cancelar**.



Nota

Si desea detener el análisis, haga clic en **Parar**. El asistente saltará al siguiente paso.

Paso 3/4 – Seleccione la acción

Una vez finalice el análisis de claves del registro, aparecerá una nueva ventana dónde podrá ver los resultados



Nota

Si no se ha detectado ninguna incidencia o ha decidido detener el análisis, se omitirá este paso del asistente.



BitDefender Total Security 2009

Limpiador del Registro de BitDefender - Paso 3 de 4

Paso 1 Paso 2 **Paso 3** Paso 4

Acción General

Elija la acción que se debe aplicar a estas claves. Puede configurar la acción general o la acción para cada clave.

Seleccionar categoría: Todas las Categorías ▾

Eliminar todas las claves (esta acción sobrescribirá la acción seleccionada en cada clave)

Acción por Clave

<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{3C4F38E7-47EB-101B-A3C9-08002B2F49FB}\InprocServer32
	Valor de la Clave: Nombre del valor:(Por defecto)
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{C27CE3C-8596-11D1-B16A-00C0F0283628}\InprocServer32
	Valor de la Clave: Nombre del valor:(Por defecto)
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{DFC09BAE-8185-31F2-AC1C-C4E437101217}\InprocServer32
	Valor de la Clave: Nombre del valor:CodeBase
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{DFC09BAE-8185-31F2-AC1C-C4E437101217}\InprocServer32\4.2.8.2
	Valor de la Clave: Nombre del valor:CodeBase
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\Installer\Products\0E23E40C6140D434FA9B96967D309AFE\SourceList
	Valor de la Clave: Nombre del valor>LastUsedSource
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls

El Limpiador de Registro analiza el Registro de Windows y elimina las claves de registro inválidas. Para mejorar el rendimiento del ordenador, recomendamos realizar una limpieza de registro siempre que lo considere necesario.

Siguiente Cerrar

Acciones

Podrá ver todas las claves del registro inválidas o huérfanas detectadas. Se le mostrará información detallada sobre cada clave (nombre, valor, prioridad, categoría).

Las claves del registro están agrupadas en función de su ubicación en el Registro de Windows.

Categoría	Descripción
Ubicaciones del Software	Claves del registro que contienen información sobre la ruta en la que están instaladas las aplicaciones de su equipo. Las claves inválidas tienen asignada una prioridad baja, lo cual significa que puede eliminarlas sin apenas riesgo alguno.
Controles Personalizados	Claves del registro que contienen información sobre las extensiones registradas en su equipo. Estas claves normalmente se utilizan para mantener las asociaciones de los archivos (para asegurarse que se inicia la



Categoría	Descripción
	<p>aplicación correcta al abrir un archivo desde el Explorador de Windows). Por ejemplo, una clave de este tipo le permitiría abrir un archivo .doc con Microsoft Word.</p> <p>Las claves inválidas tienen asignada una prioridad baja, lo cual significa que puede eliminarlas sin apenas riesgo alguno.</p>
DLLs Compartidas	<p>Claves del registro que contienen información sobre la ubicación de DLLs compartidas (Librerías de Conexión Dinámica). Las DLLs contienen funciones que las aplicaciones utilizan para realizar algunas tareas. Algunas DLLs se comparten para reducir los requisitos de espacio y memoria.</p> <p>Estas claves del registro dejan de ser válidas cuando la DLL a la que apuntan cambia de ubicación o se elimina (por ejemplo, al desinstalar un programa).</p> <p>Las claves del registro inválidas tienen asignadas una prioridad media, lo cual significa que eliminarlas puede afectar de forma negativa al sistema.</p>

Para realizar el proceso de limpieza de una forma más sencilla, seleccione una categoría del menú.

Puede elegir entre eliminar todas las categorías o sólo determinadas claves inválidas dentro de la categoría seleccionada. Si marca **Eliminar todas las claves**, todas las claves detectadas serán eliminadas. Si desea eliminar únicamente unas claves específicas, marque la opción **Eliminar** situada junto a la respectiva clave.



Nota

Por defecto, se eliminarán todas las claves inválidas detectadas.

Haga clic en **Siguiente**.

Paso 4/4 - Ver Resumen de Resultados

Aquí puede ver los resultados del análisis realizado por el Limpiador del Registro.



BitDefender Total Security 2009

Limpiador del Registro de BitDefender - Paso 4 de 4

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

Resumen de los Resultados

Debajo puede ver los resultados de la Limpieza del Registro.

Incidencias detectadas:	47
Claves eliminadas:	47
Claves omitidas:	0

Este es el resumen del proceso de limpieza del registro. Aquí puede ver el número de incidencias detectadas y el número de claves eliminadas o ignoradas.

Finalizar

Resumen de Resultados

Si ha decidido no eliminar todas las claves del registro, aparecerá una advertencia. Recomendamos revisar las incidencias correspondientes.

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

7.2.2. Recuperando Claves Eliminadas

En algunas ocasiones, después de la limpieza del registro, puede notar que su sistema no funciona correctamente o que algunas aplicaciones fallan a causa de claves registro que han sido eliminadas. Para solucionar el problema, debe recuperar las claves del registro eliminadas.

Para recuperar las claves del registro eliminadas, haga clic en **Recuperar Registro**. Deberá completar un asistente guiado de dos pasos.



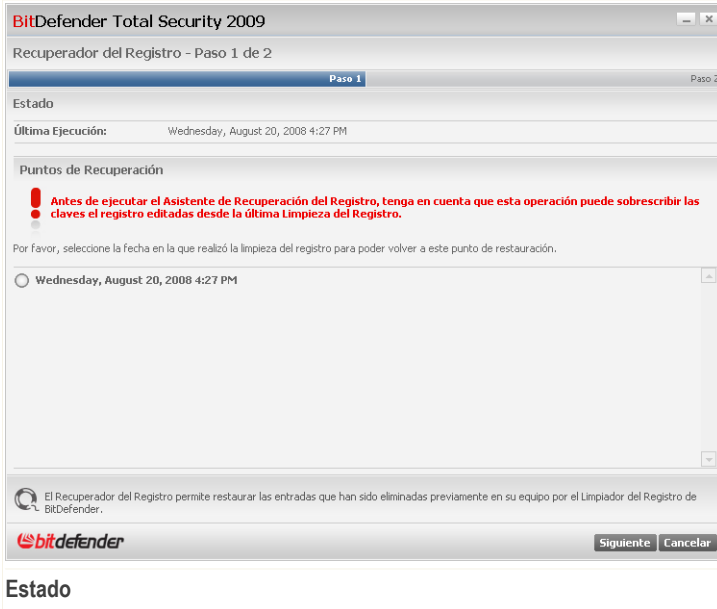
Importante

Sólo los usuarios con permisos de administrador pueden recuperar las claves eliminadas.



Paso 1/2 - Iniciar Recuperador del Registro

Desde aquí puede iniciar la recuperación del registro.



Podrá ver una lista de puntos en el tiempo en los que se realizó una Limpieza del Registro. Seleccione el punto en el tiempo sobre el que desea realizar la Recuperación del Registro.

Si está seguro que desea recuperar las claves eliminadas en ese momento, haga clic **Siguiente**.



Aviso

La recuperación de las claves eliminadas puede suponer sobrescribir las claves editadas desde la última vez que realizó la limpieza.

Paso 2/2 - Ver Resultados

Aquí puede ver si la recuperación se ha realizado con éxito.



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

7.2.3. Eliminando Archivos de Forma Permanente

Cuando elimina un archivo, ya no podrá volver acceder al mismo como lo hacía habitualmente. Sin embargo, el archivo continúa estando almacenado en su disco hasta que no se sobrescriba al copiar archivos nuevos.

Incluso cuando elimina un archivo, éste puede recuperarse utilizando programas especializados. Esto podría representar una amenaza para su privacidad si alguien intenta obtener sus datos privados.

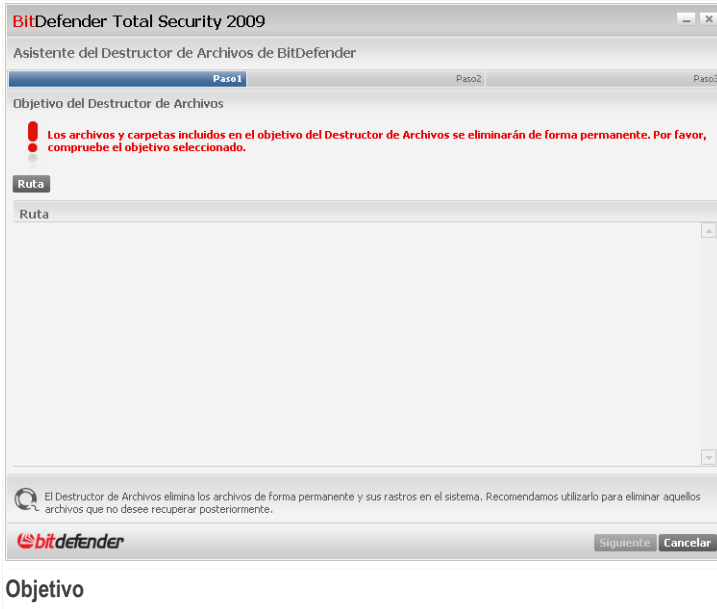
Para impedir la recuperación de datos confidenciales después de eliminarlos, puede utilizar BitDefender. BitDefender eliminará de forma permanente estos datos, al suprimirlos físicamente del disco duro.

Para eliminar archivos de forma permanente, haga clic **Destruir Archivos**. Deberá completar un asistente guiado de tres pasos.



Paso 1/3 - Seleccionar Objetivo

Aquí puede especificar los archivos y carpetas que se eliminarán de forma permanente.



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



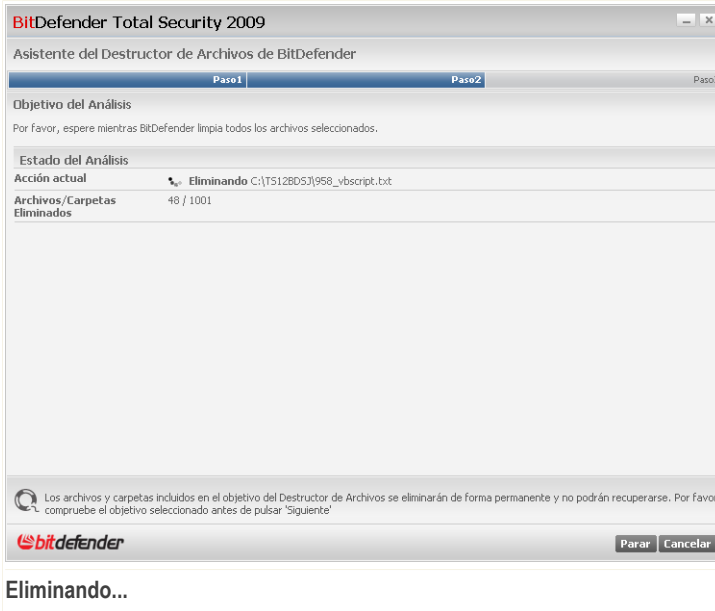
Nota

Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiente**.

Paso 2/3 - Eliminando Archivos...

BitDefender eliminará de forma permanente los archivos de las ubicaciones indicadas.



Espere a que la operación de destrucción de archivos se complete. Si desea cancelar la operación, haga clic en **Cancelar**.

Paso 3/3 - Ver Resumen de Resultados

Una vez se hayan eliminado los archivos, aparecerá una nueva ventana dónde podrá ver los resultados.



BitDefender Total Security 2009

Asistente del Destructor de Archivos de BitDefender

Paso1 Paso2 Paso3

Resumen de los Resultados

¡Todos los archivos y carpetas marcados han sido eliminados de forma permanente!

Archivos Eliminados	1
Carpetas Eliminadas	1
Archivos NO Eliminados	0
Carpetas NO Eliminadas	0

Este es un resumen del proceso de destrucción de archivos. Aquí puede ver el número de archivos y carpetas eliminados, junto con aquellos que no han podido eliminarse.

bitdefender Cerrar

Resumen de Resultados

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

7.2.4. Limpiando los Archivos de Internet

Cada vez que visita una página web se almacenan archivos temporales de Internet que permiten visualizar la página más rápidamente durante la próxima visita.

A pesar de tratarse de archivos temporales, éstos no se eliminan después de cerrar el navegador. Esto podría considerarse como un fallo de privacidad, ya que cualquier persona que acceda a su ordenador podría ver estos archivos. Con el tiempo, estos archivos acaban ocupando un espacio considerable en su disco y consumen espacio libre.

Las cookies también se almacenan en su ordenador cuando visita una página web. Las cookies son pequeños archivos que contienen información sobre sus preferencias de navegación. También pueden suponer un problema de privacidad, ya que pueden analizarse por los anunciantes para determinar sus intereses y preferencias al navegar.



Al eliminar los archivos temporales de Internet y las cookies, liberará espacio en el disco y protegerá su privacidad.

Para limpiar la carpeta de Archivos temporales de Internet, donde Internet Explorer almacena sus archivos temporales y cookies, haga clic en **Limpiar Archivos Temporales de Internet**. Deberá completar un asistente guiado de tres pasos.

Paso 1/3 – Iniciar Eliminación

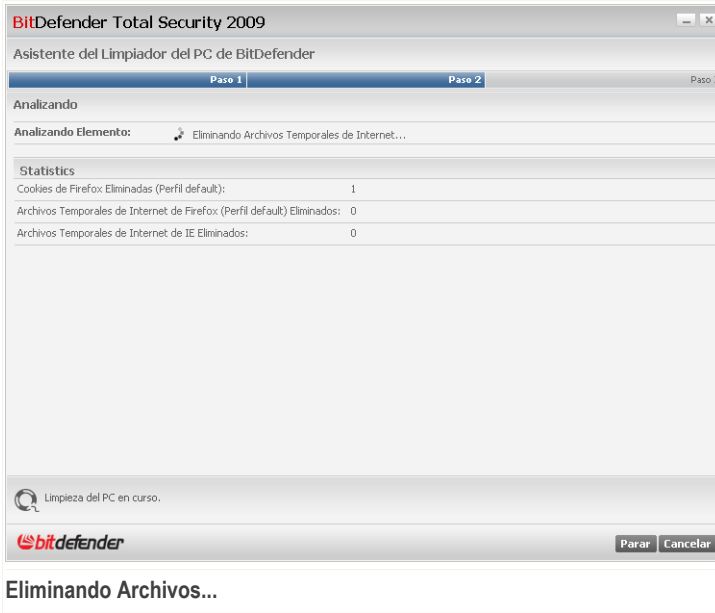
Desde aquí puede iniciar la limpieza de sus archivos temporales de Internet y cookies.



Haga clic en **Siguiente**.

Paso 2/3 - Eliminando Archivos...

El limpiador empezará a eliminar los archivos temporales de Internet y cookies.



Espere a que el Limpiador finalice la limpieza de los archivos temporales de Internet y las cookies. Si desea cancelar la operación, haga clic en **Cancelar**.

Paso 3/3 - Ver Resumen de Resultados

Una vez finalice la limpieza de los archivos, aparecerá una nueva ventana dónde podrá ver los resultados.



Puede ver las estadísticas de los objetos eliminados.
Haga clic en **Aceptar** para cerrar la ventana.

7.2.5. *Buscar Duplicados*

Los archivos duplicados consumen espacio en el disco duro. Piense qué ocurriría si tuviera el mismo archivo .mp3 almacenado en tres carpetas diferentes.

Para detectar y eliminar los archivos duplicados en su equipo puede utilizar el Buscador de Duplicados. De este modo conseguirá más espacio libre en sus discos duros.

Para buscar archivos duplicados, haga clic en **Buscar Duplicados**. Deberá completar un asistente guiado de cuatro pasos.

Paso 1/4 – Seleccione el Objetivo de Búsqueda

Aquí puede indicar dónde buscar los archivos duplicados.



Haga clic en **Ruta** y seleccione la ubicación en la que el Buscador de Duplicados deberá buscar archivos duplicados. La rutas de los elementos seleccionados aparecerá en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento.



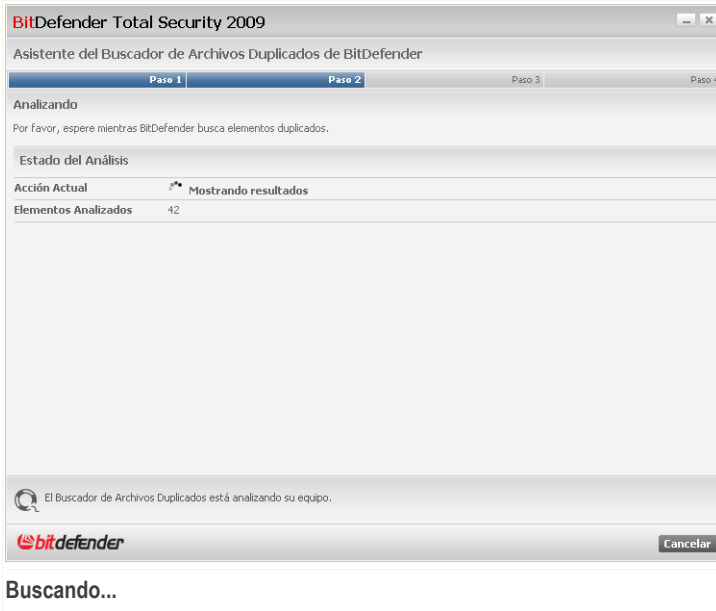
Nota

Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiete**.

Paso 2/4 - Buscando...

El Buscador de Duplicados iniciará la búsqueda de archivos duplicados.



Puede ver el estado de la búsqueda y las estadísticas.

Espere a que el Buscador de Duplicados complete la búsqueda. Si desea cancelar la operación, haga clic en **Cancelar**.

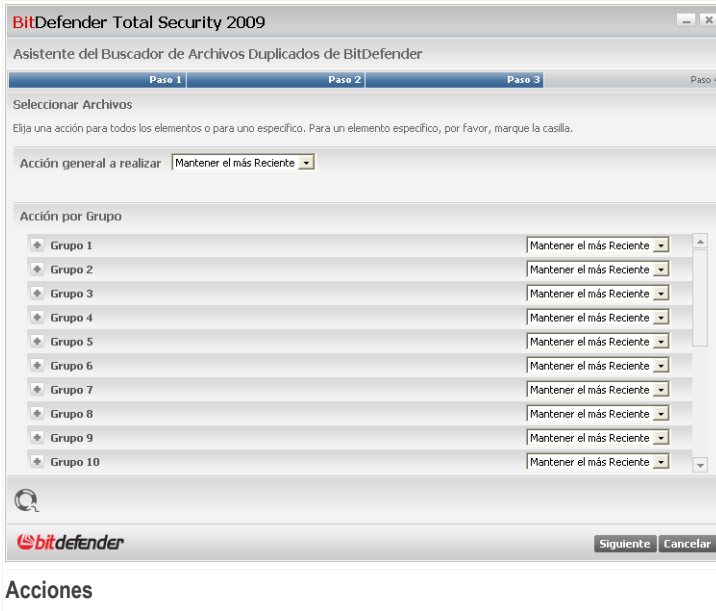
Paso 3/4 – Seleccione la acción

Una vez finalice la búsqueda, aparecerá una nueva ventana dónde podrá indicar las acciones a realizar con los archivos duplicados detectados.




Nota

Si no se encuentran archivos duplicados, puede saltarse este paso.



Acciones

Los archivos duplicados detectados están organizados en grupos. Si hace clic en el botón  situado junto a un grupo, verá información sobre los archivos duplicados (ruta completa, tamaño, fecha de creación y modificación).

Puede seleccionar una acción global que se aplicará a todos los archivos duplicados que se detecten, pero también puede seleccionar una acción para cada uno de los grupos. Dispone de las siguientes opciones en el menú:

Acción	Descripción
Guardar los más nuevos	Los archivos duplicados más recientes se mantendrán, mientras que los otros archivos duplicados se eliminarán.
Guardar los más antiguos	Los archivos duplicados de mayor antigüedad se mantendrán, mientras que los otros archivos duplicados se eliminarán.
Ninguna acción	No se aplicará ninguna acción sobre los archivos duplicados.



Si desea aplicar una acción global a todos los objetos del grupo, seleccione la acción deseada desde el menú correspondiente. Si sólo quiere eliminar algunos de los archivos del grupo, marque la casilla **Eliminar** cercana a cada uno de los archivos a eliminar.



Nota

La acción global no sobrescribirá la acción que ha elegido para algunos archivos o grupos en concreto. Por ejemplo, si selecciona **Guardar los más nuevos** como acción global, pero modifica la acción de un archivo o grupo, se aplicará la acción global a todos los archivos excepto en los que haya seleccionado una acción particular.

Haga clic en **Siguiente**.

Paso 4/4 - Ver Resumen de Resultados

Aquí podrá ver los resultados del análisis del Buscador de Duplicados.

The screenshot shows the 'Asistente del Buscador de Archivos Duplicados de BitDefender' window. It has a progress bar with four steps: Paso 1, Paso 2, Paso 3, and Paso 4 (selected). The main content area is titled 'Resumen de los Resultados' and contains the following text: 'No se ha eliminado ningún archivo. Abajo puede ver las estadísticas de esta tarea de buscador de duplicados. Puede ejecutar el asistente en cualquier momento desde el apartado Optimizador, Panel de tareas'. Below this is a table with the following data:

Elementos analizados	2
Grupos de Archivos Duplicados	1
Archivos Duplicados	2

At the bottom of the window, there is a footer with the BitDefender logo, a 'Ejecutar de nuevo' button, and a 'Cerrar' button. Below the screenshot, the text 'Resumen de Resultados' is repeated.

Haga clic en **Repetir** para iniciar una nueva búsqueda de archivos duplicados, o pulse **Aceptar** para cerrar la ventana.



7.2.6. Desfragmentando los Discos Duros

Cuando copia un archivo con un tamaño superior al bloque de espacio libre más grande, se produce una fragmentación del archivo. Al no existir el espacio suficiente para almacenar el archivo de forma íntegra, éste se fragmenta en varios bloques. Cuando accede al archivo fragmentado, los datos se leen desde las diferentes ubicaciones donde se encuentran los bloques que forman el archivo.

La fragmentación de los archivos reduce la velocidad de acceso al archivo, disminuye el rendimiento del sistema y acelera el desgaste del disco duro.

Para reducir la fragmentación de los archivos debe desfragmentar los discos periódicamente. La desfragmentación reorganiza físicamente los datos del disco duro, ordenando los fragmentos de los archivos uno detrás de otro. También crea espacios de espacio disco para prevenir la desfragmentación de nuevos archivos.

Se recomienda desfragmentar el disco duro para:

- acceder a los archivos con más rapidez.
- mejorar el rendimiento global del equipo.
- prolongar la vida del disco duro.

Para desfragmentar el disco duro, haga clic en **Desfragmentar Discos**. Deberá completar un asistente guiado de tres pasos.



Nota

La desfragmentación del disco puede llevar un tiempo, dado que implica mover porciones de datos almacenados de un sitio a otro. Recomendamos realizar la desfragmentación cuando no esté utilizando el ordenador.

Paso 1/3 - Analizando...

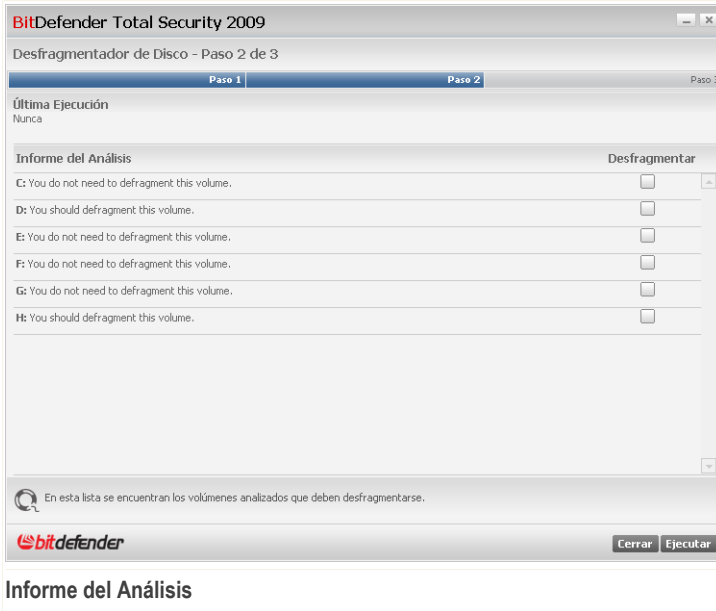
El Desfragmentador de Disco analizará el disco duro para determinar si es necesaria o no la desfragmentación.



Espere a que el Desfragmentador de Disco finalice el análisis. Si desea cancelar la operación, haga clic en **Cancelar**.

Paso 2/3 - Ver Informe del Análisis

Una vez se ha completado el análisis, aparecerá una nueva ventana dónde podrá ver los resultados e iniciar la desfragmentación del disco, en caso necesario.



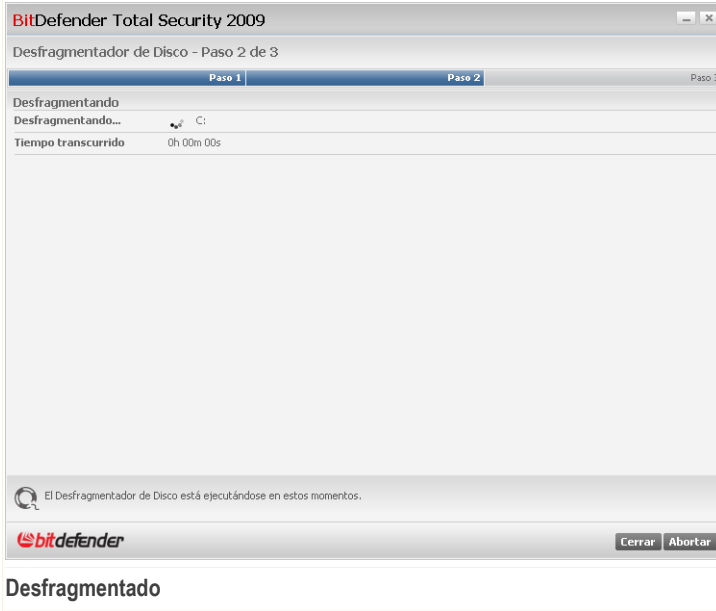
Compruebe el informe de análisis.

Si ningún volumen de disco necesita desfragmentación, haga clic en **Cerrar** para cerrar la ventana. De lo contrario, seleccione la opción **Desfragmentar** correspondiente al volumen de disco que necesita desfragmentación y haga clic en **Ejecutar** para iniciar la desfragmentación.



Nota

El Desfragmentador de Disco necesitará un 15% de espacio libre en el disco para poder funcionar correctamente. Si no hay espacio suficiente en el disco, la desfragmentación se cancelará.



Espere a que la desfragmentación del disco finalice. Puede cancelar la desfragmentación del disco en cualquier momento haciendo clic en **Abortar**.

Paso 3/3 - Ver Informe de la Desfragmentación

Una vez se complete la desfragmentación del disco, aparecerá una nueva ventana dónde podrá ver las estadísticas de la desfragmentación.



BitDefender Total Security 2009

Desfragmentador de Disco - Paso 3 de 3

Paso 1 Paso 2 Paso 3

Informe de la desfragmentación

Disco

C: Defragmentation was cancelled by the user.

Ha decidido cancelar el proceso de desfragmentación del disco. Puede iniciarlo de nuevo en cualquier momento desde el apartado Optimizador, Panel de tareas

Este es un resumen de las acciones realizadas por el Desfragmentador de Disco. El Desfragmentador re-organiza los datos del disco duro, de modo que los fragmentos que componen cada archivo se almacenen juntos.

 **Aceptar**

Informe de la Desfragmentación

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



8. Administrador de Archivos

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

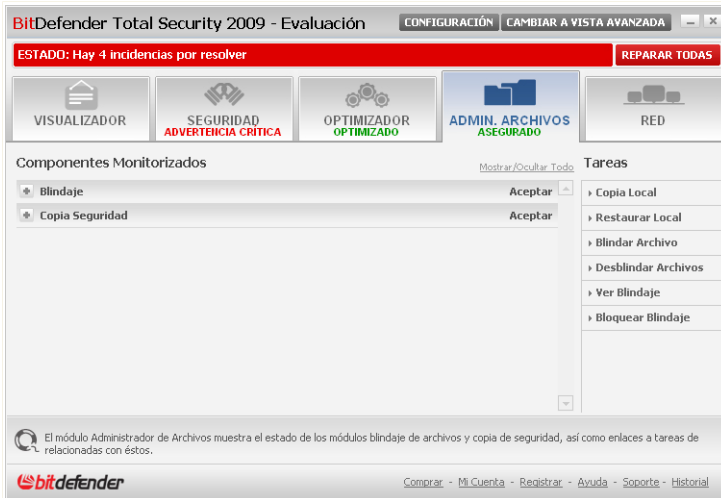
Copia de Seguridad. La protección antivirus por sí sola no es suficiente para proteger sus datos más valiosos. Imagine que su sistema está libre de virus, pero que de algún modo, el equipo falla en el momento que más lo necesita. En este tipo de situaciones es donde el apartado Administrador de Archivos resulta sumamente útil. Con BitDefender puede realizar copias de seguridad de forma segura.

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

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

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

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



Administrador de Archivos

El módulo Administrador de Archivos consta de dos apartados:

- **Componentes Monitorizados** - Le permite ver la lista completa de todos los componentes monitorizados por cada módulo de seguridad. Puede elegir los módulos que desea monitorizar. Recomendamos activar la monitorización de todos los componentes.
- **Tareas** - Aquí encontrará enlaces a las tareas de seguridad más importantes: copia de seguridad local, restauración y blindaje de archivos.

8.1. Componentes Monitorizados

Los componentes monitorizados se agrupan en varias categorías.

El componente monitorizado es el siguiente:

Categoría	Descripción
Blindaje de archivos	Es un área de almacenamiento protegida, situada dentro de su equipo, en la que puede guardar información personal o archivos confidenciales. Al estar cifrada, los documentos que



Categoría	Descripción
	contenga no serán vulnerables a tentativas de robo o agujeros de seguridad.
Copia de Seguridad	Le permite realizar copias de los documentos importantes almacenados su sistema. Recomendamos utilizar esta característica para almacenar sus datos de forma segura.

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

8.1.1. Blindaje de archivos

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

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

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

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

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

8.1.2. Copia de Seguridad

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



<i>Incidencia</i>	<i>Descripción</i>
Hace x día(s) que realizó una tarea de copia offline	El módulo de copia offline le permite realizar copias de los documentos importantes almacenados su sistema.

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

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

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

8.2. Tareas

Dispone de los siguientes botones:

- **Copia Local** - inicia el asistente que le permite realizar copias de los datos más importantes en su equipo, en un CD, en una ubicación de la red o en otro disco duro.
- **Restauración Local** - inicia el asistente que le permite recuperar los datos copiados en su equipo, en un CD, en una ubicación de la red o en otro disco duro.
- **Configuración de Copia** - desde aquí puede configurar e iniciar las operaciones de copia con más detalle.



Nota

Para más información, por favor, consulte el capítulo *“Copias de Seguridad Avanzadas”* (p. 300).

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

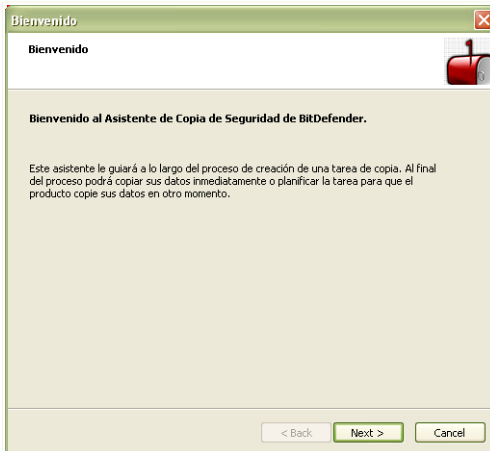


8.2.1. Realizando Copias de Seguridad Locales

Al hacer clic en **Copia Local** se iniciará un asistente que le guiará a través del proceso de creación de tareas de copia de seguridad. Al final del proceso será capaz de copiar sus datos al instante o planificar una tarea para que el producto realice la copia automáticamente en otro momento.

Paso 1/5 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

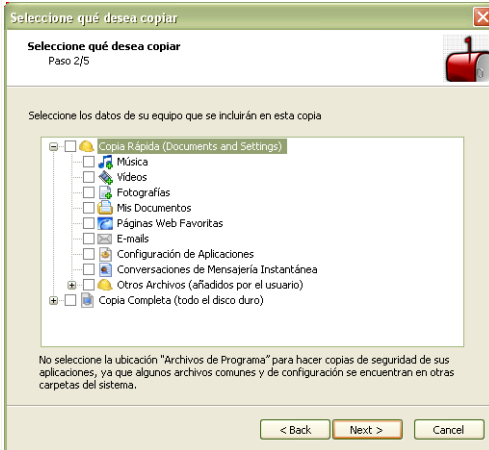


Ventana de Bienvenida

Haga clic en **Siguiente**.

Paso 2/5 - Seleccionar los datos a Copiar

Desde aquí puede seleccionar los datos de su ordenador que desea copiar.



Selección de los datos a Copiar

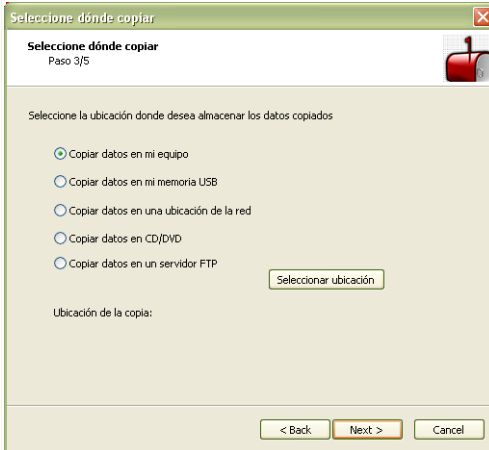
Puede elegir entre **Copia Rápida** (su música, vídeos, fotografías, emails, configuración de aplicaciones, etc.) y **Copia Completa** (todas las particiones).

Haga clic en **Otros archivos**, para añadir otros archivos de su Escritorio a la **Copia Rápida**. La **Copia Completa** puede personalizarse fácilmente seleccionando las carpetas que desea copiar.

Haga clic en **Siguiente**.

Paso 3/5 - Seleccionar donde hacer Copia

Aquí puede seleccionar la ubicación dónde se guardarán los datos copiados.



Seleccione donde hacer la copia

Dispone de las siguientes opciones:

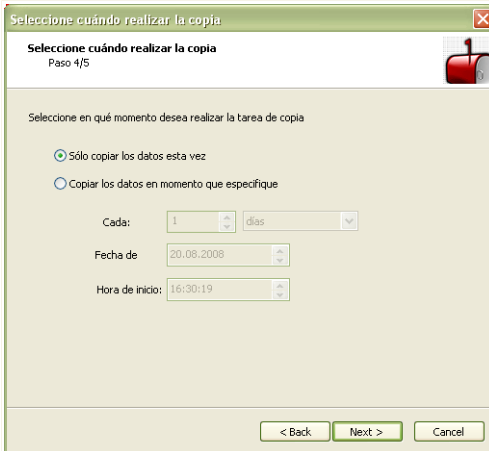
- Copiar datos en mi equipo
- Copiar datos en mi memoria USB
- Copiar datos en una ubicación de la red
- Copiar datos en CD/DVD
- Copiar datos en un servidor FTP

Si decide guardar los datos copiados en su equipo, una memoria USB o una ubicación de la red, haga clic en **Seleccionar ubicación** e indique dónde quiere guardar los datos.

Haga clic en **Siguiente**.

Paso 4/5 - Seleccionar cuando realizar la Copia

Desde aquí podrá seleccionar el momento en que desea realizar la copia de sus datos.



Seleccionar cuando realizar copia

Dispone de las siguientes opciones:

- **Sólo copiar datos esta vez**
- **Copiar datos y planificar la tarea**

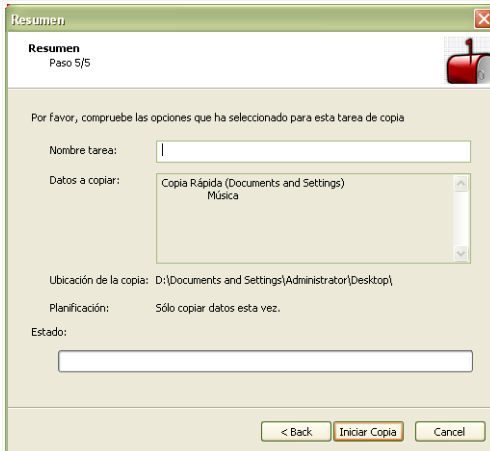
Para copiar sus datos inmediatamente haga clic en **Sólo copiar datos esta vez**. Si desea programar el producto para que realice la copia automáticamente en otro momento, haga clic en **Copiar datos y planificar la tarea**.

Si selecciona **Copiar datos y planificar la tarea**, puede indicar la frecuencia con las que se realizará la copia: diariamente o semanalmente. Además, puede indicar la fecha y hora de inicio.

Haga clic en **Siguiente**.

Paso 5/5 - Resumen

Desde aquí puede revisar la configuración de la tarea.



Resumen

Debe introducir el nombre de la tarea en el campo correspondiente.

Haga clic en **Iniciar copia** si está de acuerdo con la configuración detallada.

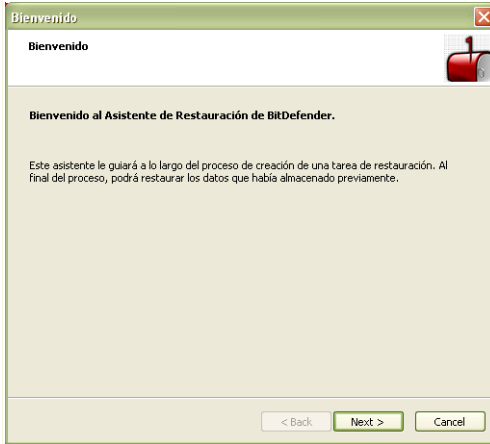
Haga clic en **Finalizar**.

8.2.2. Restaurando las Copias de Seguridad Locales

Al hacer clic en **Restauración Local** se iniciará un asistente que le guiará a través del proceso de restauración de sus datos copiados.

Paso 1/4 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

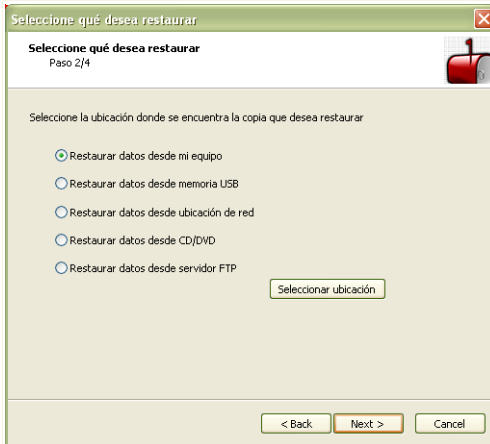


Ventana de Bienvenida

Haga clic en **Siguiente**.

Paso 2/4 - Seleccione la Copia a restaurar

Aquí puede seleccionar la ubicación desde dónde desea restaurar los archivos.



Seleccione la Copia a restaurar

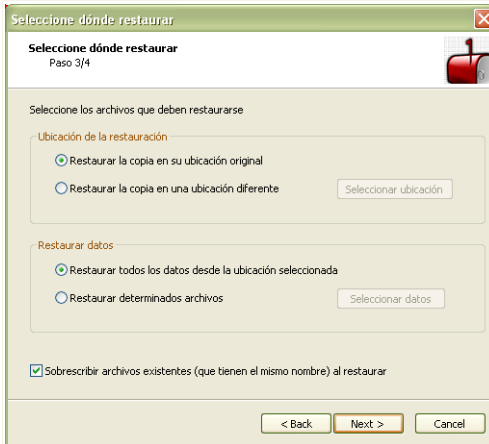
Dispone de las siguientes opciones:

- Restaurar datos desde mi equipo
- Restaurar datos desde memoria USB
- Restaurar datos desde ubicación de red
- Restaurar datos desde CD/DVD
- Restaurar datos desde servidor FTP

Haga clic en **Siguiente**.

Paso 3/4 - Seleccionar la Ubicación de Restauración y los Archivos

Aquí puede especificar los archivos que desea restaurar y la ubicación dónde desea restaurarlos.



Seleccionar la Ubicación de Restauración y los Archivos

Dispone de las siguientes opciones:

- Restaurar la copia a su ubicación original
- Restaurar la copia en una ubicación diferente
- Restaurar todos los datos desde la ubicación de copia seleccionada
- Restaurar archivos específicos
- Sobrescribir los archivos existentes al restaurar

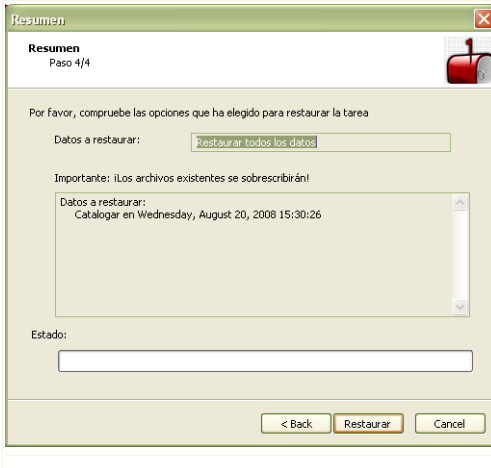
Si desea restaurar los datos en otra carpeta, o restaurar únicamente determinados archivos, seleccione la ubicación y los datos haciendo clic en el botón correspondiente.

Para evitar sobrescribir los archivos existentes al realizar la restauración, desmarque la casilla **Sobrescribir los archivos existentes al restaurar**.

Haga clic en **Siguiente**.

Paso 4/4 - Resumen

Desde aquí puede revisar la configuración de la tarea de restauración.



Haga clic en **Restaurar** si está de acuerdo con la configuración detallada.

Haga clic en **Finalizar**.

8.2.3. Añadiendo Archivos al Blindaje

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

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

Paso 1/6 - Seleccione el Objetivo

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



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



Nota

Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiente**.

Paso 2/6 - Seleccione el Blindaje

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



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

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

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

Haga clic en **Siguiente**.

Paso 3/6 – Crear un Blindaje

Aquí puede especificar la información del nuevo Blindaje.



BitDefender 2009

Blindaje - Blindar Archivo

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

Crear Blindaje

Por favor especifique la nueva contraseña del blindaje de archivos y configure su ubicación y su capacidad.

Introducir ruta del Blindaje de Archivos: **Explorar**

Letra de la Unidad: J: ▾

Introducir contraseña del Blindaje de Archivos: La contraseña debe tener como mínimo 8 caracteres.

Confirmar contraseña del Blindaje de Archivos:

Introducir tamaño del Blindaje (MB): 50 El tamaño sólo debe contener números.

Indica la letra de la unidad para abrir el Blindaje de Archivos.

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

Creación del Blindaje

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

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



Nota

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

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



Nota

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

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



Nota

La contraseña debe contener 8 caracteres como mínimo.

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



Nota

El tamaño sólo debe contener dígitos.

Haga clic en **Siguiente**.

Se le dirigirá al paso 5.

Paso 4/6 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.

BitDefender 2009

Blindaje - Blindar Archivo

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

Solicitar Contraseña del Blindaje

Por Favor, introduzca la contraseña del blindaje seleccionado.

Contraseña: La contraseña debe tener como mínimo 8 caracteres.

Ir al siguiente paso del asistente.

Atrás **Siguiente** **Cancelar**

Confirmar contraseña



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

Paso 5/6 - Resumen

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

Finalizar	
Operación	Añadir 1 Archivos/Carpetas a nuevo Blindaje
Nombre	fvtest2
Ruta	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Estado	Bloqueado

Por favor, revise las operaciones seleccionadas y haga clic en **Siguiente** si desea continuar.
Haga clic en **Atrás** si desea realizar algún cambio.

Ir al siguiente paso del asistente.

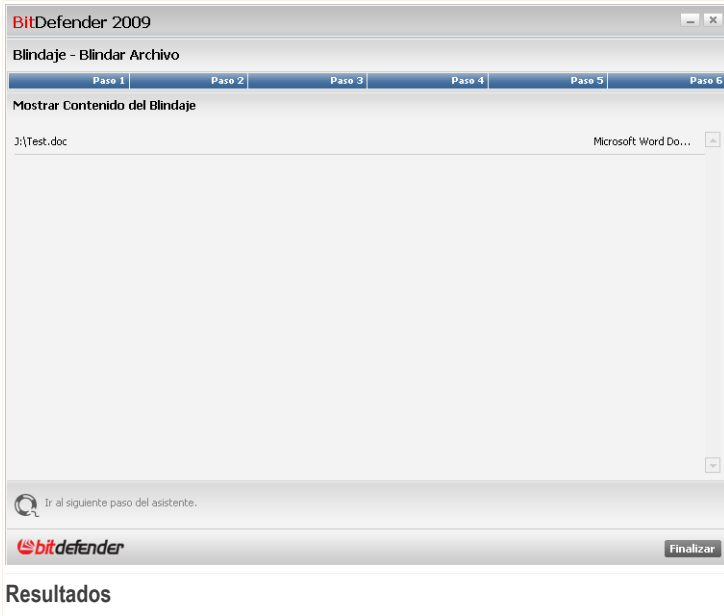
bitdefender Atrás Siguiente Cancelar

Resumen

Haga clic en **Siguiente**.

Paso 6/6 – Resultados

Aquí puede ver el contenido del blindaje.



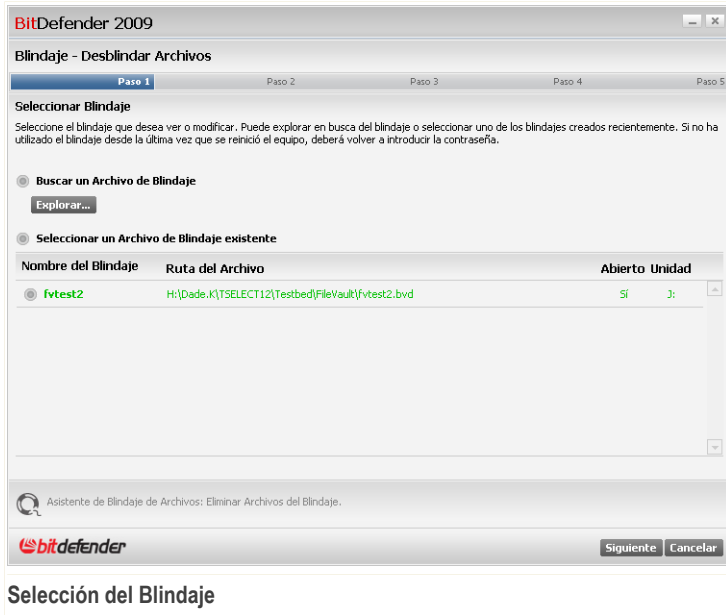
Haga clic en **Finalizar**.

8.2.4. Eliminando Archivos del Blindaje

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

Paso 1/5 - Seleccione un Blindaje

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



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

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

Haga clic en **Siguiente**.

Paso 2/5 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.



BitDefender 2009

Blindaje - Desblindar Archivos

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5

Solicitar Contraseña del Blindaje

Por favor, introduzca la contraseña del blindaje seleccionado.

Contraseña: La contraseña debe tener como mínimo 8 caracteres.

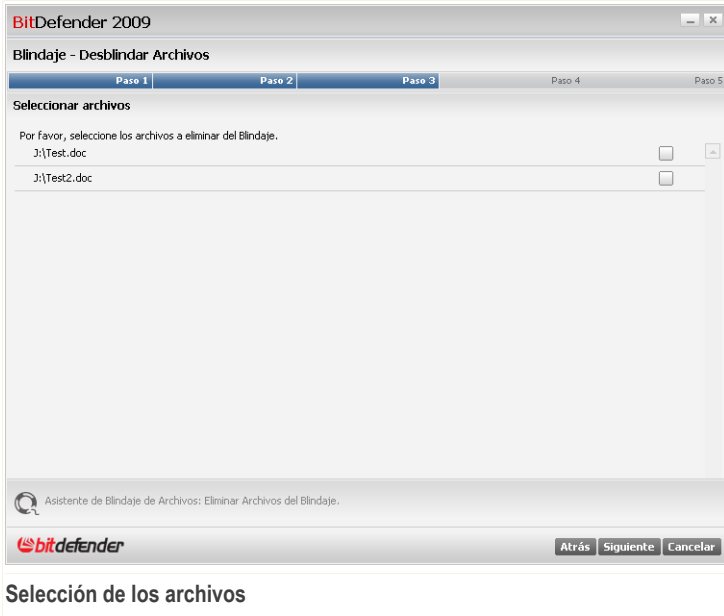
Ir al siguiente paso del asistente.

Confirmar contraseña

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

Paso 3/5 – Seleccione los Archivos

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



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

Paso 4/5 - Resumen

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



BitDefender 2009

Blindaje - Desblindar Archivos

Paso 1 Paso 2 Paso 3 Paso 4 Paso 5

Finalizar

Operación	Quitar 0 archivos del Blindaje
Nombre	fvtest2
Ruta	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Estado	Abierto en J:

Por favor, revise las operaciones seleccionadas y haga clic en **Siguiente** si desea continuar.
Haga clic en **Atrás** si desea realizar algún cambio.

Ir al siguiente paso del asistente.

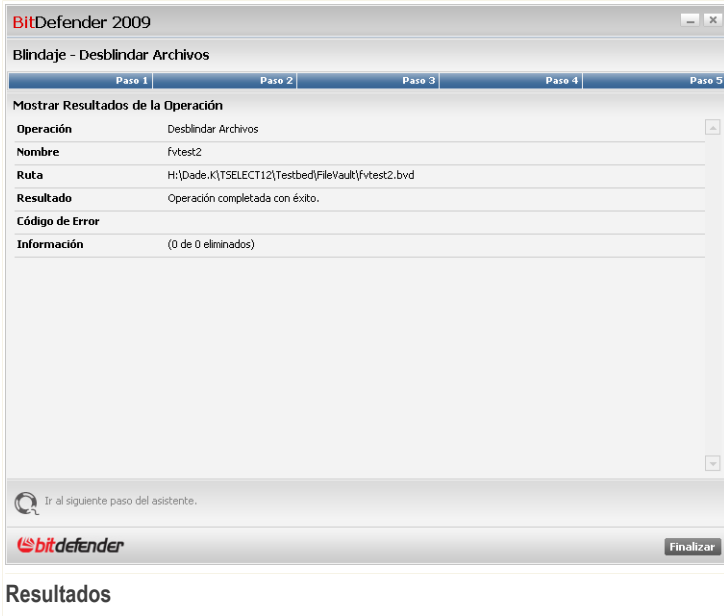
Atrás Siguiente Cancelar

Resumen

Haga clic en **Siguiente**.

Paso 5/5 – Resultados

Aquí puede ver los resultados de la operación.



Haga clic en **Finalizar**.

8.2.5. Visualizando los Archivos del Blindaje

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

Paso 1/4 - Seleccione el Blindaje

Aquí puede especificar el blindaje cuyo contenido desea visualizar.



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

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

Haga clic en **Siguiente**.

Paso 2/4 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.



BitDefender 2009

Blindaje - Ver Blindaje


Paso 1 Paso 2 Paso 3 Paso 4

Solicitar Contraseña del Blindaje

Por favor, introduzca la contraseña del blindaje seleccionado.

Contraseña: La contraseña debe tener como mínimo 8 caracteres.

Indique la contraseña de acceso al Blindaje.



Confirmar contraseña

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

Paso 3/4 - Resumen

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



BitDefender 2009

Blindaje - Ver Blindaje

Paso 1 Paso 2 Paso 3 Paso 4

Finalizar

Operación	Ver Contenido del Blindaje
Nombre	fvtest2
Ruta	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Estado	Bloqueado

Por favor, revise las operaciones seleccionadas y haga clic en **Siguiente** si desea continuar.
Haga clic en **Atrás** si desea realizar algún cambio.

Ir al siguiente paso del asistente.

Atrás **Siguiente** **Cancelar**

Resumen

Haga clic en **Siguiente**.

Paso 4/4 – Resultados

Desde aquí puede ver los archivos que contiene el blindaje.



Haga clic en **Finalizar**.

8.2.6. Bloqueando un Blindaje

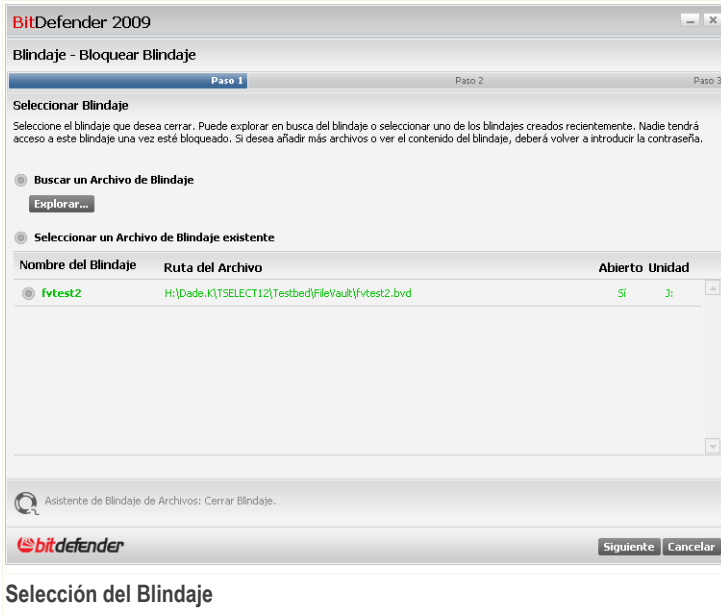
El blindaje de archivos se basa en un archivo (archivo de blindaje) almacenado en su equipo con extensión `bvd`. Este archivo puede abrirse (montar unidad) o bloquearse (desmontar unidad).

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

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

Paso 1/3 - Seleccione el Blindaje

Aquí puede indicar el blindaje que desea bloquear.



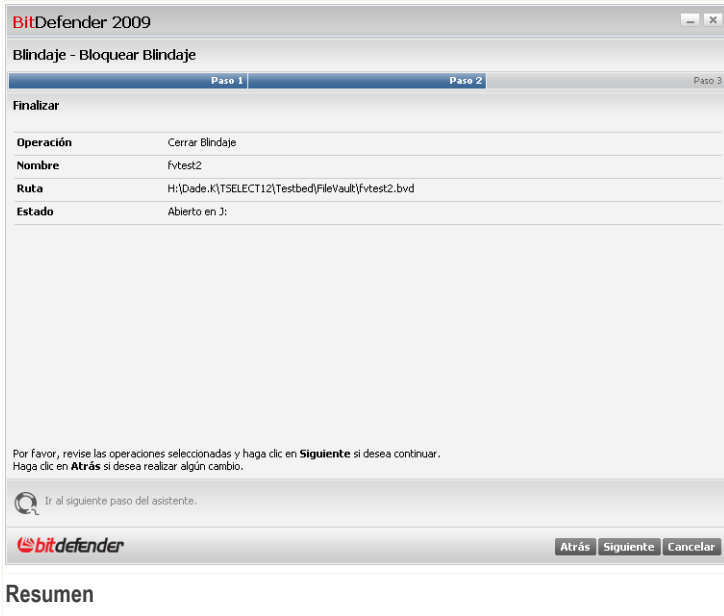
Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje.

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

Haga clic en **Siguiente**.

Paso 2/3 - Resumen

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



Haga clic en **Siguiente**.

Paso 3/3 – Resultados

Aquí puede ver los resultados de la operación.



BitDefender 2009

Blindaje - Bloquear Blindaje

Paso 1 | Paso 2 | Paso 3

Mostrar Resultados de la Operación

Operación	Cerrar Blindaje
Nombre	fvtest2
Ruta	H:\Dade.K\TSELECT12\Testbed\FileVault\fvtest2.bvd
Resultado	Operación completada con éxito.
Código de Error	
Información	Archivo de blindaje bloqueado con éxito.

Ir al siguiente paso del asistente.

Finalizar

Resultados

Haga clic en **Finalizar**.



9. Red

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

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

The screenshot shows the BitDefender Total Security 2009 interface. At the top, there is a navigation bar with 'RED' selected. Below it, a status bar indicates 'ESTADO: Hay 4 incidencias por resolver'. The main area is divided into several sections: 'INTERNET' with a globe icon and IP address '10.10.0.1', a network diagram showing a central hub connected to three nodes, and a 'Tareas' section with a dropdown menu. The interface also includes a footer with the BitDefender logo and navigation links.

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.

Introduzca una contraseña

Se requiere una contraseña para unirse a o crear una red por razones de seguridad (protegerá el acceso a su equipo a través de la red de administración).

Introduzca la contraseña:

Repita la contraseña:

OK Cancelar

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.

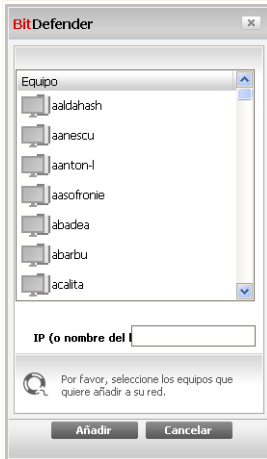
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

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

The screenshot shows a dialog box titled "BitDefender". Inside, 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

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.



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" with the text "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 is a checkbox with the text "No volver a mostrar este mensaje durante esta sesión." At the bottom right 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.

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.

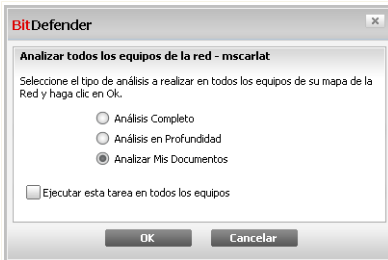
This is an identical screenshot to the one above, showing the BitDefender password prompt dialog box with the text "Debe introducir la contraseña de administración de red.", a password field with seven dots, a checkbox for "No volver a mostrar este mensaje durante esta sesión.", and "OK" and "Cancelar" buttons.

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.



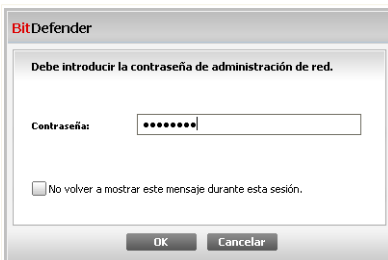
Selección del Tipo de Análisis

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



Categoría	Descripción
Configuración del Blindaje de Archivos	Desde aquí puede activar / desactivar el Blindaje de Archivos.
Configuración General	Desde aquí puede activar / desactivar el modo juego, portátil, contraseñas, barra de actividad del análisis y otras opciones.

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

10.1. Seguridad local

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

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

10.2. Seguridad online

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



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

10.3. Configuración del Control Parental

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

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

10.4. Configuración de la Red

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

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



10.5. Configuración del Blindaje de Archivos

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

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

10.6. Configuración General

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

Elemento	Descripción
Modo Juego	El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
Modo Portátil	El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.
Contraseña de la Configuración	Al activar esta opción, protegerá la configuración de BitDefender de modo que sólo pueda modificarla la persona que conozca la contraseña.
Contraseña del Control Parental	Al activar esta opción, puede restringir la configuración del Control Parental, de modo que sólo pueda cambiar la configuración la persona que conozca la contraseña.
BitDefender News	Active esta opción si desea recibir noticias importantes sobre BitDefender, las actualizaciones del producto y las nuevas amenazas de seguridad.
Alertas de Notificación del Producto	Al activar esta opción, recibirá alertas de información sobre la actividad del producto.
Barra de Actividad del Análisis	La Barra de Actividad del Análisis le muestra el progreso de la actividad del análisis de BitDefender. La barra gris representa la actividad de análisis de su equipo, la barra naranja representa la actividad de su equipo en Internet.



<i>Elemento</i>	<i>Descripción</i>
Cargar BitDefender al iniciar Windows	Al activar esta opción, la interfaz de BitDefender se cargará al iniciar el sistema. Esta opción no afecta al nivel de protección.
Enviar Informes de Virus	Al activar esta opción, enviará informes de análisis virus a los Laboratorios BitDefender para su análisis. Los informes no contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.
Detección de Epidemias	Al activar esta opción, enviará informes sobre amenazas potenciales a los Laboratorios BitDefender para su análisis. Los informes no contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.



11. Barra de Estado

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

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



Barra de Estado

11.1. Seguridad local

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



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

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

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**.



<i>Incidencia</i>	<i>Descripción</i>
Protección en tiempo real del tráfico web (HTTP) activada	Recomendamos mantener activada la protección web (HTTP) para proteger su equipo frente al malware que se propaga a través de páginas web y la descarga de archivos potencialmente maliciosos.
Protección del tráfico de correo en tiempo real activada	La protección del tráfico de correo le asegura que sus e-mails son analizados en busca de malware y filtrados en busca de spam.
Protección del tráfico IM en tiempo real activada	Recomendamos activar la protección IM por completo para proteger su equipo y cifrar sus conversaciones.
Control de Identidad activado	Le ayuda a mantener a salvo su información confidencial, al analizar todo el tráfico web y el correo en busca de determinadas cadenas de texto. Recomendamos activar el Control de Identidad para mantener a salvo sus datos confidenciales (dirección de correo, IDs de usuario, contraseñas, números de tarjetas de crédito, etc) y impedir su robo.
Cifrado de conversaciones de IM activado	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.
Antiphishing activado para Mozilla Firefox	BitDefender le protege contra los intentos de phishing mientras navega por Internet.
Antiphishing activado para Internet Explorer	BitDefender le protege contra los intentos de phishing mientras navega por Internet.

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

1. Haga clic en los botones **Reparar** de cada incidencia para corregir las vulnerabilidades una por una.



2. Si un problema no se soluciona al momento, siga los pasos del asistente para repararlo.

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

11.3. Seguridad de la red

Cuando su equipo forma parte de una red, es necesario protegerse frente a hackers e intentos de conexión no autorizados a su sistema.

Las incidencias relativas a la seguridad de la red 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>
Cortafuego activado	Protege su equipo frente a hackers y ataques externos.

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

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

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

11.4. Control parental

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

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



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

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

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

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

11.5. Blindaje de archivos

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

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

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

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

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



11.6. Optimizador

Las incidencias relativas al rendimiento de su equipo 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>
Nunca ha realizado una limpieza del registro	El Limpiador del Registro analiza el Registro de Windows y elimina las claves inválidas. Realice una limpieza del registro de vez en cuando para mejorar el rendimiento de su equipo.
Nunca ha realizado una limpieza del equipo	Si realiza una limpieza del equipo de vez en cuando, mejorará su rendimiento. Realice una limpieza del equipo en el momento que considere oportuno.
Nunca ha ejecutado el buscador de archivos duplicados	El Buscador de Archivos Duplicados optimiza el espacio de su disco al buscar aquellos archivos duplicados en su sistema. Ejecútelos en el momento que considere oportuno.
Nunca ha realizado una desfragmentación del disco	El Desfragmentador de Disco reorganiza físicamente los datos del disco duro para que los fragmentos que componen cada archivo se almacenen juntos. Realice una desfragmentación del disco en el momento que considere oportuno.

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**.



11.7. Copia de Seguridad

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

<i>Incidencia</i>	<i>Descripción</i>
Hace x día(s) que realizó una tarea de copia offline	El módulo de copia offline le permite realizar copias de los documentos importantes almacenados su sistema.

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

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

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

11.8. 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>
Comprobación de Vulnerabilidades activada	Monitoriza las Actualizaciones de Microsoft Windows y Microsoft Office, así como las contraseñas de las cuentas de Windows, para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.
Actualizaciones Críticas de Microsoft	Instala las actualizaciones críticas de Microsoft disponibles.



<i>Incidencia</i>	<i>Descripción</i>
Otras actualizaciones de Microsoft	Instala las actualizaciones no-críticas de Microsoft disponibles.
Actualizaciones Automáticas de Windows activadas	Instala las nuevas actualizaciones de seguridad de Windows en el momento en que están disponibles.
Admin (Contraseña Segura)	Indica la fortaleza de la contraseña de determinados usuarios.

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

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

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



12. Registro

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

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

BitDefender Total Security 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: **DBA3EE27571F96A3C7F2**
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 Internet Total 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, si las tareas de copia se han realizado sin errores, etc.

BitDefender

Módulo Historial y Eventos

Antivirus

Protección en tiempo real

Nombre acción	Acción Realizada	Fecha y hora
Protección en tiempo real	Activado	20.08.2008 17:19:43
Análisis de Comportamie...	Activado	20.08.2008 17:19:43
Protección en tiempo real	Desactivado	20.08.2008 17:19:34
Protección en tiempo real	Activado	20.08.2008 17:06:29
Protección en tiempo real	Desactivado	20.08.2008 17:02:38
Protección en tiempo real	Activado	20.08.2008 16:52:45
Protección en tiempo real	Desactivado	20.08.2008 16:52:39
Protección en tiempo real	Activado	20.08.2008 16:52:03
Protección en tiempo real	Desactivado	20.08.2008 16:51:54

Tareas bajo demanda

Nombre acción	Nombre de la tarea	Fecha y hora
Análisis finalizado.	249	20.08.2008 17:04:19
Análisis finalizado.	249	20.08.2008 17:03:57
Análisis finalizado.	249	20.08.2008 17:03:36
Análisis finalizado.	249	20.08.2008 17:03:11
Análisis finalizado.	Análisis Manual	20.08.2008 17:00:44
Análisis cancelado.	Asistente de Excluso...	20.08.2008 16:57:48
Análisis cancelado.	Ms Documentos	20.08.2008 16:55:36
Análisis cancelado.	Análisis Rápido del Sis...	20.08.2008 16:55:29
Análisis cancelado.	Análisis Completo	20.08.2008 16:55:22

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 Limpiar Log Actualizar OK

Eventos

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

- **Antivirus**
- **Cortafuego**
- **Antispam**
- **Control de Privacidad**
- **Control Parental**



- **Actualización**
- **Optimizador**
- **Copia de Seguridad**
- **Red**
- **Cifrado de IM**
- **Blindaje de Archivos**

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

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



Administración Avanzada



14. General

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

14.1. Visualizador

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

The screenshot shows the BitDefender Total Security 2009 - Evaluación interface. At the top, there is a red status bar indicating "ESTADO: Hay 3 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 with a list of modules: Antivirus, Antispam, Control Parental, Control de Privacidad, Cortafuego, Vulnerabilidad, Copia Seguridad, Cifrado, Optimizador, 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" and "Actividad de la Red" with bar charts. The "Estadísticas" table shows: Archivos analizados: 1049, Archivos desinfectados: 0, Virus detectados: 0, Último análisis: Nunca, and Próximo análisis: Nunca. The "General" section shows: Última actualización: Nunca, Mi Cuenta: testare.automata@live.com, Registro: Evaluación, and Caduca en: 30 días. At the bottom, there is a footer with the BitDefender logo and links for "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", and "Historial".

Estadísticas	
Archivos analizados:	1049
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.
- **Internet** - Indica la evolución del tráfico de la red filtrado por el Cortafuego de BitDefender durante el último periodo. La altura de la barra indica la intensidad del tráfico durante ese intervalo de tiempo.

14.1.1. Estadísticas

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

<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.
Análisis de puertos bloqueados	Indica el número de análisis de puertos bloqueados por el Cortafuego de BitDefender. Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers que buscan puertos abiertos en su equipo para intentar aprovecharse de ellos. Mantenga activados el Cortafuego y el Modo Oculto en todo momento para estar protegido frente a los análisis de puertos.
Tareas de copia completadas	Indica cuantas veces ha realizado copias de seguridad de sus datos.

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.
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

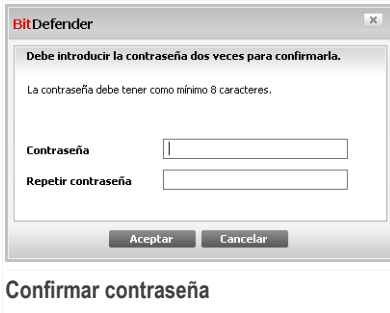
- **Activar protección por contraseña** - permite introducir una contraseña para proteger la configuración de BitDefender.



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:



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

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

Si quiere que se le solicite la contraseña sólo cuando cambie la configuración del Control Parental, marque la opción **Preguntar/aplicar contraseña sólo para el Control Parental**. Por otro lado, si ha definido una contraseña sólo para el Control Parental y desmarca esta opción, se solicitará la respectiva contraseña al cambiar cualquier opción de BitDefender.



Importante

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

- **Preguntarme si deseo configurar la contraseña al activar el Control Parental** - se le pedirá que configure una contraseña cuando active el Control Parental y no haya ninguna contraseña definida. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control Parental que ha configurado exclusivamente para un usuario.
- **Mostrar Noticias de BitDefender (noticias relacionadas con la seguridad)** - ocasionalmente muestra noticias acerca de las epidemias de virus, enviadas desde los servidores de BitDefender.
- **Mostrar pop-ups (notas en pantalla)** - muestra pop-ups acerca del estado del producto.
- **Cargar BitDefender al iniciar Windows** - carga BitDefender automáticamente al iniciar el sistema. Recomendamos mantener esta opción seleccionada.
- **Activar barra de Actividad del Análisis** - activa/desactiva la **Barra de Actividad del Análisis** al iniciar Windows. Desmarque esta casilla si no desea que la Barra de Actividad se muestre más.



Nota

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

14.2.2. Configuración del Informe de Virus

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

Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otra información, ni serán utilizados con fines comerciales. Los datos proporcionados incluirán únicamente el nombre del país y del virus, y serán utilizados exclusivamente para crear informes y estadísticas.

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

Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otra información, y no serán empleados con fines comerciales. La información enviada sólo contiene el posible virus y sólo será utilizada para detectar nuevos virus.

14.3. Información del Sistema

BitDefender le permite ver, desde una sola ventana, todas las opciones y aplicaciones registradas para ejecutarse al iniciar el sistema. De esta manera, podrá monitorizar la actividad del sistema y de las aplicaciones instaladas, así como identificar posibles infecciones del sistema.

Para obtener información del sistema, diríjase al apartado **General > Sistema** en la Vista Avanzada.



Información del Sistema

La lista contiene todos los objetos cargados al iniciar el sistema así como los objetos cargados por diferentes aplicaciones.

Hay tres botones disponibles:

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



Nota

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

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



15. Antivirus

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

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



Nota

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

- **Análisis bajo demanda** - permite detectar y eliminar el malware que ya reside en el sistema. Se trata del clásico análisis antivirus iniciado por el usuario - usted selecciona la unidad, carpeta o archivo que BitDefender debe analizar, y BitDefender lo analizará cuando se lo indique. Las tareas de análisis le permiten crear rutinas de análisis personalizadas, que pueden planificarse para que se ejecuten regularmente.

15.1. Protección en Tiempo Real

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

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



Protección en Tiempo Real

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



Importante

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

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

15.1.1. Configurando el Nivel de Protección

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

Hay 3 niveles de seguridad:



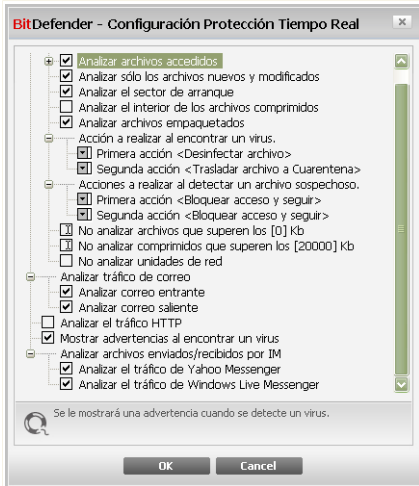
Nivel de Protección	Descripción
Tolerante	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. Los programas y mensajes entrantes se analizan sólo en busca de virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se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

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

15.1.2. Personalizando el Nivel de Protección

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

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



Configuración de la Protección en Tiempo Real

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



Nota

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

- **Analizar archivos accedidos y transferencias P2P** - analiza los archivos a los que accede y las comunicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). Más adelante podrá seleccionar el tipo de archivos a analizar.

Opción		Descripción
Analizar archivos accedidos	Analizar todos los archivos	Se analizarán todos los archivos, independientemente de su tipo.
	Analizar sólo programas	Únicamente se analizarán los archivos con las siguientes extensiones: .exe; .bat; .com;



Opción	Descripción
	.dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml y .nws.
Analizar extensiones definidas	Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ",".
Analizar en busca de software de riesgo	Analizar en busca de software de riesgo. Los archivos detectados con este método se tratarán como archivos infectados. El software que incluya componentes de adware puede funcionar incorrectamente si esta opción está activada. Seleccione Omitir dialers y aplicaciones en el análisis si quiere excluir este tipo de archivos del análisis.
Analizar el sector de arranque	Para analizar el sector de arranque del sistema.
Analizar el interior de los archivos comprimidos	Para analizar el contenido de los archivos comprimidos. Con esta opción activada su ordenador puede ralentizarse un poco.
Analizar archivos empaquetados	Para analizar todos los archivos empaquetados.
Primera acción	En el menú desplegable, seleccione la primera acción que desea realizar al encontrar archivos infectados o sospechosos.
Bloquear acceso y seguir	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
Desinfectar archivo	Desinfecta los archivos infectados.



Opción	Descripción
Eliminar archivo	Elimina los archivos infectados inmediatamente y sin previa advertencia.
Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena.
Segunda acción	En el menú desplegable, seleccione la segunda acción que desea realizar al encontrar archivos infectados o sospechosos, en caso que falle la primera acción.
Bloquear acceso y seguir	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
Eliminar archivo	Elimina los archivos infectados inmediatamente y sin previa advertencia.
Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena.
No analizar archivos que superen los [x] Kb	Introduzca el tamaño máximo de los archivos a analizar. Si el tamaño es 0 Kb, se analizarán todos los archivos, independientemente de su tamaño.
No analizar comprimidos que superen los [20000] Kb	Introduzca el tamaño máximo de los archivos comprimidos a analizar, en kilobytes (KB). Si desea analizar todos los archivos comprimidos, independientemente de su tamaño, introduzca el valor 0.
No analizar unidades de red	Si esta opción está activada, BitDefender no analizará los recursos compartidos de la red, consiguiendo un acceso a la red más rápido. Recomendamos activar esta opción sólo si la red a la que pertenece está protegida por una solución antivirus.

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

Dispone de las siguientes opciones:



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

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

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

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

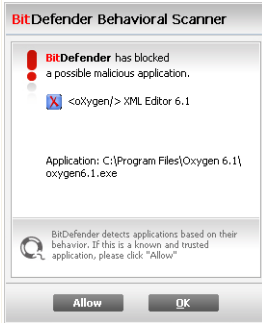
- **Analizar archivos enviados/recibidos por IM.** Para analizar los archivos que reciba o envíe a través de Yahoo Messenger o Windows Live Messenger, seleccione la casilla correspondiente.

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

15.1.3. Configurando el Análisis de Comportamiento

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

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

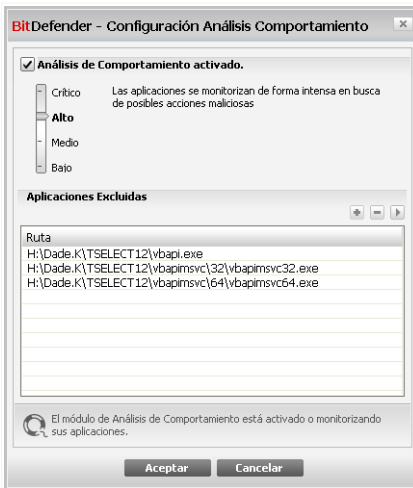


Alerta del Análisis de Comportamiento

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

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

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



Configuración del Análisis de Comportamiento

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



Importante

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

Configurando el Nivel de Protección

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



Nota

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

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

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

Administrando las Aplicaciones Excluidas

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

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

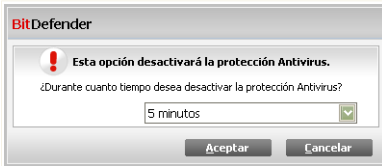
- **Add** - exclude a new application from scanning.
- **Remove** - remove an application from the list.



- Edit - edit an application path.

15.1.4. Desactivando la Protección en Tiempo Real

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



Desactivar Protección en Tiempo Real

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



Aviso

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

15.1.5. Configurando la Protección Antiphishing

BitDefender ofrece protección antiphishing en tiempo real para:

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

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

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



Lista Blanca Antiphishing

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

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



Nota

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

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

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

15.2. Análisis Bajo Demanda

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



a su sistema; y en analizar sus mensajes de correo o cualquier archivo descargado o copiado en su PC.

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

Para configurar e iniciar un análisis bajo demanda, dirjase al apartado **Antivirus > Análisis** en la Vista Avanzada.

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 4 incidencias por resolver REPARAR TODAS

Resistente **Análisis** Exclusiones Cuarentena

General

Antivirus

Antispam

Control Parental

Control de Privacidad

Cortafuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Tareas del sistema

- Análisis en Profundidad**
Última Ejecución: 20.08.2008 16:52:47
- Análisis Completo**
Última Ejecución: Nunca
- Análisis Rápido del Sistema**
Última Ejecución: Nunca
- Análisis del Autologon**
Última Ejecución: 09.05.2008 19:16:42

Tareas del usuario

- Mis Documentos**
Última Ejecución: Nunca

Otras tareas

- Análisis Contextual**
- Detección de Dispositivos**

Nueva Tarea Ejecutar Tarea

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

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

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. 187).

Existen 3 tipos de tareas de análisis:

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

Tarea Predeterminada	Descripción
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Completo de Sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, BitDefender analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Rápido del Sistema	Analiza las 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.
Análisis del Autologon	Analiza los elementos que se ejecutan cuando un usuario inicia sesión en Windows. El Análisis del Autologon se inicia 3 minutos después que el usuario inicio sesión.



Nota

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





recomendamos ejecutar estas tareas con baja prioridad, o preferiblemente, cuando no utilice el equipo.

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

Existe una tarea llamada **Mis Documentos**. Utilice esta tarea para analizar las carpetas del usuario que está utilizando: **Mis Documentos**, **Escritorio e Inicio**. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.

- **Otras tareas** - contiene una lista de otras tareas de análisis. Estas tareas de análisis se refieren a tipos de análisis alternativos que no se pueden ejecutar desde esta ventana. Sólo puede modificar sus opciones o ver los informes de análisis.

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

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



Nota

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

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

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



15.2.2. Utilizando el Menú Contextual

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

The screenshot shows the BitDefender Total Security 2009 interface. The title bar reads "BitDefender Total Security 2009 - Evaluación" and "CAMBIAR A VISTA BÁSICA". A red status bar at the top indicates "ESTADO: Hay 4 incidencias por resolver" and a "REPARAR TODAS" button. The main window has tabs for "Residente", "Análisis", "Exclusiones", and "Cuarentena". On the left is a sidebar with various security features like "Antivirus", "Antispam", "Control Parental", etc. The main area displays "Tareas del sistema" with a list of tasks: "Análisis en Profundidad", "Análisis Completo", "Análisis Rápido del Sistema", and "Análisis del Autologon". Below this is "Tareas del usuario" with "Mis Documentos". A context menu is open over the "Análisis Contextual" task, listing options: "Rutas", "Programador", "Logs", "Clonar", "Eliminar", and "Abrir". At the bottom of the window, there is a "bitdefender" logo and navigation links: "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", "Historial".

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**).



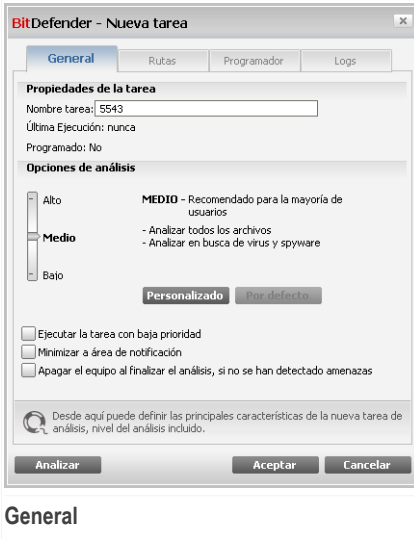
Nota

Para más detalles acerca del módulo **Informes**, consulte "**Viendo los Informes del Análisis**" (p. 206).



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.



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

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

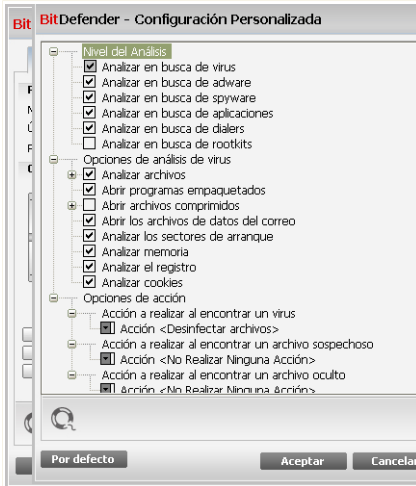
- **Ejecutar el análisis con prioridad baja.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
- **Minimizar ventana de análisis a la barra de tareas.** Minimiza la ventana de análisis 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
Analizar en busca de virus	Analizar en busca de virus conocidos. BitDefender detecta también cuerpos de virus incompletos, eliminando así cualquier posible amenaza que pueda afectar la seguridad de su sistema.
Analizar en busca de adware	Analiza en busca de adware. Estos archivos se tratarán como si fuesen archivos infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada.



Opción	Descripción
Analizar en busca de spyware	Analiza en busca de spyware. Estos archivos se tratarán como si fuesen archivos infectados.
Analizar en busca de aplicaciones	Analiza en busca de aplicaciones legítimas que pueden utilizarse como herramientas de espionaje, para ocultar aplicaciones maliciosas u otros fines maliciosos.
Analizar en busca de dialers	Analiza en busca de dialers de números de alta tarificación. Estos archivos se tratarán como si fuesen archivos infectados. El software que incluya componentes dialer puede dejar de funcionar si esta opción está activada.
Analizar en busca de Rootkits	Analizar en busca de objetos ocultos (archivos y procesos), generalmente denominados rootkits.

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

Opción	Descripción
Analizar archivos	Analizar todos los archivos Se analizarán todos los archivos, independientemente de su tipo.
	Analizar sólo programas Para analizar sólo archivos con las siguientes extensiones: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml and nws.
	A n a l i z a r extensiones definidas Para analizar sólo los archivos que tienen las extensiones indicadas por el usuario. Dichas extensiones deben estar separadas por ",".
Abrir programas empaquetados	Para analizar el interior de los archivos empaquetados.



Opción	Descripción
Abrir archivos comprimidos	Para analizar el contenido de los archivos comprimidos. El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema. Haga clic en el campo Límite de tamaño de comprimidos e introduzca el tamaño máximo de los archivos comprimidos a analizar, en kilobytes (KB).
Abrir los archivos comprimidos adjuntos en el correo	Para analizar el interior de los archivos comprimidos del correo electrónico.
Analizar los sectores de arranque	Para analizar el sector de arranque del sistema.
Analizar memoria	Analiza la memoria en busca de virus y otros tipos de malware.
Analizar registro	Analiza las entradas del registro.
Analizar cookies	Analiza los archivos de las cookies.

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

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



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

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

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los archivos sospechosos. Estos archivos aparecerán en el informe de análisis.
Eliminar archivos	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.



Nota

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

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

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los archivos ocultos. Estos archivos aparecerán en el informe de análisis.
Mover a la Cuarentena	Trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse



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

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

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

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



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

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

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



Nota

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

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



Estableciendo el Objetivo del Análisis

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



Objetivo del Análisis

Puede ver la lista de unidades locales, de red o 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

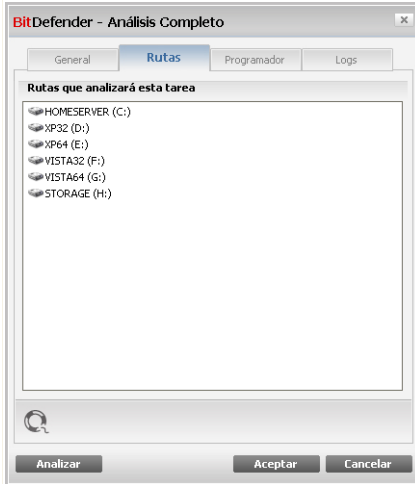
Si desea analizar todo el sistema en busca de virus, seleccione la casilla correspondiente a **Todas las unidades**.

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

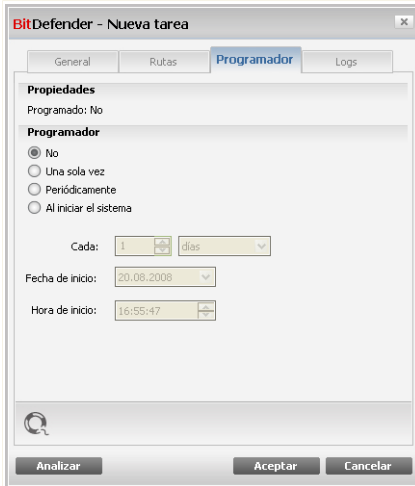
Las tareas **Análisis Completo** y **Análisis en Profundidad** analizarán todas las unidades locales, mientras que la tarea **Análisis Rápido del Sistema** sólo analizará las carpetas **Windows** y **Archivos de Programa**.

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 tipo de análisis bajo demanda:

- **Análisis Inmediato** - ejecuta una de las tareas de análisis del sistema o definidas por el usuario.
- **Análisis Contextual** - haga clic con el botón derecho en el archivo o carpeta que desee analizar y seleccione la opción BitDefender Antivirus 2009.
- **Análisis Arrastrar y Soltar** - arrastre y suelte un archivo o la carpeta sobre la **Barra de Actividad de Análisis**.
- **Análisis Manual** - utilice el Análisis Manual de BitDefender para seleccionar directamente los archivos y carpetas a analizar.

Análisis Inmediato

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

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

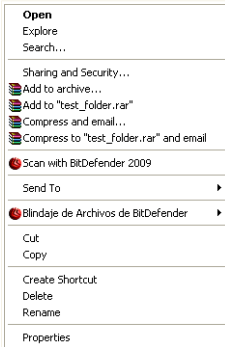
- haga doble clic en la tarea de análisis que desee.
- haga clic en el botón  **Analizar** correspondiente a la tarea.
- seleccione la tarea y haga clic en **Ejecutar Tarea**

Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado "*Analizador de BitDefender*" (p. 202).



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

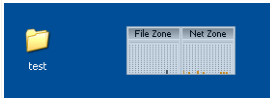
Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **BitDefender Antivirus 2009**.

Aparecerá el Analizador de BitDefender y se iniciará el análisis. Para más información, por favor, consulte el apartado *“Analizador de BitDefender”* (p. 202).

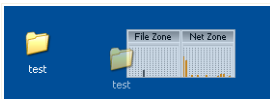
Puede modificar las opciones del análisis o ver los informes en la ventana **Propiedades** de la tarea **Análisis del Menú Contextual**.

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. 202).



Análisis Manual

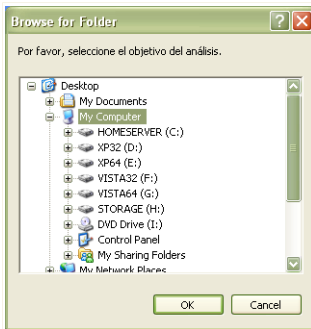
El análisis manual consiste en seleccionar directamente los objetos a analizar con la opción de Análisis Manual de BitDefender desde la carpeta de BitDefender en el menú Inicio.



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. 202).

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...OGRA~1\COMMON~1\SYSTEM\OLEDB~1\MSDMINE.DLL

Tiempo Transcurrido: 00:00:01

Archivos/Segundo: 65

Estadísticas del Análisis

Elementos Analizados:	65
Elementos No Analizados:	0
Elementos Infectados:	0
Elementos Sospechosos:	0
Elementos Ocultos:	0
Procesos Ocultos:	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.

Espera 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 - 249

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

EICAR-Test-File (not a virus) 1 incidencia restante (desinfección fallida)

Contador de incidencias resueltas: 1

Ruta del archivo	Nombre de la amenaza	Resultado de la acción
D:\Documents and Settings\A...tor\Desktop\av_testbed\3.vir	Win32.Parte.C	desinfectado

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

Acciones

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

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

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias.

Pueden aparecer las siguientes opciones en el menú:

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



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

Paso 3/3 – Ver Resultados

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

BitDefender 2009 - 249

Análisis Antivirus - Paso 3 de 3

	Paso1	Paso2	Paso3
Resumen de los Resultados			
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

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. Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

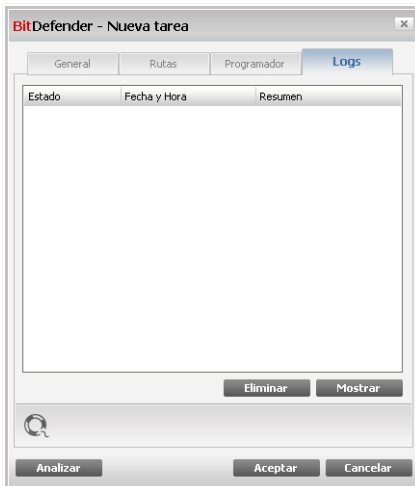
Objetos Sospechosos Detectados por BitDefender

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:



Archivo Log de BitDefender

File Edit View Favorites Tools Help

Address: D:\Documents and Settings\All Users\Application Data\BitDefender\Desktop\Profiles\Logs\deep_scan\1219240375_3_00.xml

BitDefender - Archivo Log

Producto : BitDefender Total Security 2009
Versión : BitDefender UIScanner v.12
Tarea de análisis : Análisis en Profundidad
Fecha del log : 16:52:55 20/08/2008
Ruta del log : D:\Documents and Settings\All Users\Application Data\BitDefender\Desktop\Profiles\Logs\deep_scan\1219240375_3_00.xml

Rutas de Análisis:

- Ruta 0000: D:\Program Files\BitDefender\BitDefender 2009\uiscan.exe
- Ruta 0001: H:\Dade.k\TSELECT12\vbapimsvc32\vbapimsvc32.exe
- Ruta 0002: H:\Dade.k\TSELECT12\vbapl.exe
- Ruta 0003: D:\WINDOWS\system32\wscript.exe
- Ruta 0004: D:\WINDOWS\system32\Dllhost.exe
- Ruta 0005: D:\Program Files\BitDefender\BitDefender 2009\secenter.exe
- Ruta 0006: D:\WINDOWS\system32\wuauclt.exe
- Ruta 0007: D:\WINDOWS\system32\svchost.exe
- Ruta 0008: D:\WINDOWS\system32\alg.exe
- Ruta 0009: D:\Program Files\BitDefender\BitDefender 2009\ysserv.exe
- Ruta 0010: D:\Program Files\Yahoo!\Messenger\ymgr_tray.exe
- Ruta 0011: D:\Program Files\Common Files\Script Debugger IDE\Shared\Debug\mdm.exe
- Ruta 0012: D:\Program Files\Common Files\BitDefender\BitDefender Update Service\livesrv.exe
- Ruta 0013: D:\WINDOWS\system32\ctfmon.exe
- Ruta 0014: D:\Program Files\BitDefender\BitDefender 2009\bdagent.exe
- Ruta 0015: D:\WINDOWS\system32\igmpsvcs.exe
- Ruta 0016: D:\Program Files\Browser Mouse\Browser Mouse\1.0\lwbwheel.exe
- Ruta 0017: D:\WINDOWS\system32\ghpncps.exe
- Ruta 0018: D:\WINDOWS\system32\hcmd.exe

Done My Computer

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.

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

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.

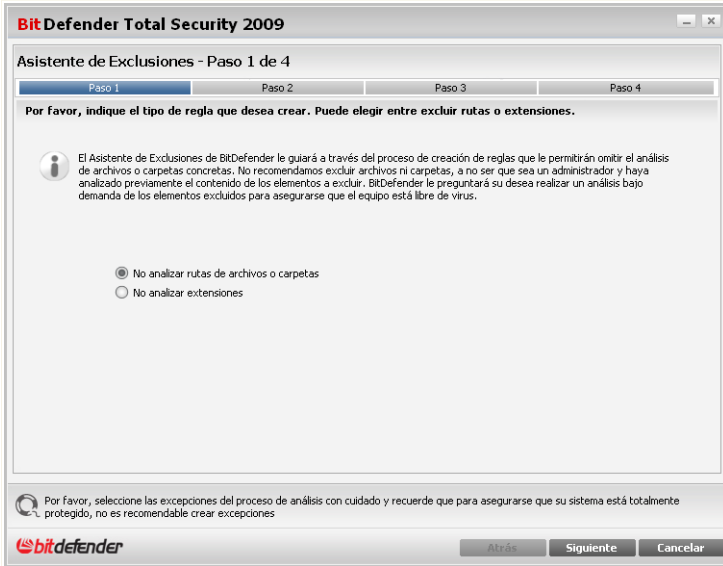
Puede hacer clic en **Descartar** para cancelar los cambios realizados en la tabla, siempre y cuando no los hay guardado pulsando el botón **Aplicar**.

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



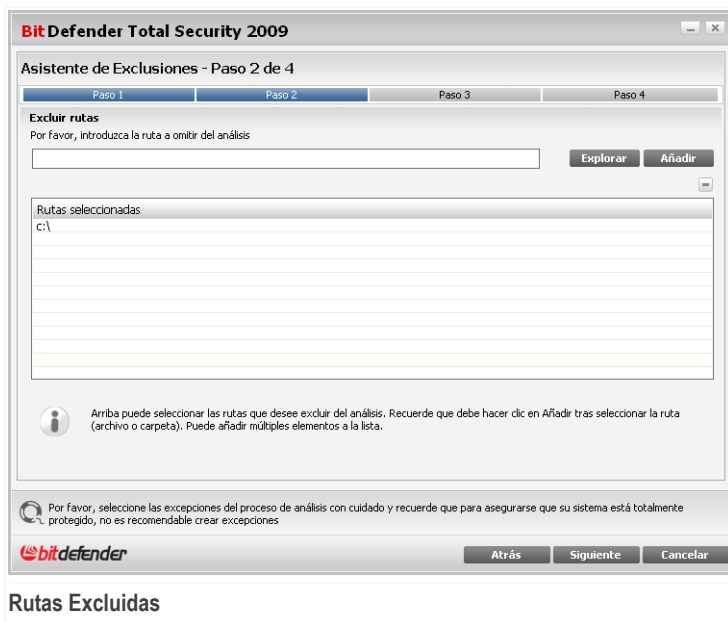
Tipo de Objeto

Seleccione la opción de exclusión de ruta de análisis.

Haga clic en **Siguiete**.



Paso 2/4 – Indique las Rutas a Excluir



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

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



Nota

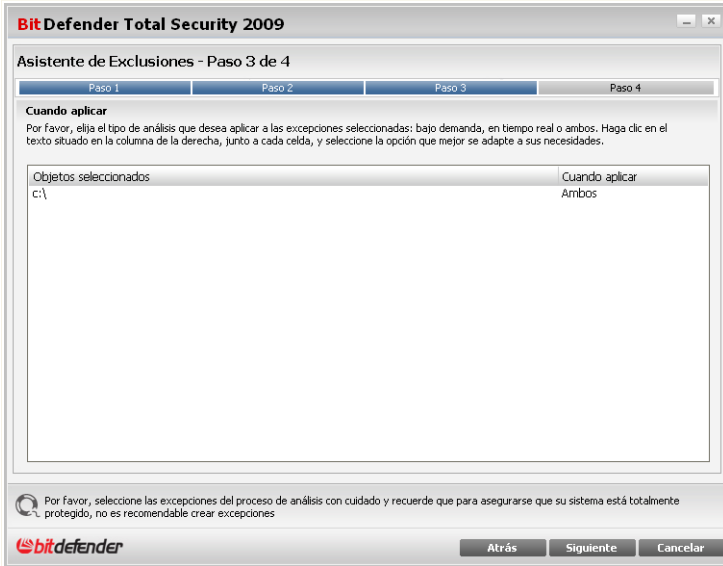
Si la ruta seleccionada no existe, aparecerá un mensaje de error. Haga clic en **Aceptar** y compruebe la validez de ruta.

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

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



Paso 3/4 – Seleccione el Tipo de Análisis



Tipo de Análisis

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

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

Haga clic en **Siguiente**.



Paso 4/4 – Analice los Archivos Excluidos




Analice los Archivos Excluidos

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

Haga clic en **Finalizar**.

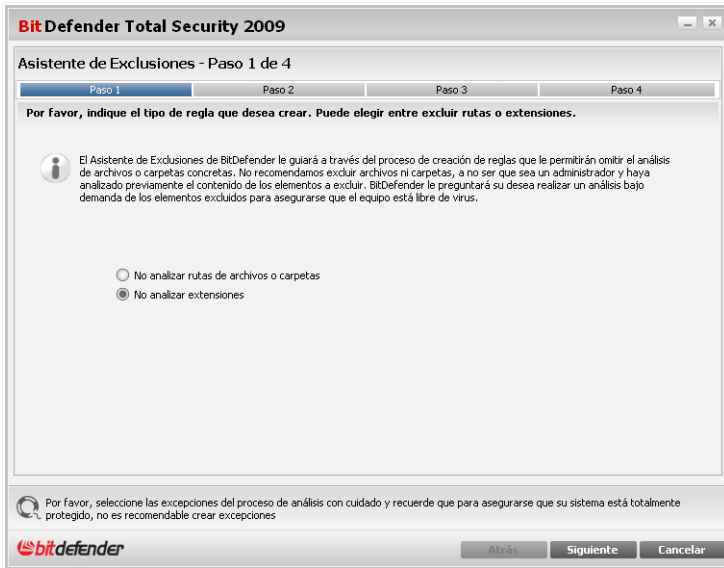
Haga clic en **Aplicar** para guardar los cambios.

15.3.2. Excluyendo Extensiones del Análisis

Para excluir extensiones del 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

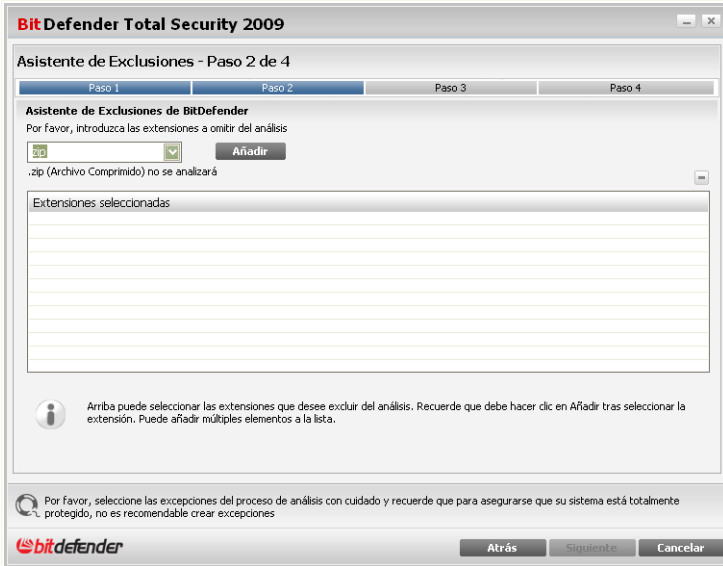


Tipo de Objeto

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

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
*.zip (Archivo Comprimido)	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 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.

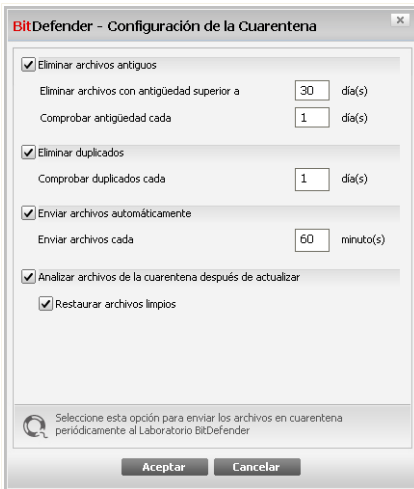
Para ver y administrar los archivos en cuarentena y configurar sus opciones, diríjase al apartado **Antivirus > Cuarentena** en la Vista Avanzada.



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. Antispam

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

16.1. Comprensión del Antispam

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

16.1.1. Los Filtros Antispam

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



Nota

Puede activar/desactivar cada uno de estos filtros desde el apartado [Configuración](#) del módulo **Antispam**.

Listas de Amigos y Lista de Spammers

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

Puede gestionar la Lista de Amigos / Spammers desde la [Vista Avanzada](#) o desde la [Barra de Herramientas Antispam](#) integrada en los clientes de correo más utilizados.



Nota

Recomendamos añadir los nombres y las direcciones de correo de sus amigos a la **Listas de Amigos**. BitDefender no bloquea los mensajes que provienen de esta lista; de



manera que al añadir a sus amigos a esta lista se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de Entrada.

Filtro de Caracteres

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

Filtro de Imágenes

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

Filtro URL

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

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

Filtro NeuNet (Heurístico)

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

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



Nota

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

Filtro Bayesiano

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

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

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



Importante

Puede corregir las decisiones del módulo Bayesiano utilizando los botones  **Es Spam** y  **No Spam** desde la **Barra de Herramientas Antispam**.



Nota

Cada vez que realiza una actualización:

- se añaden nuevas firmas al **Filtro de Imágenes**.
- se añaden nuevos enlaces al **Filtro URL**.
- se añaden nuevas reglas al **Filtro NeuNet (Heurístico)**.

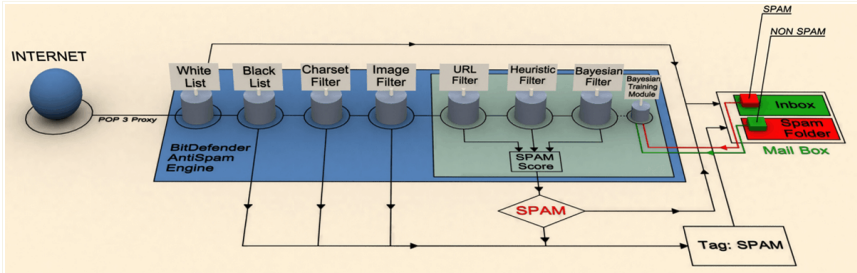
De esta manera se aumenta la eficacia de los motores Antispam.

Para protegerle contra los spammers, BitDefender puede realizar actualizaciones automáticas. Mantenga activada la opción **Actualización automática**.



16.1.2. Funcionamiento del Antispam

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



Funcionamiento del Antispam

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

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

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

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

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

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

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



Nota

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

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

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



Importante

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

16.2. Estado

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



BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Estado Configuración

General

Antivirus

Antispam

Control Parental

Control de Privacidad

CortaFuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Antispam activado

Lista de Amigos 112_items Amigos

Lista de Spammers 584_items Spammers

Nivel de protección

Agresivo

Moderado

Tolerante

DE MODERADO A AGRESIVO

Esta es la opción recomendada. Útil para si normalmente recibe un gran volumen de spam. Puede producir falsos positivos (mensajes legítimos calificados erróneamente como spam). Configurando las listas de Amigos/Spammers y entrenando al Filtro Bayesiano conseguirá a reducir el número de falsos positivos.

Por Defecto

Estadísticas Antispam

Mensajes recibidos (esta sesión): 0

Mensajes Spam (esta sesión): 0

Total de mensajes recibidos: 0

Total de mensajes spam: 0

El módulo Administrador de Archivos muestra el estado de los módulos blindaje de archivos y copia de seguridad, así como enlaces a tareas de relacionadas con éstos.

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

Estado del Antispam

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



Importante

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

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

16.2.1. Estableciendo el Nivel de Protección

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



Hay 5 niveles de protección:

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

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



16.2.2. Configurando la Lista de Amigos

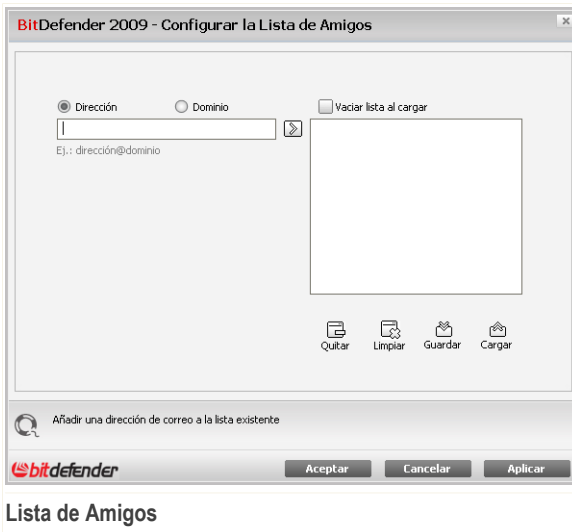
La Lista de Amigos es una lista que contiene todas las direcciones de e-mail de las que quiere recibir mensajes, independientemente de su contenido. Los mensajes de sus amigos no serán marcados como spam, aunque su contenido tenga múltiples características del correo no solicitado.




Nota

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

Para configurar la Lista de Amigos, haga clic en **Amigos** (o haga clic en el botón  **Amigos** de la **Barra de Herramientas Antispam**).



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

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



Importante

Sintaxis: nombre@dominio.com.



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



Importante

Sintaxis:

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

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

Use los botones **Guardar**/ **Cargar** para guardar/cargar la **Lista de amigos** en la ubicación deseada. El archivo tendrá la extensión **.bw1**.

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



Nota

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

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

16.2.3. Configurando la Lista de Spammers

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



Nota

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

Para configurar la Lista de Spammers, haga clic en **Spammers** (o haga clic en el botón **Spammers** de la **Barra de Herramientas Antispam**).



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

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



Importante

Sintaxis: nombre@dominio.com.

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







Importante

Sintaxis:

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



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

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

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

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



Importante

Si desea reinstalar BitDefender, recomendamos guardar las listas de **Amigos / Spammers** antes de iniciar el proceso, para así volver a cargarlas cuando finalice la reinstalación.

16.3. Configuración

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



The screenshot shows the BitDefender Total Security 2009 - Evaluación interface. At the top, there is a status bar indicating "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. The main window is titled "Configuración" and contains a tree view of settings. The "Configuración Antispam" category is expanded, showing three sub-categories: "Configuración Antispam", "Filtros Antispam Básicos", and "Filtros Antispam Avanzados". Each sub-category has a "+" sign next to it, indicating it is expandable. The "Configuración Antispam" sub-category is further expanded, showing several options with checkboxes: "Marcar el mensaje como spam en el asunto", "Marcar el mensaje como phishing en el asunto", "Listas de Amigos/Spammers", "Añadir automáticamente los destinatarios a la Lista de Amigos", "Añadir automáticamente a la Lista de Amigos", "Añadir automáticamente a la Lista de Spammers", "Bloquear mensajes redactados con caracteres Asiáticos", "Bloquear mensajes redactados con caracteres Cirílicos", "Activar el Motor de Aprendizaje (Bayesiano)", "Limitar el tamaño del diccionario a 200000 palabras", "Entrenar el Motor de Aprendizaje (Bayesiano) con los mensajes salientes", "Filtro URL", "Filtro NeuNet(Heurístico)", "Bloquear contenido explícito", and "Filtro de imágenes". At the bottom of the configuration window, there are "Aplicar" and "Por defecto" buttons. Below the configuration window, there is a footer with the BitDefender logo and navigation links: "Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial".

Configuración Antispam

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



Nota

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

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

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

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



16.3.1. Configuración Antispam



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

16.3.2. Filtros Antispam Básicos

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



Nota

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

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

16.3.3. Filtros Antispam Avanzados

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



Nota

El tamaño recomendado es de: 200.000 palabras.



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



17. Control Parental

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

Puede configurar Control Parental para que bloquee:

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



Importante

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

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

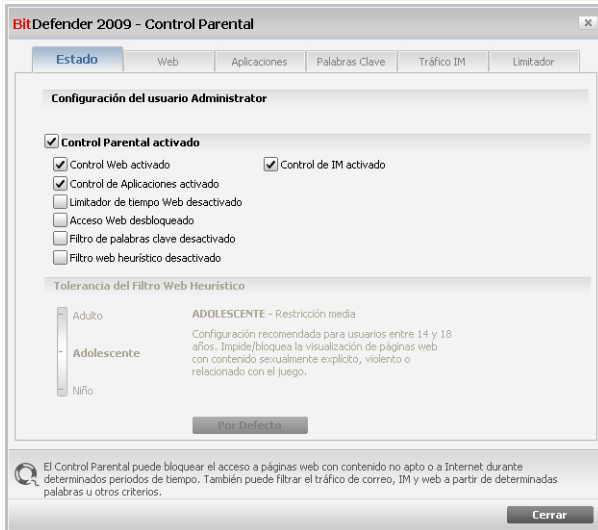
1. Crear una cuenta de usuario de Windows limitada (estándar) para sus hijos.



Nota

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

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



Estado del Control Parental

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

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



Importante

Mantenga el módulo **Control Parental** activado para proteger a sus hijos contra el contenido inapropiado usando sus reglas de acceso personalizadas.

2. Establezca una contraseña para proteger la Configuración del Control Parental. Para más información, por favor, consulte el apartado *“Protegiendo la Configuración del Control Parental”* (p. 239) de esta guía.
3. Seleccione las casillas correspondientes a los controles de protección que desee utilizar:
 - **Control Web** - para filtrar la navegación web según las reglas establecidas en el apartado **Web**.
 - **Control de Aplicaciones** - para bloquear el acceso a las aplicaciones que ha especificado en el apartado **Control de Aplicaciones**.



- **Control de Mensajería Instantánea** - para permitir o bloquear los chats con los contactos IM según las reglas establecidas en el apartado **Tráfico IM**.
 - **Limitador de Tiempo Web** - para permitir o bloquear el acceso web según el horario especificado en el apartado **Limitador**.
 - **Acceso Web** - para bloquear el acceso a todas las páginas web (no sólo las que aparecen en el apartado **Web**).
 - **Filtro de Palabras Clave** - para filtrar el acceso a páginas web, correo y mensajería instantánea según las reglas especificadas en el apartado **Palabras Clave**.
 - **Filtro Web Heurístico** - para filtrar el acceso web según las reglas predefinidas basadas en categorías por edad.
4. Para sacar el máximo provecho de las características del Control Parental, debe configurar los diferentes tipos de Control. Para aprender a configurar este módulo, diríjase a los siguientes temas de este capítulo.

17.1.1. Protegiendo la Configuración del Control Parental

Si no es el único usuario con permisos de administrador que utiliza este ordenador, es recomendable que proteja su configuración de BitDefender con una contraseña. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control Parental que ha configurado exclusivamente para un usuario.

Cuando active el Control Parental, BitDefender le solicitará introducir una contraseña.



Control Parental de BitDefender - Contraseña

Para asegurarse que es el único que cambia la configuración del Control Parental, recomendamos proteger este módulo con una contraseña. Por defecto, sólo protegerá el módulo de Control Parental, pero puede cambiar esta opción desde la ventana de Opciones Avanzadas

¿Desea establecer ahora la contraseña?

Contraseña

Repetir contraseña

La contraseña debe tener 8 caracteres como mínimo.

No preguntar contraseña al activar el Control Parental



Establecer la Protección por Contraseña

Para establecer la protección por contraseña, realice lo siguiente:

1. Introduzca la contraseña en el campo **Contraseña**.
2. Para confirmar la contraseña, introdúzcala de nuevo en el campo **Repetir contraseña**.
3. Haga clic en **Aceptar** para guardar la contraseña y cerrar la ventana.

De ahora en adelante, si quiere cambiar la configuración del Control Parental, se le solicitará introducir la contraseña. Los otros administradores del equipo (si existen) también tendrán que introducir esta contraseña para cambiar la configuración del Control Parental.



Nota

Esta contraseña no protege el resto de configuraciones de BitDefender.

En el caso que no introduzca ninguna contraseña y no desea que vuelva a aparecer esta ventana, marque la casilla **No solicitar la contraseña al activar el Control Parental**.



17.1.2. Configurando el Filtrado Heurístico de Webs

El filtro web heurístico analiza las páginas web y bloquea aquellas con contenido potencialmente inapropiado.

Para filtrar el acceso web a partir de unas reglas predeterminadas para diferentes edades, deberá cambiar el nivel de tolerancia. Arrastre el control deslizante a través de la escala para fijar el nivel de protección que considere apropiado para el usuario seleccionado.

Hay 3 niveles de tolerancia:

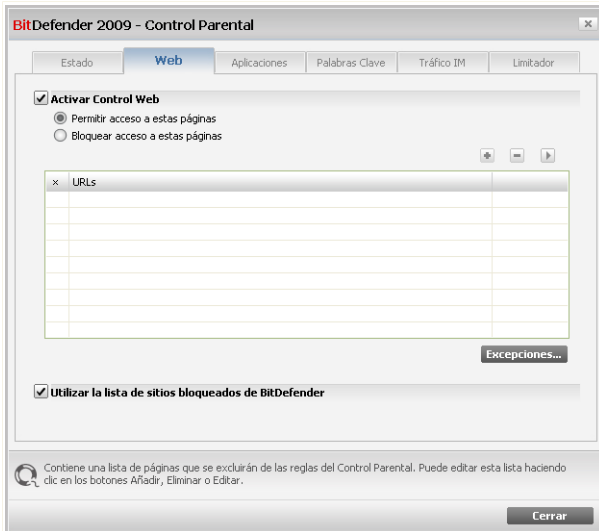
<i>Nivel de tolerancia</i>	<i>Descripción</i>
Niño	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios menores de 14 años. Se bloqueará el acceso a las páginas web con contenido potencialmente dañino para los niños (porno, sexualidad, drogas, hacking, etc).
Adolescente	Se bloqueará el acceso a páginas web según la configuración recomendada para los usuarios entre 14 y 18 años. Se bloqueará el acceso a las páginas web con contenido sexual, pornográfico o adulto.
Adulto	Ofrece un acceso sin restricción a todas las páginas web, independientemente de su contenido.

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

17.2. Control Web

El **Control Web** le ayuda a bloquear el acceso a los sitios web con contenido inapropiado. Se le facilitará una lista de páginas web candidatas a bloquearse, que se actualizará a través del proceso de actualización.

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



Control Web

Para activar esta protección marque la casilla correspondiente a **Activar el control Web**.

Marque la casilla **Permitir acceso a estas páginas/Bloquear acceso a estas páginas** para ver la lista de los sitios autorizados/bloqueados. Haga clic en **Excepciones..** para ver la ventana que contiene la lista complementaria.

Las reglas pueden introducirse manualmente. En primer lugar, seleccione **Permitir acceso a estas páginas/Bloquear acceso a estas páginas** para permitir o bloquear el acceso a las páginas web indicadas en el asistente. A continuación, haga clic en el botón **Añadir** para iniciar el Asistente de Configuración.

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

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



17.2.1. Asistente de Configuración

El Asistente de Configuración consta de un paso.

Paso 1/1 – Especificar las páginas Web

BITDefender 2009 - Asistente de Sitios

Escribir URL

Puede introducir una dirección web o direcciones que contengan caracteres comodín.
Ejemplo: puede bloquear las direcciones que contengan la palabra "cigarros" introduciendo "*cigarros*".

Finalizar Cancelar

Especifique las páginas web

Haga clic en **Añadir**, escriba el sitio web para el que se aplicará la regla y haga clic en **Finalizar**.



Importante

Sintaxis:

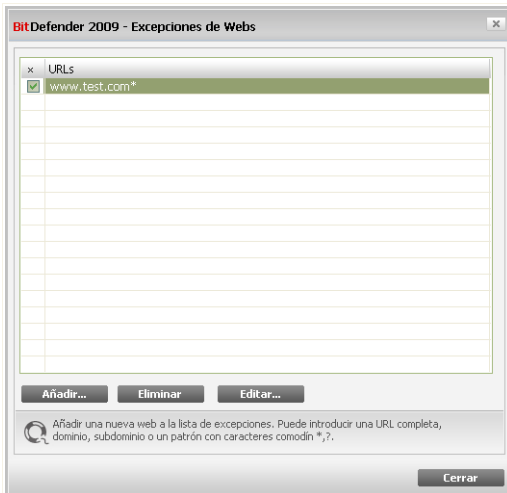
- *.xxx.com - la acción de la regla se aplicará a todos los sitios web que terminen con .xxx.com;
- *porn* - la acción de la regla se aplicará a todos los sitios web que contengan porn en la dirección del sitio web;
- www.*.com - la acción de la regla se aplicará a todos los sitios web que tengan el sufijo de dominio com;
- www.xxx.* - la acción de la regla se aplicará a todos los sitios web que empiecen con www.xxx. sin importar el sufijo de dominio.



17.2.2. Especificar Excepciones

A veces puede necesitar establecer algunas excepciones a una regla determinada. Por ejemplo, puede crear una regla para que se bloqueen todas las páginas que contienen la palabra "killer" (sintaxis: *killer*). Sin embargo, sabe que existe una página llamada `killer-music` donde los visitantes pueden escuchar música online. Para crear una excepción a la regla debe dirigirse a la ventana **Excepciones** y definir una excepción a la regla.

Haga clic en **Excepciones...** Aparecerá la siguiente ventana:



Especificando Excepciones

Haga clic en **Añadir...** para especificar las excepciones. Aparecerá el **Asistente de Configuración**. Complete los pasos del asistente para crear la excepción.

Para borrar una regla, selecciónela y haga clic en **Eliminar**. Para modificar una regla selecciónela y haga clic en **Editar** o haga doble clic en la misma. Para desactivar temporalment una regla sin borrarla, desmarque la casilla correspondiente.

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



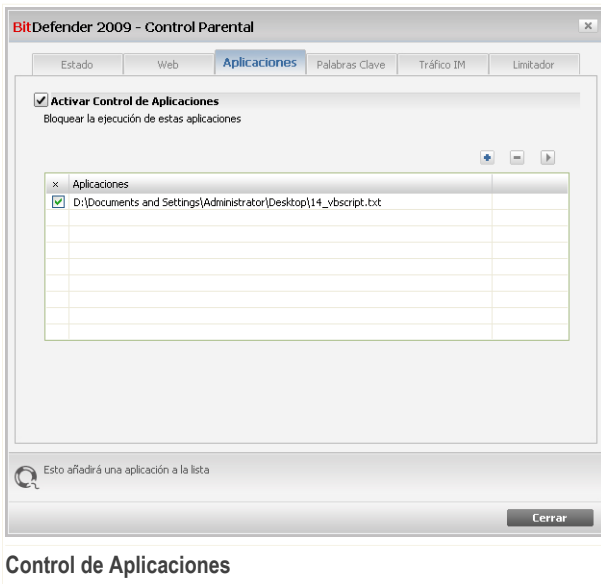
17.2.3. Lista Negra de Webs de BitDefender

Para ayudarle a proteger a sus hijos, BitDefender le proporciona una lista negra de páginas con contenido o posible contenido inapropiado. Para bloquear las páginas que aparecen en esta lista seleccione **Utilizar la lista de sitios bloqueados de BitDefender**.

17.3. Control de Aplicaciones

El **Control de Aplicaciones** ayuda a bloquear la ejecución de cualquier aplicación. Juegos, software de mensajería, u otro tipo de software y malware pueden bloquearse de esta forma. La aplicaciones bloqueadas de esta manera también están protegidas contra modificaciones y no pueden ser copiadas o movidas.

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





Para activar esta protección marque la casilla correspondiente a **Activar el Control de Aplicaciones**.

Las reglas deben introducirse manualmente. Haga clic en el botón **Añadir** para iniciar el Asistente de Configuración.

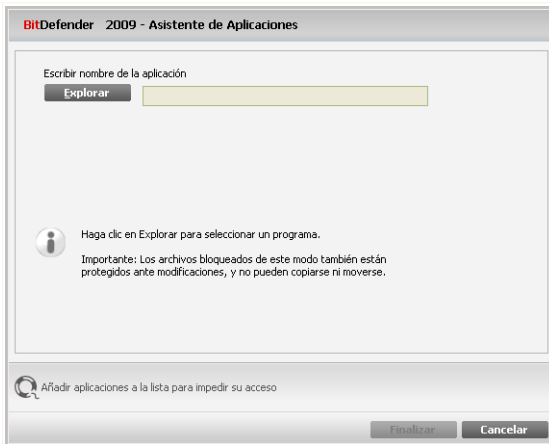
Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar una regla selecciónela y haga clic en el botón **Editar**, o haga doble clic sobre la regla. Para desactivar temporalmente una regla sin eliminarla, desmarque la casilla correspondiente a la regla.

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

17.3.1. Asistente de Configuración

El Asistente de Configuración consta de un paso.

Paso 1/1 – Seleccionar la aplicación a bloquear



Seleccione la aplicación que desea bloquear

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



17.4. Filtro de Palabras Clave

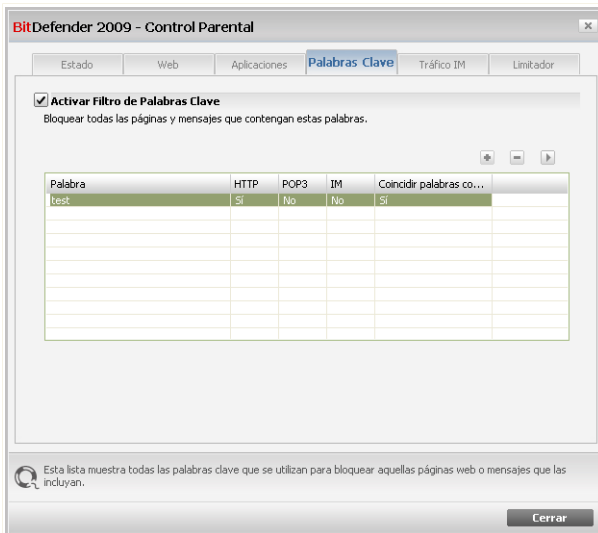
El Filtro de Palabras Clave le ayuda a bloquear el acceso a los correos, páginas web o conversaciones de chat que contengan las palabras especificadas. A través del Filtro de Palabras Clave puede impedir que sus hijos vean palabras o frases inapropiadas mientras están conectados a Internet.



Nota

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

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



Filtro de Palabras Clave

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

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

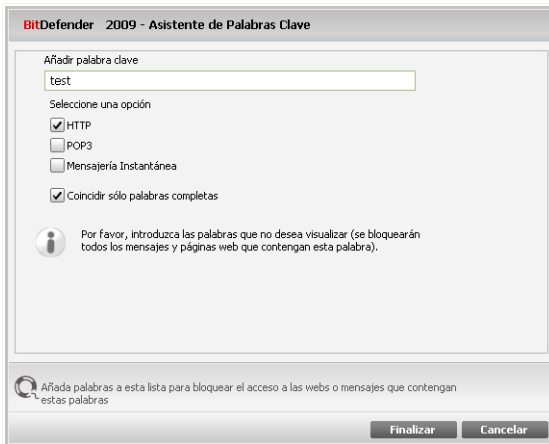


Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para editar una regla existente, haga doble clic encima de la regla o haga clic en el botón **Editar** y realice los cambios oportunos en la ventana de configuración.

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

17.4.1. Ventana de Configuración

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



Escribir la palabra clave

Debe configurar los siguientes parámetros:

- **Palabra clave** - escriba en el campo editable la palabra o frase que desea bloquear.
- **Protocolo tipo** - seleccione el protocolo que BitDefender debe analizar en busca de la palabra o frase indicada.

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



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

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

17.5. Control de Mensajería Instantánea (IM)

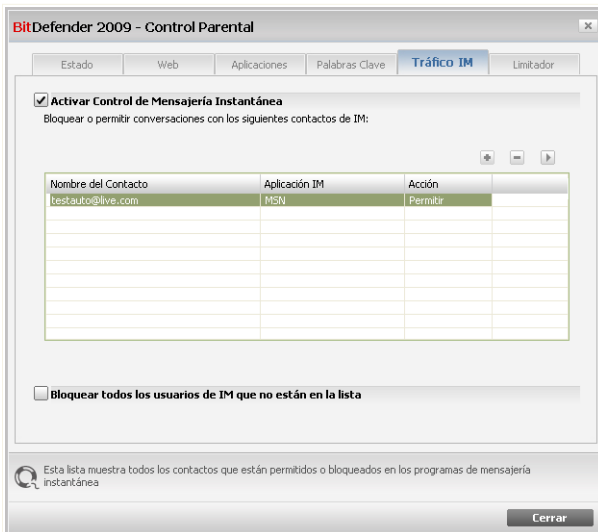
El Control de Mensajería Instantánea (IM) le permite especificar los contactos con los que sus hijos pueden chatear.



Nota

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

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



Control de Mensajería Instantánea



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

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

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

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

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

17.5.1. Ventana de Configuración

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

Introduzca aquí el nombre del contacto que desea añadir a la lista de restricciones
testauto@live.com

Seleccione el tipo de programa de IM
MSN Live Messenger

Acción
 Bloquear conversaciones con este contacto
 Permitir conversaciones con este contacto

Añadir un contacto IM sobre el que bloquear o permitir las conversaciones

Haga clic aquí para permitir conversaciones IM con el contacto indicado

Finalizar Cancelar

Añadir un Contacto IM

Siga estos pasos:

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



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

17.6. Limitador de Tiempo Web

El **Limitador de Tiempo Web** le ayuda a permitir o bloquear el acceso web a los usuarios o aplicaciones durante los intervalos de tiempo indicados.



Nota

BitDefender se actualizará independientemente de la configuración del **Limitador de Tiempo Web**.

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

The screenshot shows the 'BitDefender 2009 - Control Parental' window with the 'Limitador' tab selected. The 'Activar Limitador de Tiempo Web' checkbox is checked. Below it, there is a grid for setting intervals. The grid has columns for days of the week (D, L, M, M, J, V, S) and rows for time intervals from 00:00 to 12:00. A legend indicates that white cells mean 'permitido' (allowed) and grey cells mean 'bloqueado' (blocked). Buttons for 'Marcar Todos', 'Quitar Todos', and 'Aplicar' are at the bottom of the grid. A 'Cerrar' button is at the bottom right of the window.

Intervalos	D	L	M	M	J	V	S
00:00 - 01:00							
01:00 - 02:00							
02:00 - 03:00							
03:00 - 04:00							
04:00 - 05:00							
05:00 - 06:00							
06:00 - 07:00							
07:00 - 08:00							
08:00 - 09:00							
09:00 - 10:00							
10:00 - 11:00							
11:00 - 12:00							

Limitador de Tiempo Web



Para activar esta protección marque la casilla correspondiente a **Activar el limitador de tiempo para Web**.

Seleccione los intervalos de tiempo en los que se bloquearán todas las conexiones a Internet. También puede hacer clic en **Marcar todos** para seleccionar todas las celdas, y en consecuencia, bloquear todo el acceso a páginas web. Si hacer clic en **Quitar todos**, se permitirá el acceso a webs en todo momento.



Importante

Las casillas coloreadas en gris representan intervalos de tiempo en los que todas las conexiones a internet están bloqueadas.

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



18. Control de Privacidad

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

18.1. Estado del Control de Privacidad

Para configurar el Control de Privacidad y ver información relacionada con su actividad, haga clic **Control Privacidad > Estado** en la Vista Avanzada.

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Estado | Identidad | Registro | Cookie | Script

General

Antivirus

Antispam

Control Parental

Control de Privacidad

Cortafuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Control de privacidad activado
Control de Identidad desactivado

Nivel de protección

Agresivo **TOLERANTE**

Por defecto

Tolerante

Personalizado **Por Defecto**

Estadísticas del Control de Privacidad

Información privada bloqueada:	0
Registro bloqueados:	0
Cookies bloqueadas:	0
Scripts bloqueados:	0

El módulo Protección de la Privacidad está desactivado. Marque esta casilla para activarlo. Para mayor seguridad de sus datos, recomendamos mantener la protección de Privacidad activada en todo momento.

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

Estado del Control de Privacidad



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



Importante

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

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

- **Control de Identidad** - protege sus datos confidenciales filtrando todo el tráfico web (HTTP), de correo (SMTP) y mensajería instantánea saliente según las reglas creadas en el apartado **Identidad**.
- **Control del Registro** - le pedirá permiso cada vez que un programa intente modificar un entrada del registro para ejecutarse cuando inicie Windows.
- **Control de Cookies** - le pedirá permiso cada vez que una nueva página web intente guardar una cookie.
- **Control de Scripts** - le pedirá permiso cada vez que una página web intente activar un script u otro tipo contenido activo.

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

18.1.1. Configurando el Nivel de Protección

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

Hay 3 niveles de seguridad:

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



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

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

18.2. Control de Identidad

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

Tanto si se trata de su dirección de e-mail o como de su número de tarjeta de crédito, cuando esta información no cae en buenas manos puede resultar peligrosa: puede ahogarse entre una multitud de mensajes de spam o encontrar vacía su cuenta bancaria.

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

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

¿Por qué usar el Control de Identidad?

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

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



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

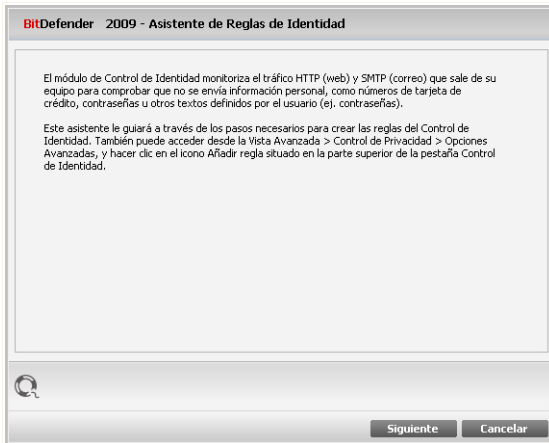
Por ejemplo, puede recibir mensajes que simulan provenir de su banco/caja y le soliciten actualizar su información bancaria urgentemente. Este mensaje incluye un enlace a una página web en la que debe introducir la información personal actualizada. Aunque puedan parecer legítimos, tanto la dirección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

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

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



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

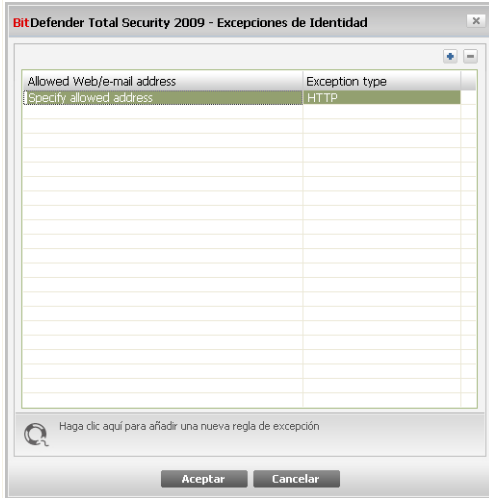
Introduzca una breve descripción de la regla en el campo editable. Como los datos bloqueados (las cadena de texto) no se muestran en texto plano cuando accede a la regla, es importante introducir una breve descripción que le ayude a identificar fácilmente los datos que protege.

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

18.2.2. Definiendo las Excepciones

En algunos casos, es necesario crear excepciones a las reglas de identidad. Imaginemos que ha creado una regla para impedir el envío de su número de tarjeta de crédito en páginas web. En el momento que su número de tarjeta se envíe a una página web, la página en cuestión se bloqueará. Pero si realmente quisiera comprar una película DVD en una tienda online segura, tendría que crear una excepción para dicha regla.

Para abrir la ventana dónde puede crear excepciones, haga clic en **Excepciones**.



Excepciones

Para añadir una excepción, siga estos pasos:

1. Haga clic en **Añadir** para introducir una nueva entrada en la tabla.
2. Haga doble clic en **Indique las direcciones permitidas** e introduzca la dirección de la página, el correo electrónico o el contacto de mensajería que desea añadir como excepción.
3. Haga doble clic en **Seleccionar tipo** y en el menú, seleccione la opción correspondiente al tipo de dirección que ha introducido previamente.
 - Si ha introducido una página web, seleccione la opción **HTTP**.
 - Si ha introducido una dirección de e-mail, seleccione la opción **SMTP**.
 - Si ha introducido un contacto de mensajería instantánea, seleccione **IM**.

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

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

18.2.3. Administrando Reglas

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



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

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

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.

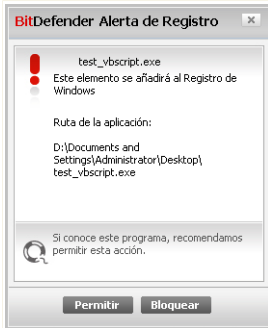
Editar regla

18.3. Control del registro

El **Registro** es un componente muy importante de Windows. El sistema operativo emplea el registro para guardar su configuración, los programas instalados, los datos del usuario etc.

El **Registro** también se utiliza para definir los programas que se deben iniciar automáticamente con cada inicio de Windows. Los virus utilizan esta funcionalidad para ejecutarse automáticamente cuando el usuario reinicia el ordenador.

El **Control del Registro** monitoriza toda la actividad del Registro Windows – acción que puede resultar muy útil para detectar Troyanos. Este módulo le advierte cada vez que un programa intenta modificar una entrada en el registro para poder ejecutarse con cada inicio del sistema.



Aviso de Registro

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

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

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



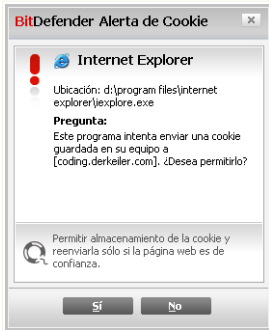
Nota

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

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



Para evitar estos casos, use nuestro **Control de cookie**. Si se lo mantiene activado, **Control de cookies** le pedirá la autorización cada vez que un nuevo sitio web intenta enviar una cookie:



Alerta de Cookie

Podrá ver el nombre de la aplicación que trata de enviar la cookie.

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

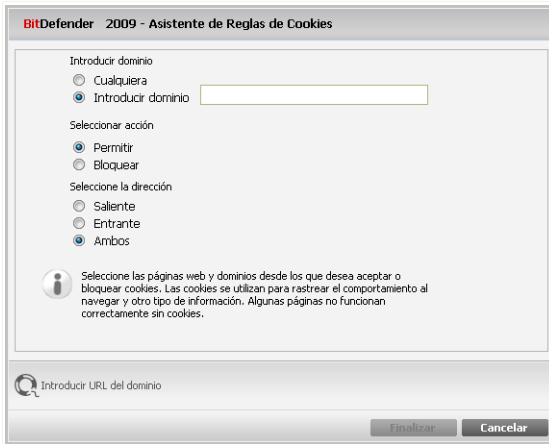
Esto le ayudará a decidir cuáles son los sitios web de confianza y cuáles no.



Nota

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

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



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**.

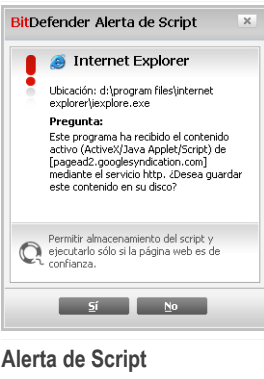
Haga clic en **Finalizar**.

18.5. Control de Scripts

Los **Scripts** y otros códigos, como los **Controles ActiveX** y los **Applets de Java**, se utilizan para crear páginas web interactivas, aunque también pueden ser programados para tener efectos dañinos. Los elementos ActiveX, por ejemplo, pueden obtener el acceso total a sus datos y, por consiguiente, pueden leer los datos de su ordenador, borrar información, copiar contraseñas e interceptar mensajes mientras está conectado a Internet. Sólo debería aceptar contenido activo de las webs que conozca y sean de confianza.

BitDefender le permite elegir entre ejecutar o bloquear estos elementos.

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

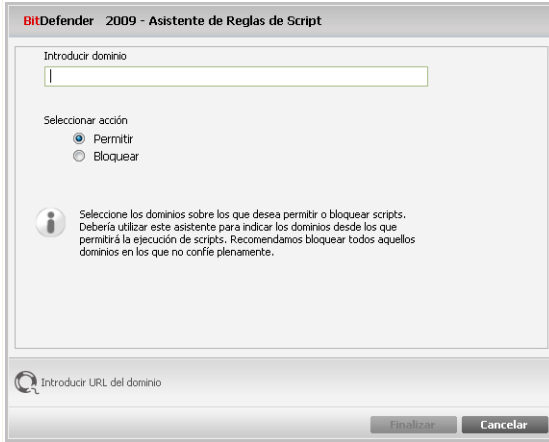


Alerta de Script

Puede ver el nombre del recurso.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No** para crear una nueva regla de permiso, que será listada en la tabla de reglas. A partir de este momento, no recibirá más notificaciones cuando el mismo sitio intente enviarle contenido activo.

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



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>
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

Haga clic en **Finalizar**.



19. Cortafuego

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



Nota

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

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

19.1. Configuración

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



The screenshot shows the BitDefender Total Security 2009 interface. At the top, it says "ESTADO: Hay 2 incidencias por resolver" and "REPARAR TODAS". The "Configuración" tab is active, showing "Cortafuego activado".

Configuración | Red | Reglas | Actividad

Cortafuego activado

Nombre del equipo: dbucures2-xp32
IPs del equipo: 10.10.15.244/16
Puertas de enlace: 10.10.0.1

Bytes enviados: 411.2 KB (0.0 B/s)
Bytes recibidos: 4.0 MB (704.0 B/s)
Análisis de puertos detectados: 0
Paquetes perdidos: 11
Puertos abiertos: 11
Conexiones entrantes: 0
Conexiones salientes: 0

Acción Predeterminada:

Permitir Todo (Modo Trabajo)
 Permitir Programas Conocidos
 Informe
 Bloquear Todo

[Opciones Avanzadas](#)
[Mostrar lista blanca](#)

Entrante: 0.63K | 120s | 50s | 0s
Saliente: 0.00K | 120s | 60s | 0s

El Cortafuego protege su equipo de los intentos de conexión entrantes y salientes no autorizados, así como frente a hackers y ataques externos.

[Comprar](#) - [Mi Cuenta](#) - [Registrar](#) - [Ayuda](#) - [Soporte](#) - [Historial](#)

Configuración del Cortafuego

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



Importante

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

Existen dos tipos de categorías de información:

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



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

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

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



Nota

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

19.1.1. Estableciendo la Acción Predeterminada

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

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

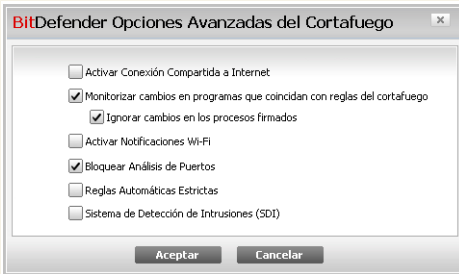
Acción predeterminada	Descripción
Permitir todo	Aplica las reglas actuales y permite todo el tráfico que no coincida con las reglas actuales sin preguntar. Esta política no es en absoluto recomendable, pero puede resultar útil para los administradores de red y jugadores.
Permitir Programas Conocidos	Aplica las reglas existentes y permite que los programas reconocidos por BitDefender (en la lista blanca) puedan establecer conexiones salientes sin preguntarle. Para



Acción predeterminada	Descripción
	<p>el resto de intentos de conexión, BitDefender solicitará su permiso.</p> <p>La lista blanca está formada por las aplicaciones más utilizadas por los usuarios. Esto incluye los navegadores web más comunes, reproductores de audio y vídeo, programas de mensajería instantánea e intercambio de archivos, y también clientes de servidores (Correo, FTP..) o aplicaciones del sistema operativo.</p>
Informe	Aplica las reglas y le consulta sobre el tráfico que no coincide con ninguna de las reglas actuales.
Bloquear todo	Aplica las reglas existentes y bloquea todos los intentos de conexión que no coincidan con ninguna de las reglas existentes.

19.1.2. Modificando las Opciones Avanzadas del Cortafuego

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



Configuración Avanzada del Cortafuego

Dispone de las siguientes opciones:

- **Activar soporte Conexión compartida a Internet (ICS)** - activa el soporte para Conexión Compartida a Internet (ICS).



Nota

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

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

Al compartir su conexión a Internet con los miembros de su red local puede experimentar un mayor nivel de consumo de recursos y puede implicar riesgos. También le quita algunos de sus puertos (aquellos abiertos por los miembros que usan su conexión de Internet).

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

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



Nota

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

Las aplicaciones firmadas suelen ser aplicaciones de confianza con un alto grado de seguridad. Puede marcar la opción **Ignorar cambios de los procesos firmados** para permitir el acceso a Internet a aquellas aplicaciones firmadas que hayan sufrido algún cambio, sin recibir ningún mensaje de alerta.

- **Activar Notificaciones Wi-Fi** - si está conectado a una red Wi-Fi, se mostrarán ventanas con información sobre diferentes eventos de red (por ejemplo, cuando un equipo se conecta a la red).
- **Bloquear Análisis de Puertos** - detecta y bloquea los ataques que intentan averiguar qué puertos tiene abiertos.

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



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

19.2. Red

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

The screenshot shows the BitDefender Total Security 2009 - Evaluación interface. The main window title is "BitDefender Total Security 2009 - Evaluación" with a "CAMBIAR A VISTA BÁSICA" button. A red status bar at the top indicates "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. The left sidebar contains a list of configuration categories: General, Antivirus, Antispam, Control Parental, Control de Privacidad, Cortafuego (highlighted), Vulnerabilidad, Copia Seguridad, Cifrado, Optimizador, Modo Juego/Portátil, Red (selected), Actualizar, and Registro. The main content area is titled "Configuración de la Red" and contains a table with columns: Adaptador, Nivel de Confianza, Oculto, Gené..., Direcciones, and Puertas d... The table has one row for "Local Area Connecti...". Below the table is a "Zonas:" section with a table for "Adaptador / Zonas" and "De Confianza". The table has one row for "Local Area Connection 2" with a sub-row for "10.10.10.10" and a "Permitir" button. At the bottom, there is a footer with the BitDefender logo and links: "Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial".

Red

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

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



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

19.2.1. Cambiando el Nivel de Confianza

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

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

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

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



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

19.2.2. Configurando el Modo Oculto

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

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

19.2.3. Modificando la Configuración Genérica

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

19.2.4. Zonas de Red

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

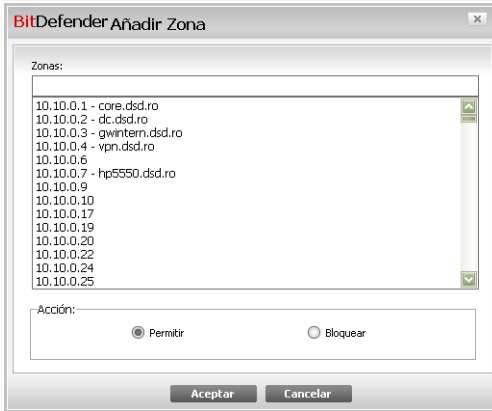
Una zona de confianza es un equipo en el que confía plenamente. Se permitirá todo el tráfico entre su equipo y el equipo de confianza. Para compartir recursos con algunos de los equipos que forman parte de una red Wi-Fi insegura, añádalos como equipos permitidos.

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

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



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



Añadir zona

Siga estos pasos:

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

19.3. Reglas

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



The screenshot shows the BitDefender Total Security 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 "Configuración", "Red", "Reglas", and "Actividad". The "Reglas" tab is selected. On the left, there is a sidebar with various security modules, including "Cortafuego" (Firewall) which is highlighted. The main area displays a list of rules under the heading "Reglas:". The first rule is checked and labeled "Ocultar Procesos del Sistema". Below this, there is a table with the following columns: "Tipos de Proceso/Ada...", "Línea C...", "Proto...", "Eventos de Red", "Puertos...", "Puertos R...", "Local", and "Acción". One rule is listed with the command "d:\program files\internet explorer\iexplore.exe". At the bottom of the rule list, there are "Reiniciar Reglas" and "Avanzado" buttons. Below the table, there is a note: "Haga clic aquí para añadir una nueva regla del cortafuego personalizada." and the BitDefender logo. At the very bottom, there are links for "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", and "Historial".

Reglas del Cortafuego

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

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

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



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

Protocolo	Descripción
Cualquiera	Incluye todos los protocolos IP.
TCP	Transmission Control Protocol (Protocolo de Control de Transmisión) – El protocolo TCP permite establecer una conexión e intercambiar flujos de datos entre dos ordenadores. TCP garantiza la entrega de los datos y también que los paquetes serán entregados en el mismo orden en el que fueron enviados.
UDP	User Datagram Protocol (Protocolo de Datagrama de Usuario) – El protocolo UDP es un transporte basado en IPs y diseñado para un alto rendimiento. Los juegos y otras aplicaciones basadas en vídeo a menudo utilizan el protocolo UDP.
Un número	Representa un protocolo IP específico (que no sea TCP ni UDP). Puede encontrar una lista completa de los números asignados a los protocolos IP en www.iana.org/assignments/protocol-numbers .

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

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

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



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

19.3.1. Añadir Reglas Automáticamente

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



Alerta Cortafuego

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

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

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



Importante

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

19.3.2. Eliminando Reglas

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

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

19.3.3. Creando y Modificando Reglas

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



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

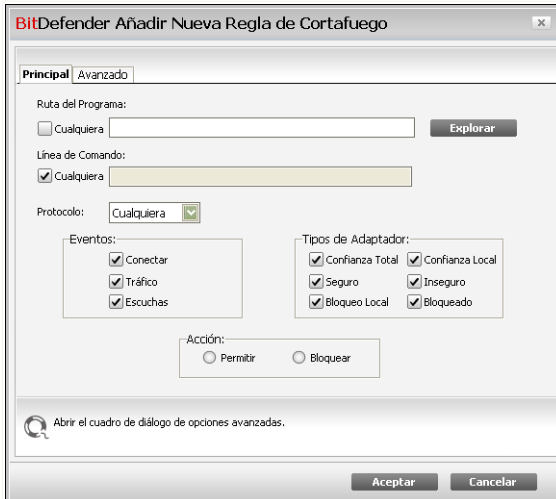
1. Haga clic en el botón **Añadir regla**. Aparecerá la ventana de configuración.
2. Configure los parámetros principales y avanzados según sus necesidades.
3. Haga clic en **Aceptar** para añadir la nueva regla.

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

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

Configurando los Parámetros Principales

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



Parámetros Principales

Puede configurar los siguientes parámetros:



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



Nota

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

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

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

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



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

Configurando los Parámetros Avanzados

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

BitDefender Añadir Nueva Regla de Cortafuego

Principal **Avanzado**

Dirección: Versión de IP:

Dirección Local:

Ip: Cualquiera

Puerto(s): Cualquiera

Dirección Remota:

Ip(s): Cualquiera

Puerto(s): Cualquiera

Aplicar esta regla sólo a los equipos conectados directamente.

Comprobar cadena del proceso padre del evento original.

Parámetros Avanzados

Puede configurar los siguientes parámetros avanzados:

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

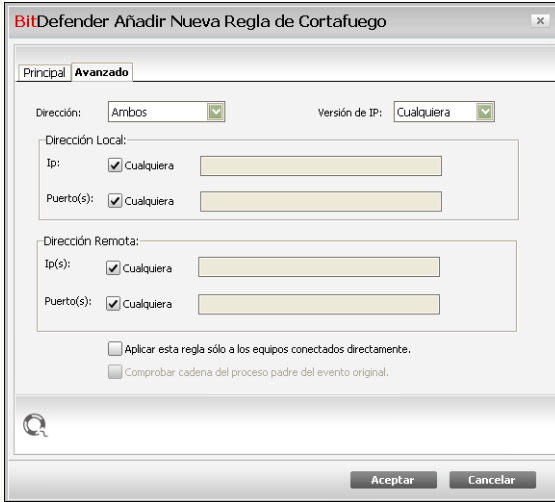


Dirección	Descripción
Saliente	La regla se aplicará sólo para el tráfico saliente.
Entrante	La regla se aplicará sólo para el tráfico entrante.
Ambos	La regla se aplicará en ambas direcciones.

- **Versión de IP.** En el menú, seleccione la versión de IP (IPv4, IPv6 o cualquiera) a la que se aplicará la regla.
- **Dirección Local.** Indique la dirección IP local y el puerto a los que se aplicará la regla, como se indica:
 - Si dispone de más de un adaptador de red, puede desmarcar la casilla **Cualquiera** e introduzca una dirección IP específica.
 - Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.
- **Dirección Remota.** Indique la dirección IP remota y el puerto a los que se aplicará la regla, como se indica:
 - Para filtrar el tráfico entre su equipo y un equipo concreto, desmarque la casilla **Cualquiera** e introduzca una dirección IP específica.
 - Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.
- **Aplicar esta regla sólo a los equipos conectados directamente.** Seleccione esta opción desea que la regla se aplique sólo a los intentos de tráfico local.
- **Comprobar cadena del proceso padre del evento original.** Sólo puede modificar esta parámetro si ha seleccionado la opción **Reglas Automáticas Estrictas** (diríjase a la pestaña **Configuración** y haga clic en **Opciones Avanzadas**). Las reglas estrictas harán que BitDefender le solicite la acción a realizar cada vez que el proceso padre de una aplicación que intenta acceder a la red/Internet sea diferente.

19.3.4. Configuración Avanzada de las Reglas

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



Configuración Avanzada de las Reglas

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



Nota

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

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

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

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

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



19.4. Control de Conexiones

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

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Configuración | Red | Reglas | **Actividad**

General

Antivirus

Antispam

Control Parental

Control de Privacidad

Cortafuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Ocultar Procesos Inactivos

Nombre del Proceso	PID/P...	Salida	Salientes...	Entrada	Entrante...	Antigüedad
System	4	2.1 KB	0.0 B/s	186.7 KB	0.0 B/s	17m 20s
10.10.15.244:Net...	UDP	990.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 5s
10.10.15.244:Net...	UDP	1.1 KB	0.0 B/s	0.0 B	0.0 B/s	17m 5s
0.0.0.0:SMB	TCP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 20s
10.10.15.244:Net...	TCP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 5s
0.0.0.0:SMB	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 20s
svchost.exe -k locale...	1712	0.0 B	0.0 B/s	84.8 KB	0.0 B/s	17m 8s
10.10.15.244:1900	UDP	0.0 B	0.0 B/s	84.8 KB	0.0 B/s	16m 57s
vserv.exe /service	360	706.0 B	0.0 B/s	790.0 B	0.0 B/s	4m 25s
0.0.0.0:10000	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	4m 24s
lsass.exe	1024	18.7 KB	0.0 B/s	22.0 KB	0.0 B/s	17m 9s
0.0.0.0:4500	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 5s
0.0.0.0:IKE	UDP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 5s
10.10.15.244:109...	TCP	597.0 B	0.0 B/s	192.0 B	0.0 B/s	11s
svchost.exe -k rpcss	1268	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 8s
0.0.0.0:RPC	TCP	0.0 B	0.0 B/s	0.0 B	0.0 B/s	17m 8s
svchost.exe -k netsvcs	1464	4.2 KB	45.3 B/s	8.0 KB	45.3 B/s	17m 8s
10.10.15.244:NTP	UDP	136.0 B	45.3 B/s	136.0 B	45.3 B/s	17m 4s

Mostrar Log Incrementar nivel de detalle del Log

Desde aquí puede ver información sobre los procesos activos en su sistema y detalles acerca de los mismos.

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

Control de Conexiones

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

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

A continuación se indica el significado de los iconos:

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



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

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

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



20. Tareas de Copia

BitDefender incluye un módulo de Copia de Seguridad que le ayudará a copiar los datos importantes que tiene en su sistema. Puede guardar las copias en su equipo, en discos extraíbles o en una ubicación de la red, para asegurarse que podrá restaurar los datos cuando sea necesario. La restauración se realiza a través de un proceso sumamente sencillo.

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 4 incidencias por resolver REPARAR TODAS

Copia Seguridad

General
Antivirus
Antispam
Control Parental
Control de Privacidad
CortaFuego
Vulnerabilidad
Copia Seguridad
Cifrado
Optimizador
Modo Juego/Portátil
Red
Actualizar
Registro

Tareas de Copia
Última Ejecución: 20 august 2008 16:30:39
Copia Local

Tareas de Restauración
Última Ejecución: 20 august 2008 16:30:42
Restaurar Local

Configuración de Copia
Configuración

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

Tareas de Copia

Dispone de los siguientes botones:

- **Copia Local** - inicia un asistente de cinco pasos que le guiará en el proceso de copia local de sus datos.
- **Restauración Local** - inicia un asistente de cuatro pasos que le guiará en el proceso de restauración de los datos copiados localmente.



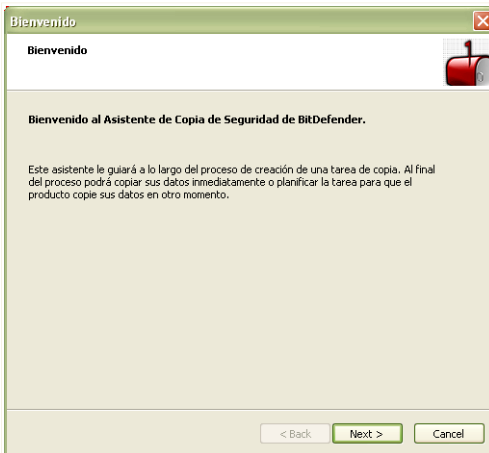
- **Configuración** - abre la aplicación de Copia de Seguridad de BitDefender, la cual le permite **configurar y ejecutar operaciones de copia de seguridad en detalle**.

20.1. Realizando Copias de Seguridad Locales

Al hacer clic en **Copia Local** se iniciará un asistente que le guiará a través del proceso de creación de tareas de copia de seguridad. Al final del proceso será capaz de copiar sus datos al instante o planificar una tarea para que el producto realice la copia automáticamente en otro momento.

20.1.1. Paso 1/5 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

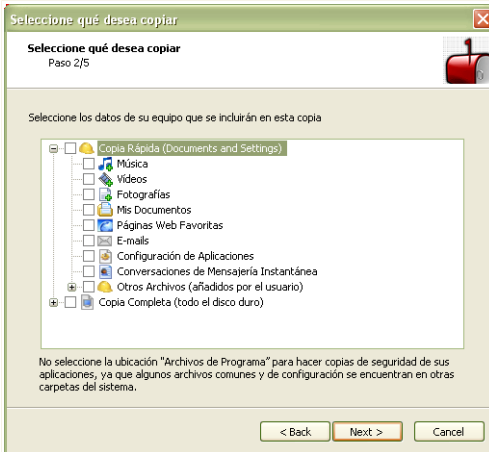


Ventana de Bienvenida

Haga clic en **Siguiente**.

20.1.2. Paso 2/5 - Seleccionar los datos a Copiar

Desde aquí puede seleccionar los datos de su ordenador que desea copiar.



Selección de los datos a Copiar

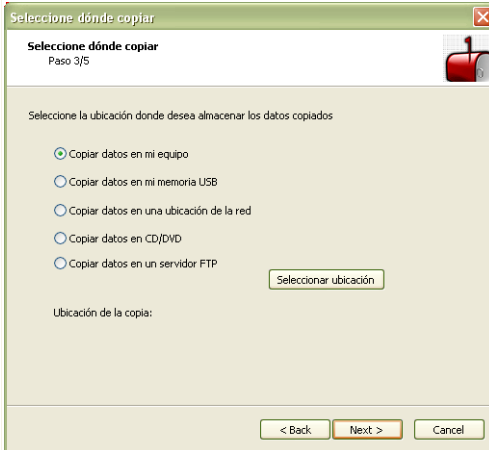
Puede elegir entre **Copia Rápida** (su música, vídeos, fotografías, emails, configuración de aplicaciones, etc.) y **Copia Completa** (todas las particiones).

Haga clic en **Otros archivos**, para añadir otros archivos de su Escritorio a la **Copia Rápida**. La **Copia Completa** puede personalizarse fácilmente seleccionando las carpetas que desea copiar.

Haga clic en **Siguiente**.

20.1.3. Paso 3/5 - Seleccionar donde hacer Copia

Aquí puede seleccionar la ubicación dónde se guardaran los datos copiados.



Selección de destino de copia

Dispone de las siguientes opciones:

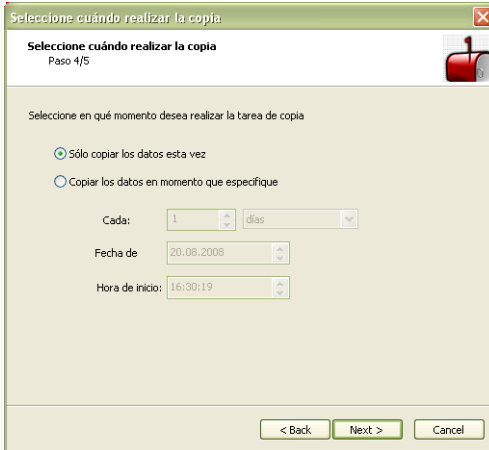
- Copiar datos en mi equipo
- Copiar datos en mi memoria USB
- Copiar datos en una ubicación de la red
- Copiar datos en CD/DVD
- Copiar datos en un servidor FTP

Si decide guardar los datos copiados en su equipo, una memoria USB o una ubicación de la red, haga clic en **Seleccionar ubicación** e indique dónde quiere guardar los datos.

Haga clic en **Siguiente**.

20.1.4. Paso 4/5 - Selección de cuándo realizar la copia

Desde aquí podrá seleccionar el momento en que desea realizar la copia de sus datos.



Seleccionar cuando realizar copia

Dispone de las siguientes opciones:

- **Sólo copiar datos esta vez**
- **Copiar datos y planificar la tarea**

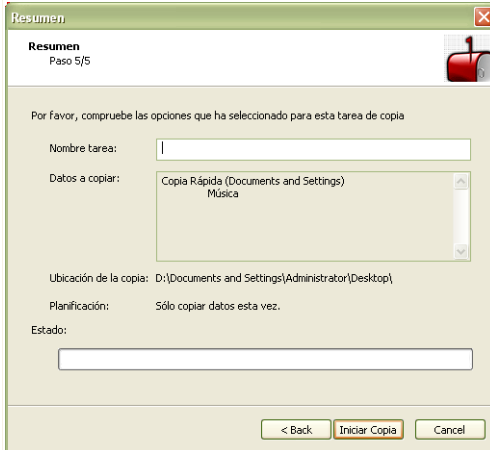
Para copiar sus datos inmediatamente haga clic en **Sólo copiar datos esta vez**. Si desea programar el producto para que realice la copia automáticamente en otro momento, haga clic en **Copiar datos y planificar la tarea**.

Si selecciona **Copiar datos y planificar la tarea**, puede indicar la frecuencia con la que se realizará la copia: diariamente o semanalmente. Además, puede indicar la fecha y hora de inicio.

Haga clic en **Siguiente**.

20.1.5. Paso 5/5 - Resumen

Desde aquí puede revisar la configuración de la tarea.



Resumen

Debe introducir el nombre de la tarea en el campo correspondiente.

Haga clic en **Iniciar copia** si está de acuerdo con la configuración detallada.

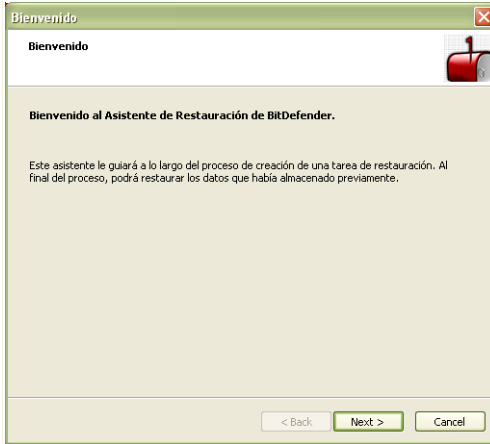
Haga clic en **Finalizar**.

20.2. Restaurando las Copias de Seguridad Locales

Al hacer clic en **Restauración Local** se iniciará un asistente que le guiará a través del proceso de restauración de sus datos copiados.

20.2.1. Paso 1/4 - Ventana de Bienvenida

Esta es sólo una ventana de bienvenida.

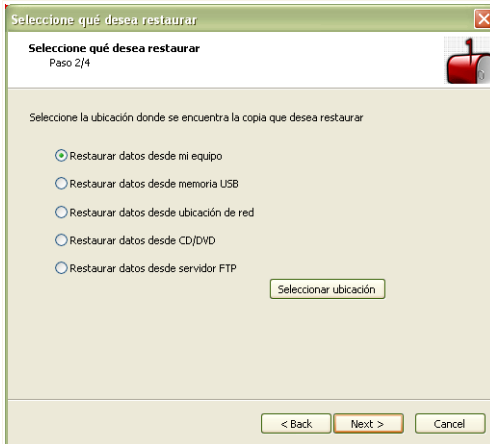


Ventana de Bienvenida

Haga clic en **Siguiente**.

20.2.2. Paso 2/4 - Seleccione la Copia a restaurar

Aquí puede seleccionar la ubicación desde dónde desea restaurar los archivos.



Seleccione la Copia a restaurar

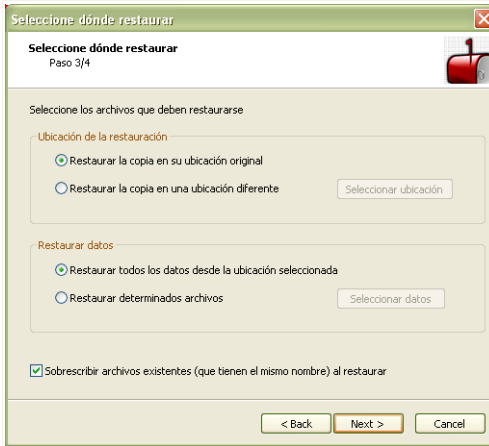
Dispone de las siguientes opciones:

- Restaurar datos desde mi equipo
- Restaurar datos desde memoria USB
- Restaurar datos desde ubicación de red
- Restaurar datos desde CD/DVD
- Restaurar datos desde servidor FTP

Haga clic en **Siguiente**.

20.2.3. Paso 3/4 - Seleccionar la Ubicación de Restauración y los Archivos

Aquí puede especificar los archivos que desea restaurar y la ubicación dónde desea restaurarlos.



Seleccionar la Ubicación de Restauración y los Archivos

Dispone de las siguientes opciones:

- Restaurar la copia a su ubicación original
- Restaurar la copia en una ubicación diferente
- Restaurar todos los datos desde la ubicación de copia seleccionada
- Restaurar archivos específicos
- Sobrescribir los archivos existentes al restaurar

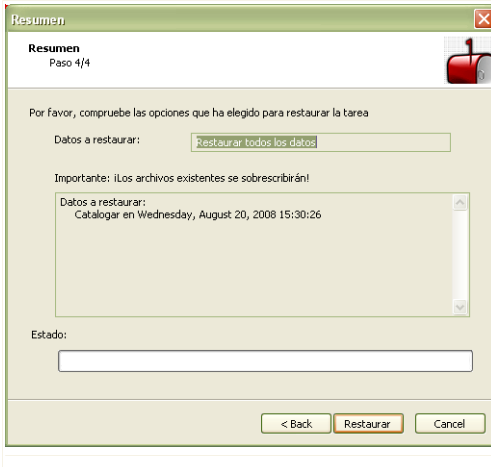
Si desea restaurar los datos en otra carpeta, o restaurar únicamente determinados archivos, seleccione la ubicación y los datos haciendo clic en el botón correspondiente.

Para evitar sobrescribir los archivos existentes al realizar la restauración, desmarque la casilla **Sobrescribir los archivos existentes al restaurar**.

Haga clic en **Siguiente**.

20.2.4. Paso 4/4 - Resumen

Desde aquí puede revisar la configuración de la tarea de restauración.



Haga clic en **Restaurar** si está de acuerdo con la configuración detallada.

Haga clic en **Finalizar**.

20.3. Copias de Seguridad Avanzadas

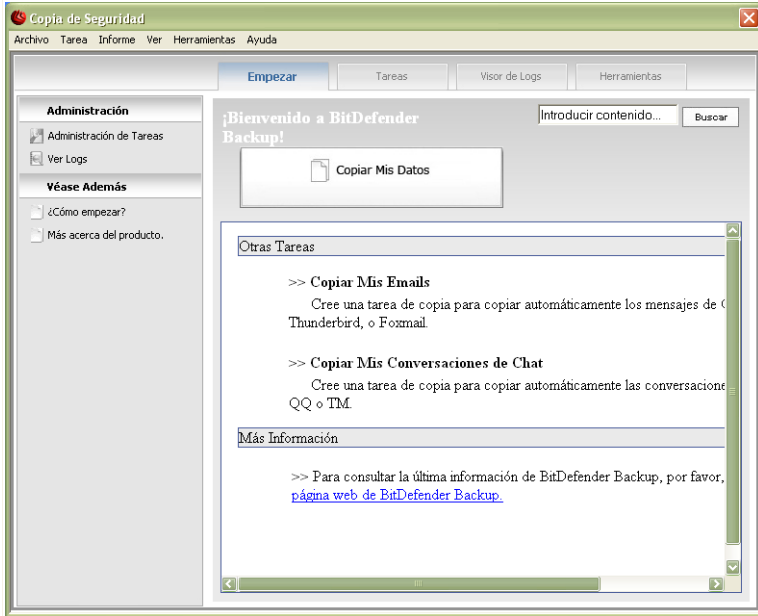
Si necesita realizar operaciones de copia y restauración más complejas puede utilizar la solución Copia de Seguridad de BitDefender. La solución Copia de Seguridad de BitDefender ofrece:

- una variedad de operaciones de copia, como compresión, cifrado, filtrado de archivos y velocidad de copia.
- control refinado al restaurar archivos (por ejemplo, puede restaurar los datos copiados en un momento determinado).
- funciones avanzadas de programación (por ejemplo, puede optar por iniciar la tarea de copia en un momento determinado o cuando el equipo esté inactivo).
- un visor de sucesos que le permite mantener un registro de las operaciones de copia y restauración, así como los errores que puedan producirse.

En este apartado encontrará información sobre la interfaz gráfica y características de la aplicación Copia de Seguridad de BitDefender.



Para abrir la aplicación Copia de Seguridad de BitDefender, haga clic en **Configuración de Copia**.

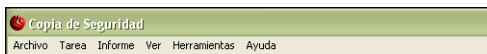


Copia de Seguridad de BitDefender

Hay dos maneras de configurar y realizar operaciones de Copias de Seguridad. Puede realizarlo desde la **Barra de Menú** de la parte superior, o haga clic en la pestaña desde la **Barra de Navegación**.

20.3.1. Barra de Menú

Hay seis menús de que puede utilizar para realizar todas las opciones de la solución Copia de Seguridad de BitDefender.



Barra de Menú



Archivo

- **Crear Nueva Tarea:** Muestra un cuadro de diálogo para crear una tarea de copia u otro tipo de tarea.
- **Abrir Archivo de Copia:** Muestra un cuadro de diálogo para abrir el archivo de copia o el catálogo de ajustes para realizar una restauración.
- **Salir:** Permite salir del apartado de copias de seguridad de BitDefender.

Tarea

- **Copia:** Realiza una copia de seguridad de la tarea seleccionada. Si ha seleccionado más de una tarea de copia, se ejecutarán todas las indicadas.
- **Restaurar Archivo:** Restaura la tarea seleccionada. Si ha seleccionado más de una tarea, se ejecutarán todas las indicadas.
- **Restaurar Datos por Fecha:** Restaura la tarea seleccionada a una fecha determinada. Si ha seleccionado más de una tarea, se ejecutarán todas las indicadas.
- **Planificar:** Planifica la ejecución de la tarea o modifica la planificación existente.
- **Eliminar Planificación:** Elimina la planificación de la tarea seleccionada.
- **Eliminar:** Elimina la tarea seleccionada. Si ha seleccionado más de una tarea, eliminará todas las indicadas.
- **Eliminar Todo:** Elimina todas las tareas del administrador de tareas.
- **Explorar Destino:** Permite ver los datos que han sido copiados de la tarea seleccionada.
- **Modificar Opciones:** Modifica las opciones de la tarea seleccionada.
- **Propiedades:** Permite modificar las propiedades de la tarea seleccionada, como el origen de los datos, nombre, destino, etc. de la tarea.

Informe

- **Ver Informe:** Si la tarea seleccionada contiene opciones de seguridad, permite ver el contenido del informe de la tarea.
- **Guardar como:** Guarda el contenido del informe seleccionado a un archivo especificado.
- **Imprimir:** Imprime el contenido del informe seleccionado.
- **Limpiar Todo:** Elimina el contenido del informe seleccionado.
- **Actualizar:** Actualiza el contenido del informe seleccionado.

Ver

- **Empezar:** Si no se muestra la ventana de inicio, esta opción permite visualizarla.
- **Administrador de Tarea:** Si no se muestra la ventana de tareas, esta opción permite visualizarla.
- **Visor de Logs:** Si no se muestra la ventana del visor de logs, esta opción permite visualizarla.



- **Herramientas:** Si no se muestra la ventana de herramientas, esta opción permite visualizarla.
- **Mostrar Barra de Menú :** Oculta la Barra de Menú. Para visualizarla, pulse ALT.
- **Mostrar Cuadrícula:** Muestra u oculta la cuadrícula. Esto se aplica tanto al visor de logs como al administrador de tareas.

Herramientas

- **Asistente de Copia:** Inicia el asistente de copias de seguridad.
- **Asistente de Restauración:** Inicia el asistente de restauración.
- **Grabar:** Inicia la herramienta de grabación de CD/DVD/ISO o una herramienta de grabación.
 - Grabar CD/DVD
 - Grabar Archivos ISO
 - Ver Información Grabadora
- **Exportar Todas las Tareas:** Exporta todas las tareas creadas a un archivo especificado.
- **Importar Tareas:** Importar tareas desde un archivo .JOB, .TXT, o .XML.
- **Exportar Logs:** Exporta los logs a un archivo .TXT o .XML.
 - A un archivo TXT
 - A un archivo XML
- **Importar Logs:** Importa los logs desde un archivo .TXT o .XML.
 - Desde un archivo TXT
 - Desde un archivo XML
- **Opciones:** Modifica la opciones globales de sus copias de seguridad.
 - General
 - Informes y Logs
 - Planificador de Tareas

Ayuda

- **Tema de Ayuda:** Muestra los temas de ayuda.
- **Buscar:** Permite buscar los temas que contienen la palabra seleccionada.
- **BitDefender en la Web:** Le dirige a la página web de BitDefender, dónde podrá buscar noticias relacionadas con el producto o soporte técnico.
- **Acerca de BitDefender Backup:** Muestra el copyright, versión y edición relacionada con Copia de Seguridad de BitDefender.

20.3.2. Barra de Navegación

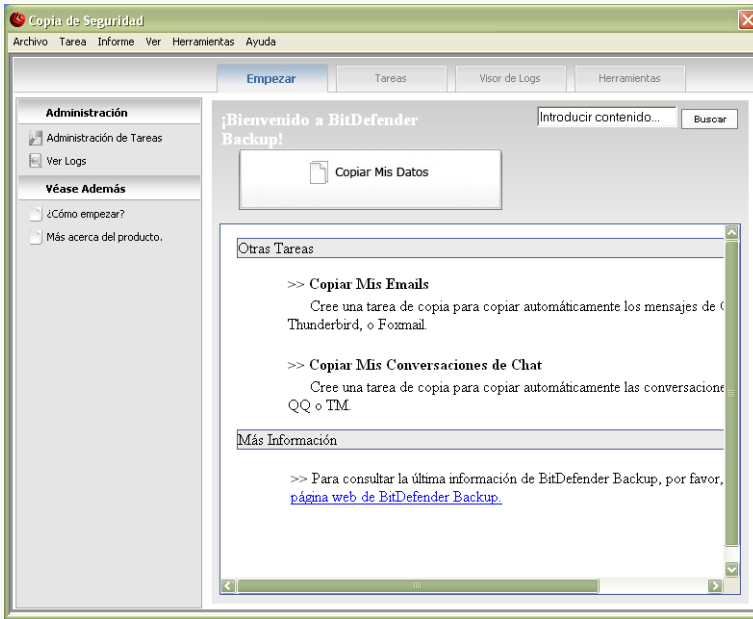
La **Barra de Navegación**, situada en la parte superior de la ventana principal y justo debajo de la **Barra de Menú**, le permite acceder las siguientes opciones:



- Empezar
- Tareas
- Visor de Logs
- Herramientas

Empezar

El área **Empezar** le ayuda a realizar copias de su correo, conversaciones de chat y datos con suma facilidad.



Empezar

Puede ir a la ventana **Empezar** siguiendo alguno de estos pasos:

- Haga clic en **Empezar** en la **Barra de Navegación**.
- Haga clic **Ver** en la **Barra de Menú** y seleccione **Empezar**.
- Utilice el método abreviado pulsando **CTRL+Alt+S**.



Para realizar una copia de seguridad de sus documentos, fotografías o conversaciones de chat a través de una sola tarea, haga clic en el botón **Copiar Mis Datos** y siga las instrucciones del asistente de tres pasos.

Para realizar una copia de seguridad de su correo, haga clic en el botón **Copiar Mis Emails** y siga las instrucciones del asistente de tres pasos.

Para realizar una copia de seguridad de sus conversaciones de chat, haga clic en el botón **Copiar Mis Conversaciones** y siga las instrucciones del asistente de tres pasos.

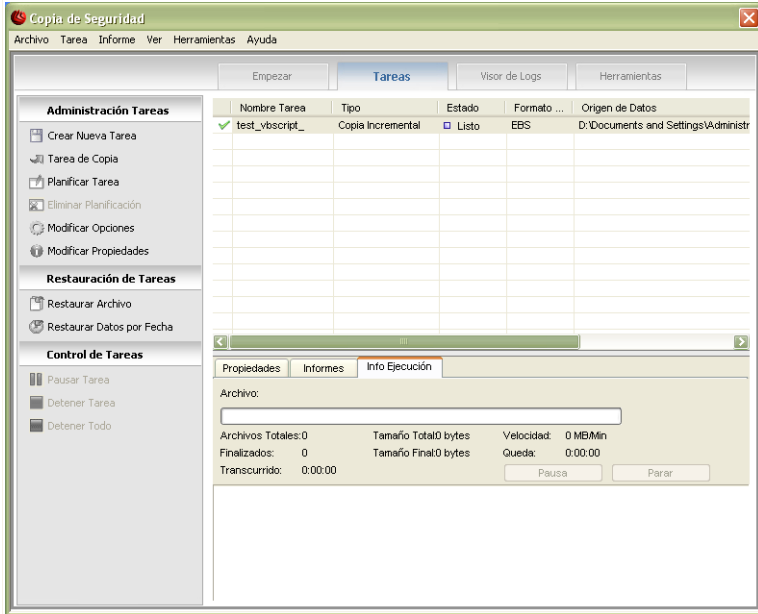


Nota

El proceso, que consta de 3 pasos, se describe en el apartado **Crear Nueva Tarea**.

Tareas

La ventana **Tareas** se utiliza para ver las tareas de copia, las propiedades de la tarea, los informes, y para monitorizar la velocidad de ejecución. Desde esta ventana puede comprobar las propiedades de la tarea y su estado, modificar la configuración de la tarea o realizar tareas de backup o restauración.



Tareas

Puede acceder a la ventana **Tareas** siguiendo alguno de estos pasos:

- Haga clic en **Tareas** en la **Barra de Navegación**.
- Haga clic en **Ver** en la **Barra de Menú** y seleccione **Tareas**.
- Utilice el método abreviado pulsando **CTRL+Alt+M**.

En la parte izquierda verá una lista de operaciones rápidas, como las siguientes:

Administración Tareas.

- **Crear Nueva Tarea**
- **Tarea de Copia**
- **Planificar Tarea**
- **Eliminar Planificación**
- **Modificar Opciones**
- **Modificar Propiedades**



Restaurar Tarea

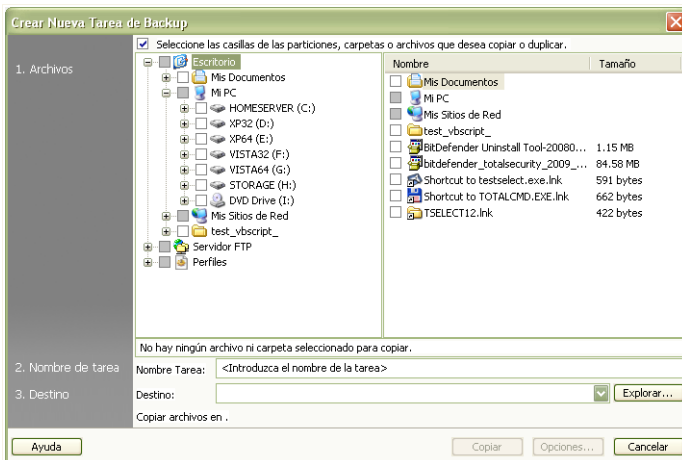
- Restaurar Archivo
- Restaurar Datos a un Punto en Tiempo

Control de Tareas

- Pausar Tareas
- Parar Tarea
- Parar Todo

Crear Nueva Tarea

Para realizar una copia de seguridad de sus documentos importantes, fotos o conversaciones de chat en una misma tarea, haga clic en el botón **Crear Nueva Tarea** y siga el asistente de tres pasos.



Crear Nueva Tarea

1. Haga clic en las casillas para seleccionar las particiones, carpetas o archivos que desea copiar.

Al seleccionar un elemento de la ventana de la izquierda, su contenido se mostrará en la parte derecha para ayudarle a mejorar su selección.

2. Escriba un nombre para la tarea de copia, o aceptando el nombre por defecto.

El nombre por defecto se genera automáticamente al seleccionar los archivos o carpetas que desea copiar, pero puede modificarlo.



3. Haga clic en **Explorar** para seleccionar dónde desea guardar los datos en su archivo de copia.

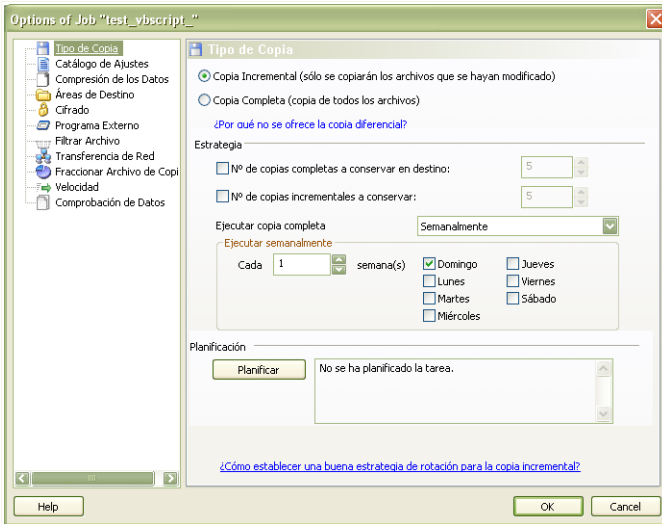


Nota

No olvide hacer clic en **Copiar** para iniciar el proceso, o en **Cancelar** para detenerlo. Para ajustar su configuración, haga clic en **Opciones**.

Cuadro de Diálogo de Opciones de Backup

Existen varias subopciones en el cuadro de diálogo de **Opciones**.



Cuadro de Diálogo de Opciones de Backup

Tipo de Copia

BitDefender Backup soporta dos tipos de copia.

- **Copia Completa:** Copia todos los datos de la carpeta origen indicada y los guarda en la carpeta de destino. Al realizar una copia completa, la Copia de Seguridad de BitDefender copiará todos los datos, NO sólo aquellos que hayan sido modificados.
- **Copia Incremental:** La primera vez que se ejecuta, actúa igual que la Copia Completa y copia todos los datos. Cuando se ejecute posteriormente, sólo



copiará los archivos nuevos y aquellos que hayan sido modificados. Cada vez que se ejecuta una Copia Incremental, se crea un archivo de copia.

La Copia Completa y la Incremental pueden combinarse en una **Rotación de Copia**. Por ejemplo, puede crear una Copia Completa cada Domingo, y una Copia Incremental cada día para añadir las modificaciones que se hagan en los archivos a lo largo de la semana. Así es como se configuraría: Seleccionar **Semanalmente** en el menú, **1** en el campo **Cada semana** y marcar Domingo. Esta copia completa del domingo eliminaría todas las copias anteriores, y sería la base para la Copia Incremental.

Catálogo de Ajustes

Se utiliza para indexar la información de cada copia y es la base de los procesos de Copia Incremental y Restauración. El catálogo de ajustes (*.ecs) contiene un índice de todos los archivos y carpetas del archivo de copia. Cada índice contiene datos sobre la hora en que se ha realizado la copia, la carpeta de la copia, el nombre de los ficheros y las propiedades. Los datos pueden restaurarse desde el catálogo.

El nombre del catálogo de ajustes se genera automáticamente en función de la carpeta de destino. Para modificar el catálogo de ajustes de una tarea, siga estos pasos:

1. Haga clic **Catálogo de Ajustes**.
2. Introduzca el nombre del archivo en el campo correspondiente.
3. Haga clic en **Explorar** para seleccionar la carpeta dónde desea guardar el Catálogo.
4. Haga clic en **Aceptar**.

Compresión de los Datos

BitDefender Backup puede comprimir y guardar los datos en el archivo de copia para ahorrar espacio. Soporta tres tipos de compresión: Rápida, Estándar y Máxima. Por ejemplo, para iniciar una compresión estándar, siga estos pasos:

1. Haga clic **Compresión de los Datos**.
2. Haga clic en **Compresión Estándar**.
3. Haga clic en **Aceptar**.

Áreas de Destino

Copia de Seguridad de BitDefender permite repartir el archivo de copia entre diferentes ubicaciones. Por ejemplo, si no dispone de suficiente espacio libre en una ubicación para que se realice la copia, la operación de copia continuará en otra área.

Puede añadir una o más áreas de destino para que la copia prosiga, o modificar estas áreas, siguiendo estos pasos:



1. Haga clic **Áreas de Destino**.
2. Haga clic en **Añadir** para seleccionar una nueva área de destino para guardar los datos.
3. Haga clic en **Editar** para modificar las áreas de destino definidas.
4. Haga clic en **Eliminar** para eliminar la área de destino seleccionada.
5. Haga clic en **Eliminar Todo** para eliminar todas las áreas de destino.
6. Haga clic en **Aceptar**.

Cifrado

Copia de Seguridad de BitDefender puede asegurar sus datos cifrándolos antes de que se guarden en el archivo de copia. En las opciones de seguridad de la tarea puede incluir la contraseña de protección.

Para cifrar los datos antes de realizar la copia, siga estos pasos:

1. Haga clic en **Cifrado**.
2. Seleccione el tipo de cifrado en el menú desplegable.
3. Introduzca su contraseña en el campo correspondiente.
4. Vuelva a introducir su contraseña en el campo correspondiente.
5. Haga clic en **Aceptar**.

Programa Externo

Puede iniciar comandos o programas externos justo antes o después de realizar la copia. Las aplicaciones deben ser `.exe`, `.com` o `.bat`, o algún tipo de evento como "apagar el equipo al finalizar la copia".

Para ejecutar un comando antes de iniciar la copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Antes de Iniciar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. Haga clic en **Aceptar**.

Para ejecutar un programa cuando finalice el proceso de copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Al Finalizar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. O haga clic en **Apagar Equipo** cuando finalice la copia.
5. O haga clic en **Reiniciar Equipo** cuando finalice la copia.
6. O haga clic en **Cerrar Sesión** cuando finalice la copia.
7. Haga clic en **Aceptar**.



Nota

Si desea iniciar el programa o comandos incluso si el proceso de copia falla, marque la casilla **Ejecutar programa externo aunque la tarea falle**.

Filtrar Archivo

Copia de Seguridad de BitDefender incluye opciones de filtrado para incluir o excluir los archivos concretos, tipos de archivos o carpetas, con el objetivo de ahorrar espacio y mejorar la velocidad de la copia.

Puede filtrar un archivo concreto siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Tipo de Filtro**.
3. Puede excluir o incluir tipos de archivo marcando la opción **Incluir sólo tipos de archivo seleccionados** o **Excluir tipos de archivo seleccionados**.
4. Si es necesario, puede introducir un nuevo tipo de archivo en el campo **Tipo Personalizado**, pero asegúrese que utiliza el formato `.abc`. Use `,` (coma) como separador si introduce más de un tipo. También puede añadir una breve descripción en el campo correspondiente.
5. Haga clic en **Aceptar**.

Puede filtrar un archivo en concreto siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Filtrar Archivo**.
3. Excluya o incluya archivos concretos marcando las opciones **Incluir sólo archivos especificados** o **Excluir archivos especificados**.
4. Haga clic en **Explorar** y seleccione el archivo. La ruta del archivo se añadirá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para excluir o incluir el archivo independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.

Puede filtrar una carpeta siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en la opción **Filtrar Carpeta**.
3. Excluya o incluya las carpetas específicas en las ventanas de diálogo, marcando la opción **Incluir sólo las carpetas especificadas en la regla**, o en la opción **Excluir las carpetas especificadas en la regla**.
4. Haga clic en **Explorar** y seleccione la carpeta. La ruta de la carpeta seleccionada aparecerá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para incluir o excluir carpetas independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.



Los filtros se pueden modificar siguiendo los pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en el filtro que desea modificar y a continuación **Editar**.
3. Modificar las opciones en la ventana de dialogo.
4. Haga clic en **Aceptar**.

Los filtros se pueden eliminar mediante los siguientes pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en el filtro que desea eliminar y a continuación seleccione la opción **Eliminar**.
3. Haga clic en **Eliminar todo** si desea eliminar todos los filtros.
4. Haga clic en **Aceptar**.

Transferencia de Red

Copia de Seguridad de BitDefender le permite realizar copias y restauraciones sobre los datos compartidos en grupos de trabajo conectados en red. En caso que de no poder acceder a la red, BitDefender intentará realizar éstas operaciones periódicamente. Para indicar la frecuencia y la cantidad de intentos que deben realizarse, siga estos pasos:

1. Haga clic en **Transferencia de Red**.
2. Haga clic en **Cuando falle el acceso a archivos de la red, volver a intentar el acceso**.
3. Indique la frecuencia con la que desea volver a intentar copiar los datos (en segundos).
4. Indique cuantas veces desea reintentar la copia.
5. Haga clic en **Aceptar**.



Nota

Para evitar recibir demasiada información sobre errores de la red, haga clic en **No generar ningún informe si la red no está disponible**.

Fraccionar Archivo de Copia

El archivo de copia puede fraccionarse en pequeños archivos de copia, para que puedan almacenarse en diferentes destinos (como un disquete, CD/DVD..). La Copia de Seguridad de BitDefender le ofrece dos métodos de fraccionamiento: fraccionamiento automático y basado en un tamaño.

Las opciones de fraccionamiento pueden modificarse mediante estos pasos:

1. Haga clic en **Fraccionar Archivo de Copia**.
2. Seleccione **Fraccionar automáticamente según el espacio de destino**.
3. O seleccione **Indicar tamaño a fraccionar** y seleccione el tamaño que desee en el menú desplegable.



4. Haga clic en **Aceptar**.

Velocidad

La Copia de Seguridad de BitDefender soporta tres tipos de velocidad. A mayor velocidad, mayor consumo.

La velocidad de la copia puede especificarse siguiendo estos pasos:

1. Haga clic en **Velocidad**.
2. Seleccione una velocidad entre **Máxima**, **Media** o **Baja**.
3. Haga clic en **Aceptar**.

Comprobación de Datos

Para asegurarse de que los datos copiados son seguros, siga estos pasos:

1. Haga clic **Comprobación de Datos**.
2. Haga clic **Comprobar datos durante el proceso de copia**.
3. Haga clic en **Aceptar**.

Tarea de Copia

Una vez haya creado la tarea, la copia de seguridad se realizará automáticamente. Sin embargo, puede entrar al **Administrador de Tarea** para ejecutar la copia manualmente, seleccionando la tarea y haciendo clic en la opción **Tarea de Copia** del menú.

Para tener más detalles sobre la copia en el momento de la restauración, introduzca una pequeña descripción en la ventana emergente que aparecerá. Haga clic en **Cancelar** para ignorar la descripción, o en **Aceptar** para continuar. También puede cancelar la tarea de copia haciendo clic en el botón **Cancelar Copia**.

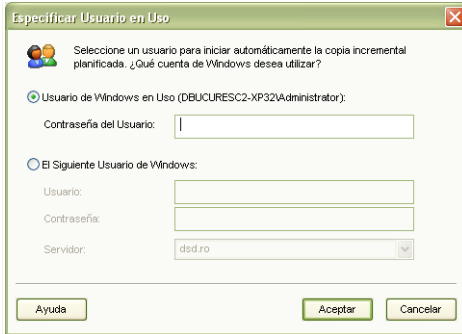


Nota

Para conseguir información más detallada, puede consultar las **Propiedades**, los **Informes** y la **Info Ejecución** de la tarea desde la ventana de la barra de estado.

Planificación de la Tarea

Desde aquí puede planificar la tarea de copia para que se realice cuando desee. Puede planificar la tarea para que se ejecute diariamente, semanalmente, mensualmente o en el momento que indique (por ejemplo, al iniciar el sistema). La **Planificación de la Tarea** es la base para automatizar las copias.



Planificación de la Tarea

Si su equipo es miembro de una red con dominio, deberá seguir unos pasos adicionales para poder planificar una tarea.

1. Seleccione la tarea que desea planificar y haga clic en **Planificación de la Tarea**.
2. Aparecerá el cuadro de diálogo del **Usuario en Uso**. Si es un usuario de dominio, por favor, introduzca su contraseña del dominio.
3. En caso contrario, seleccione **El Siguiente Usuario de Windows**.
4. Introduzca el nombre de usuario, la contraseña y el nombre del servidor de dominio.
5. Haga clic en **Aceptar**.

Tras introducir el usuario en uso, la Copia de Seguridad de BitDefender mostrará el cuadro de diálogo de **Planificación** para que pueda programar la ejecución de la tarea en el momento que considere más conveniente.

Desde aquí podrá indicar la frecuencia con la que se ejecutará la tarea: diariamente, semanalmente, una única vez, al iniciar el sistema, al iniciar sesión o cuando el equipo esté inactivo. Si la tarea se planifica diariamente, semanalmente o una única vez, también podrá definir la hora de inicio. También podrá planificar la tarea en base a una cantidad de días, semana, día del mes o fecha. Otra posibilidad es indicar la cantidad de minutos de inactividad que deben transcurrir para iniciar la tarea.

También es posible hacer múltiples planificaciones a una tarea, haciendo clic en **Mostrar planificaciones múltiples**. Haciendo clic en **Avanzado** podrá configurar opciones de planificación adicionales. Por ejemplo, puede definir la fecha de inicio y fin de la tarea.

Para precisar más la planificación de la tarea, haga clic en la pestaña **Configuración**. Existen tres subopciones.



■ **Planificación de la Tarea Completada**

- Eliminar la tarea si no está planificada para ejecutarse de nuevo.

Esta opción es útil para las tareas programadas para ejecutarse sólo una vez.

- Detener la tarea si dura más de:

Indique cuanto tiempo debe transcurrir desde el inicio de la tarea hasta que sea detenida.

■ **Tiempo de Inactividad**

- Iniciar la tarea sólo si el equipo ha estado inactivo al menos:

Indique cuanto tiempo (en minutos) debe pasar desde que el teclado o el ratón se han dejado de utilizar hasta que se pueda iniciar la tarea.

- Si el equipo no ha estado inactivo tanto tiempo, reintentar durante:

Indique durante cuanto tiempo (en minutos) debe seguir comprobándose si el equipo está inactivo.

- Detener la tarea si el ordenador deja de estar inactivo.

Indique si la tarea debe detenerse cuando vuelva a utilizarse el equipo.

■ **Administración de la Energía**

- No iniciar la tarea si el equipo funciona con batería.

Indique si desea impedir la ejecución de la tarea en aquellos momentos en los que el equipo funcione con la batería. Al marcar esta casilla alargará la duración de la batería.

- Detener la tarea al usar la batería.

Indique si la tarea debe detenerse en el momento en que el equipo empiece a utilizar la batería.

- Despertar al equipo para iniciar esta tarea.

Indique si el equipo debe iniciar la tarea incluso si está en modo Hibernación/Suspensión.

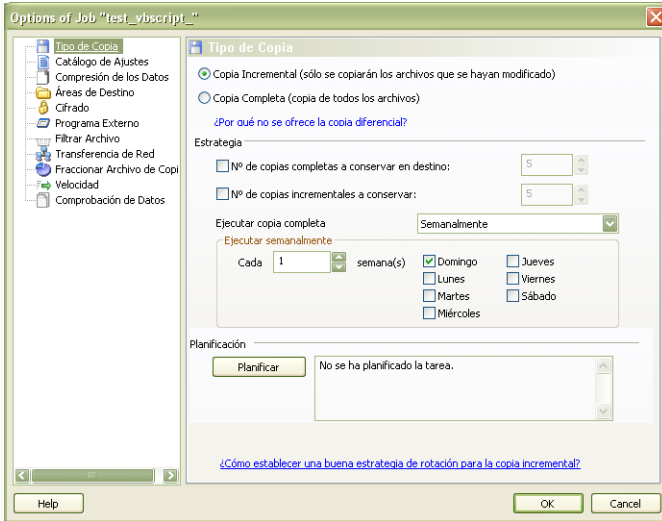
Eliminar Planificación de la Tarea

Para eliminar la planificación de la tarea, haga clic en **Eliminar Planificación** en el apartado **Administración Tareas**.

Si la tarea no está planificada, la opción **Eliminar Planificación** aparecerá en gris, indicando que no es posible utilizarla.

Modificar las Opciones de la Tarea

Para modificar las opciones de una tarea, selecciónela y haga clic en **Modificar Opciones** en el apartado **Administración Tareas**.

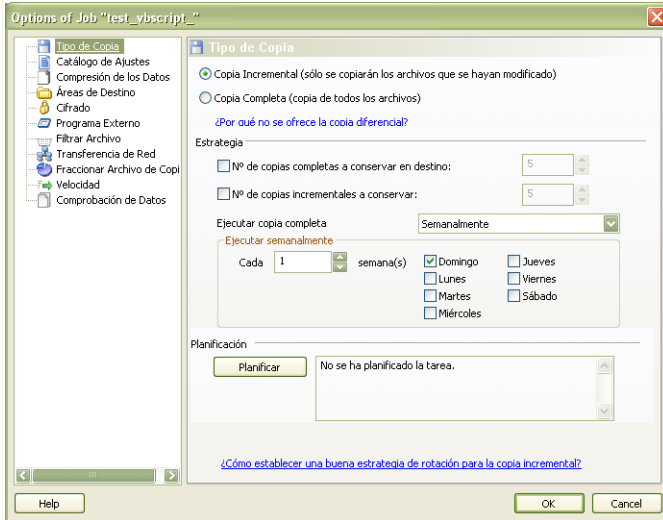


Modificar las Opciones de la Tarea

La tarea seleccionada puede ser una tarea de copia o una tarea de grabación. A continuación se explicará como modificar las opciones de cada una de ellas:

Cuadro de Diálogo de Opciones de Backup

Existen varias subopciones en el cuadro de diálogo de **Opciones**.



Cuadro de Diálogo de Opciones de Backup

Tipo de Copia

BitDefender Backup soporta dos tipos de copia.

- **Copia Completa:** Copia todos los datos de la carpeta origen indicada y los guarda en la carpeta de destino. Al realizar una copia completa, la Copia de Seguridad de BitDefender copiará todos los datos, NO sólo aquellos que hayan sido modificados.
- **Copia Incremental:** La primera vez que se ejecuta, actúa igual que la Copia Completa y copia todos los datos. Cuando se ejecute posteriormente, sólo copiará los archivos nuevos y aquellos que hayan sido modificados. Cada vez que se ejecuta una Copia Incremental, se crea un archivo de copia.

La Copia Completa y la Incremental pueden combinarse en una **Rotación de Copia**. Por ejemplo, puede crear una Copia Completa cada Domingo, y una Copia Incremental cada día para añadir las modificaciones que se hagan en los archivos a lo largo de la semana. Así es como se configuraría: Seleccionar **Semanalmente** en el menú, 1 en el campo **Cada semana** y marcar Domingo. Esta copia completa del domingo eliminaría todas las copias anteriores, y sería la base para la Copia Incremental.



Catálogo de Ajustes

Se utiliza para indexar la información de cada copia y es la base de los procesos de Copia Incremental y Restauración. El catálogo de ajustes (*.ecs) contiene un índice de todos los archivos y carpetas del archivo de copia. Cada índice contiene datos sobre la hora en que se ha realizado la copia, la carpeta de la copia, el nombre de los ficheros y las propiedades. Los datos pueden restaurarse desde el catálogo.

El nombre del catálogo de ajustes se genera automáticamente en función de la carpeta de destino. Para modificar el catálogo de ajustes de una tarea, siga estos pasos:

1. Haga clic **Catálogo de Ajustes**.
2. Introduzca el nombre del archivo en el campo correspondiente.
3. Haga clic en **Explorar** para seleccionar la carpeta dónde desea guardar el Catálogo.
4. Haga clic en **Aceptar**.

Compresión de los Datos

BitDefender Backup puede comprimir y guardar los datos en el archivo de copia para ahorrar espacio. Soporta tres tipos de compresión: Rápida, Estándar y Máxima. Por ejemplo, para iniciar una compresión estándar, siga estos pasos:

1. Haga clic **Compresión de los Datos**.
2. Haga clic en **Compresión Estándar**.
3. Haga clic en **Aceptar**.

Áreas de Destino

Copia de Seguridad de BitDefender permite repartir el archivo de copia entre diferentes ubicaciones. Por ejemplo, si no dispone de suficiente espacio libre en una ubicación para que se realice la copia, la operación de copia continuará en otra área.

Puede añadir una o más áreas de destino para que la copia prosiga, o modificar estas áreas, siguiendo estos pasos:

1. Haga clic **Áreas de Destino**.
2. Haga clic en **Añadir** para seleccionar una nueva área de destino para guardar los datos.
3. Haga clic en **Editar** para modificar las áreas de destino definidas.
4. Haga clic en **Eliminar** para eliminar la área de destino seleccionada.
5. Haga clic en **Eliminar Todo** para eliminar todas las áreas de destino.
6. Haga clic en **Aceptar**.



Cifrado

Copia de Seguridad de BitDefender puede asegurar sus datos cifrándolos antes de que se guarden en el archivo de copia. En las opciones de seguridad de la tarea puede incluir la contraseña de protección.

Para cifrar los datos antes de realizar la copia, siga estos pasos:

1. Haga clic en **Cifrado**.
2. Seleccione el tipo de cifrado en el menú desplegable.
3. Introduzca su contraseña en el campo correspondiente.
4. Vuelva a introducir su contraseña en el campo correspondiente.
5. Haga clic en **Aceptar**.

Programa Externo

Puede iniciar comandos o programas externos justo antes o después de realizar la copia. Las aplicaciones deben ser `.exe`, `.com` o `.bat`, o algún tipo de evento como "apagar el equipo al finalizar la copia".

Para ejecutar un comando antes de iniciar la copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Antes de Iniciar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. Haga clic en **Aceptar**.

Para ejecutar un programa cuando finalice el proceso de copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Al Finalizar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. O haga clic en **Apagar Equipo** cuando finalice la copia.
5. O haga clic en **Reiniciar Equipo** cuando finalice la copia.
6. O haga clic en **Cerrar Sesión** cuando finalice la copia.
7. Haga clic en **Aceptar**.



Nota

Si desea iniciar el programa o comandos incluso si el proceso de copia falla, marque la casilla **Ejecutar programa externo aunque la tarea falle**.

Filtrar Archivo

Copia de Seguridad de BitDefender incluye opciones de filtrado para incluir o excluir los archivos concretos, tipos de archivos o carpetas, con el objetivo de ahorrar espacio y mejorar la velocidad de la copia.



Puede filtrar un archivo concreto siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Tipo de Filtro**.
3. Puede excluir o incluir tipos de archivo marcando la opción **Incluir sólo tipos de archivo seleccionados** o **Excluir tipos de archivo seleccionados**.
4. Si es necesario, puede introducir un nuevo tipo de archivo en el campo **Tipo Personalizado**, pero asegúrese que utiliza el formato `.abc`. Use `,` (coma) como separador si introduce más de un tipo. También puede añadir una breve descripción en el campo correspondiente.
5. Haga clic en **Aceptar**.

Puede filtrar un archivo en concreto siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Filtrar Archivo**.
3. Excluya o incluya archivos concretos marcando las opciones **Incluir sólo archivos especificados** o **Excluir archivos especificados**.
4. Haga clic en **Explorar** y seleccione el archivo. La ruta del archivo se añadirá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para excluir o incluir el archivo independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.

Puede filtrar una carpeta siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en la opción **Filtrar Carpeta**.
3. Excluya o incluya las carpetas específicas en las ventanas de diálogo, marcando la opción **Incluir sólo las carpetas especificadas en la regla**, o en la opción **Excluir las carpetas especificadas en la regla**.
4. Haga clic en **Explorar** y seleccione la carpeta. La ruta de la carpeta seleccionada aparecerá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para incluir o excluir carpetas independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.

Los filtros se pueden modificar siguiendo los pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en el filtro que desea modificar y a continuación **Editar**.
3. Modificar las opciones en la ventana de diálogo.
4. Haga clic en **Aceptar**.

Los filtros se pueden eliminar mediante los siguientes pasos:

1. Haga clic en **Filtrar Archivo**.



2. Haga clic en el filtro que desea eliminar y a continuación seleccione la opción **Eliminar**.
3. Haga clic en **Eliminar todo** si desea eliminar todos los filtros.
4. Haga clic en **Aceptar**.

Transferencia de Red

Copia de Seguridad de BitDefender le permite realizar copias y restauraciones sobre los datos compartidos en grupos de trabajo conectados en red. En caso que de no poder acceder a la red, BitDefender intentará realizar éstas operaciones periódicamente. Para indicar la frecuencia y la cantidad de intentos que deben realizarse, siga estos pasos:

1. Haga clic en **Transferencia de Red**.
2. Haga clic en **Cuando falle el acceso a archivos de la red, volver a intentar el acceso**.
3. Indique la frecuencia con la que desea volver a intentar copiar los datos (en segundos).
4. Indique cuantas veces desea reintentar la copia.
5. Haga clic en **Aceptar**.



Nota

Para evitar recibir demasiada información sobre errores de la red, haga clic en **No generar ningún informe si la red no está disponible**.

Fraccionar Archivo de Copia

El archivo de copia puede fraccionarse en pequeños archivos de copia, para que puedan almacenarse en diferentes destinos (como un disquete, CD/DVD..). La Copia de Seguridad de BitDefender le ofrece dos métodos de fraccionamiento: fraccionamiento automático y basado en un tamaño.

Las opciones de fraccionamiento pueden modificarse mediante estos pasos:

1. Haga clic en **Fraccionar Archivo de Copia**.
2. Seleccione **Fraccionar automáticamente según el espacio de destino**.
3. O seleccione **Indicar tamaño a fraccionar** y seleccione el tamaño que desee en el menú desplegable.
4. Haga clic en **Aceptar**.

Velocidad

La Copia de Seguridad de BitDefender soporta tres tipos de velocidad. A mayor velocidad, mayor consumo.

La velocidad de la copia puede especificarse siguiendo estos pasos:

1. Haga clic en **Velocidad**.
2. Seleccione una velocidad entre **Máxima**, **Media** o **Baja**.



3. Haga clic en **Aceptar**.

Comprobación de Datos

Para asegurarse de que los datos copiados son seguros, siga estos pasos:

1. Haga clic **Comprobación de Datos**.
2. Haga clic **Comprobar datos durante el proceso de copia**.
3. Haga clic en **Aceptar**.

Modificar Opciones de una Tarea de Grabación

En el cuadro de diálogo de la tarea de grabación encontrará varias subopciones.

Grabar

Desde aquí podrá elegir si desea expulsar el disco tras la grabación, finalizar el disco o grabar datos con el sistema de archivos Joilet.

Si desea planificar la tarea, haga clic en **Planificar**.

Desde aquí puede planificar la tarea de copia para que se realice cuando desee. Puede planificar la tarea para que se ejecute diariamente, semanalmente, mensualmente o en el momento que indique (por ejemplo, al iniciar el sistema). La **Planificación de la Tarea** es la base para automatizar las copias.

Si su equipo es miembro de una red con dominio, deberá seguir unos pasos adicionales para poder planificar una tarea.

1. Seleccione la tarea que desea planificar y haga clic en **Planificación de la Tarea**.
2. Aparecerá el cuadro de diálogo del **Usuario en Uso**. Si es un usuario de dominio, por favor, introduzca su contraseña del dominio.
3. En caso contrario, seleccione **El Siguiente Usuario de Windows**.
4. Introduzca el nombre de usuario, la contraseña y el nombre del servidor de dominio.
5. Haga clic en **Aceptar**.

Tras introducir el usuario en uso, la Copia de Seguridad de BitDefender mostrará el cuadro de diálogo de **Planificación** para que pueda programar la ejecución de la tarea en el momento que considere más conveniente.

Desde aquí podrá indicar la frecuencia con la que se ejecutará la tarea: diariamente, semanalmente, una única vez, al iniciar el sistema, al iniciar sesión o cuando el equipo esté inactivo. Si la tarea se planifica diariamente, semanalmente o una única vez, también podrá definir la hora de inicio. También podrá planificar la tarea en base a una cantidad de días, semana, día del mes o fecha. Otra posibilidad es indicar la cantidad de minutos de inactividad que deben transcurrir para iniciar la tarea.



También es posible hacer múltiples planificaciones a una tarea, haciendo clic en **Mostrar planificaciones múltiples**. Haciendo clic en **Avanzado** podrá configurar opciones de planificación adicionales. Por ejemplo, puede definir la fecha de inicio y fin de la tarea.

Para precisar más la planificación de la tarea, haga clic en la pestaña **Configuración**. Existen tres subopciones.

■ **Planificación de la Tarea Completada**

- Eliminar la tarea si no está planificada para ejecutarse de nuevo.

Esta opción es útil para las tareas programadas para ejecutarse sólo una vez.

- Detener la tarea si dura más de:

Indique cuanto tiempo debe transcurrir desde el inicio de la tarea hasta que sea detenida.

■ **Tiempo de Inactividad**

- Iniciar la tarea sólo si el equipo ha estado inactivo al menos:

Indique cuanto tiempo (en minutos) debe pasar desde que el teclado o el ratón se han dejado de utilizar hasta que se pueda iniciar la tarea.

- Si el equipo no ha estado inactivo tanto tiempo, reintentar durante:

Indique durante cuanto tiempo (en minutos) debe seguir comprobándose si el equipo está inactivo.

- Detener la tarea si el ordenador deja de estar inactivo.

Indique si la tarea debe detenerse cuando vuelva a utilizarse el equipo.

■ **Administración de la Energía**

- No iniciar la tarea si el equipo funciona con batería.

Indique si desea impedir la ejecución de la tarea en aquellos momentos en los que el equipo funcione con la batería. Al marcar esta casilla alargará la duración de la batería.

- Detener la tarea al usar la batería.

Indique si la tarea debe detenerse en el momento en que el equipo empiece a utilizar la batería.

- Despertar al equipo para iniciar esta tarea.

Indique si el equipo debe iniciar la tarea incluso si está en modo Hibernación/Suspensión.



Programa Externo

Puede iniciar comandos o programas externos justo antes o después de realizar la copia. Las aplicaciones deben ser `.exe`, `.com` o `.bat`, o algún tipo de evento como "apagar el equipo al finalizar la copia".

Para ejecutar un comando antes de iniciar la copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Antes de Iniciar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. Haga clic en **Aceptar**.

Para ejecutar un programa cuando finalice el proceso de copia, siga estos pasos:

1. Haga clic en **Programa Externo**
2. Seleccione la opción **Al Finalizar la Tarea**.
3. Haga clic en **Explorar** para seleccionar el archivo de comandos o programa que desea ejecutar.
4. O haga clic en **Apagar Equipo** cuando finalice la copia.
5. O haga clic en **Reiniciar Equipo** cuando finalice la copia.
6. O haga clic en **Cerrar Sesión** cuando finalice la copia.
7. Haga clic en **Aceptar**.



Nota

Si desea iniciar el programa o comandos incluso si el proceso de copia falla, marque la casilla **Ejecutar programa externo aunque la tarea falle**.

Filtrar Archivo

Copia de Seguridad de BitDefender incluye opciones de filtrado para incluir o excluir los archivos concretos, tipos de archivos o carpetas, con el objetivo de ahorrar espacio y mejorar la velocidad de la copia.

Puede filtrar un archivo concreto siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Tipo de Filtro**.
3. Puede excluir o incluir tipos de archivo marcando la opción **Incluir sólo tipos de archivo seleccionados** o **Excluir tipos de archivo seleccionados**.
4. Si es necesario, puede introducir un nuevo tipo de archivo en el campo **Tipo Personalizado**, pero asegúrese que utiliza el formato `.abc`. Use `,` (coma) como separador si introduce más de un tipo. También puede añadir una breve descripción en el campo correspondiente.
5. Haga clic en **Aceptar**.

Puede filtrar un archivo en concreto siguiendo estos pasos:



1. Haga clic en **Filtrar Archivo**.
2. Haga clic en **Filtrar Archivo**.
3. Excluya o incluya archivos concretos marcando las opciones **Incluir sólo archivos especificados** o **Excluir archivos especificados**.
4. Haga clic en **Explorar** y seleccione el archivo. La ruta del archivo se añadirá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para excluir o incluir el archivo independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.

Puede filtrar una carpeta siguiendo estos pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en la opción **Filtrar Carpeta**.
3. Excluya o incluya las carpetas específicas en las ventanas de diálogo, marcando la opción **Incluir sólo las carpetas especificadas en la regla** o en la opción **Excluir las carpetas especificadas en la regla**.
4. Haga clic en **Explorar** y seleccione la carpeta. La ruta de la carpeta seleccionada aparecerá automáticamente en el campo **Aplicar a las siguientes carpetas**. Para incluir o excluir carpetas independientemente de su ubicación, haga clic en **Aplicar a todas las carpetas**.
5. Haga clic en **Aceptar**.

Los filtros se pueden modificar siguiendo los pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en el filtro que desea modificar y a continuación **Editar**.
3. Modificar las opciones en la ventana de diálogo.
4. Haga clic en **Aceptar**.

Los filtros se pueden eliminar mediante los siguientes pasos:

1. Haga clic en **Filtrar Archivo**.
2. Haga clic en el filtro que desea eliminar y a continuación seleccione la opción **Eliminar**.
3. Haga clic en **Eliminar todo** si desea eliminar todos los filtros.
4. Haga clic en **Aceptar**.

Comprobación de Datos

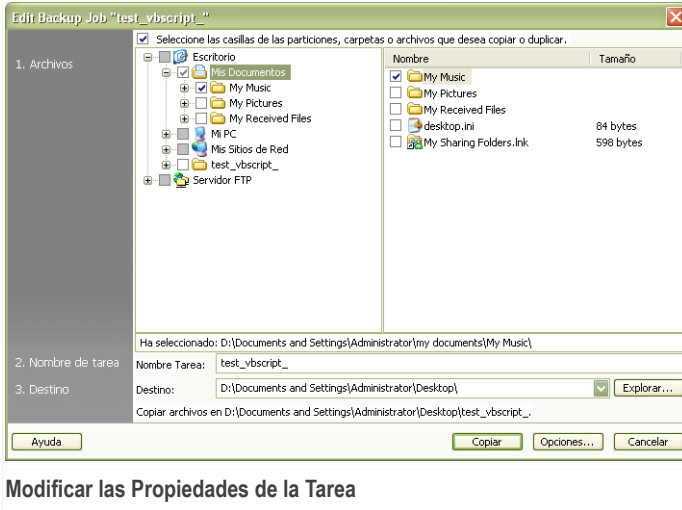
Para asegurarse de que los datos copiados son seguros, siga estos pasos:

1. Haga clic **Comprobación de Datos**.
2. Haga clic **Comprobar datos durante el proceso de copia**.
3. Haga clic en **Aceptar**.



Modificar las Propiedades de la Tarea

Puede modificar las opciones de una tarea seleccionándola y haciendo clic en **Modificar Propiedades** en el apartado **Administración Tareas**.



Modificar las Propiedades de la Tarea

1. Haga clic en las casillas para seleccionar las particiones, carpetas o archivos que desea copiar.

Al seleccionar un elemento de la ventana de la izquierda, su contenido se mostrará en la parte derecha para ayudarle a mejorar su selección.

2. Escriba un nombre para la tarea de copia, o aceptando el nombre por defecto.

El nombre por defecto se genera automáticamente al seleccionar los archivos o carpetas que desea copiar, pero puede modificarlo.

3. Haga clic en **Explorar** para seleccionar dónde desea guardar los datos en su archivo de copia.



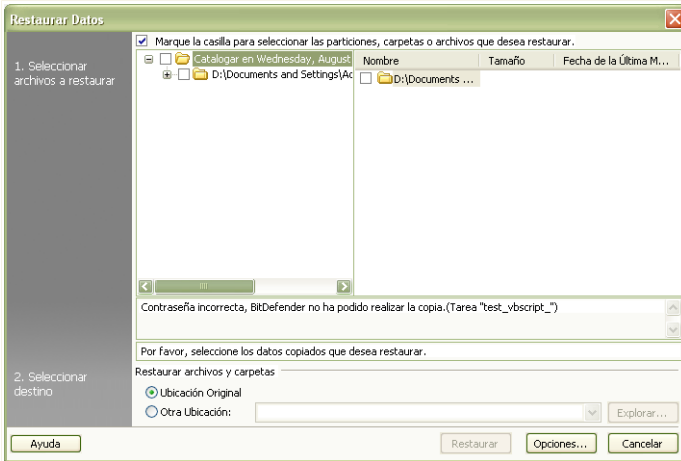
Nota

No olvide hacer clic en **Copiar** para iniciar el proceso, o en **Cancelar** para detenerlo. Para ajustar su configuración, haga clic en **Opciones**.



Restaurar un Archivo

Para restaurar sus datos, seleccione la tarea desde dónde quiere restaurar datos, haga clic en **Restaurar Archivo** en el menú **Restauración de Tareas** y siga estos pasos.



Restaurar un Archivo

1. Marque las casillas situadas junto a las particiones, carpetas, archivos que desea restaurar.

Cuando selecciona un elemento en la ventana de la izquierda, su contenido se mostrará en la parte derecha para ayudarle a mejorar su selección.

2. En la ventana **Seleccionar Ubicación de la Restauración** puede seleccionar la ubicación original de los datos o indicar una ubicación diferente.

Haga clic en **Explorar** para seleccionar dónde desea guardar los datos en su archivo de copia.



Nota

No olvide hacer clic en **Restaurar** para empezar o en **Cancelar** para cancelar la restauración.

Para ajustar su configuración, haga clic en **Opciones**.



Cuadro de Diálogo de Opciones de Restauración

Las opciones de restauración permiten indicar las acciones que realizará la Copia de Seguridad de BitDefender si los archivos a restaurarse ya existen en el destino, o modificar la fecha de modificación de cada archivo restaurado.

Cuando los archivos a restaurar ya existen

- **Omitir Archivos** BitDefender omitirá los respectivos archivos.
- **Preguntar al Usuario** BitDefender preguntará si desea reemplazar o no los archivos existentes.
- **Reemplazar Directamente** BitDefender reemplazará los archivos sin preguntar.
- **Reemplazar Antiguos** BitDefender reemplazará sólo los archivos antiguos. La antigüedad de los archivos se determina a partir de la fecha en la que fueron modificados por última vez.

Fecha de Modificación del Archivo

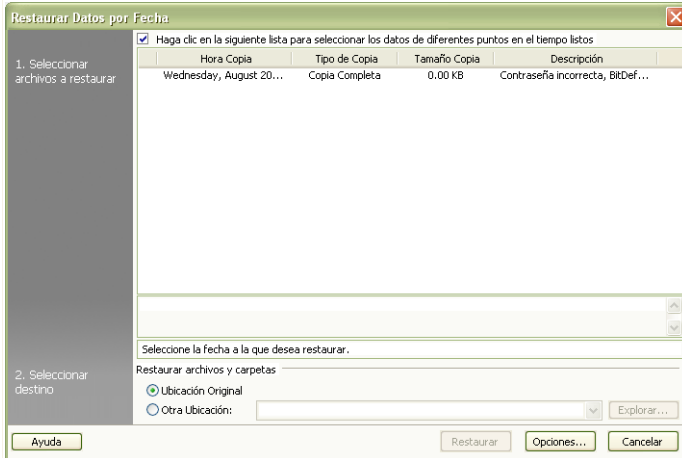
Si la opción está marcada, BitDefender cambiará la fecha de última modificación de los archivos y carpetas restaurados a la fecha actual. Sino, la fecha de modificación corresponderá a la del momento en que se hizo la copia de seguridad.

Estructura de Carpetas

Esta opción sólo se activa cuando decide realizar la restauración en una ubicación diferente a la original. Con esta opción conservará la estructura de carpetas de sus datos.

Restaurar Datos por Fecha

Para restaurar los datos copiados en un punto en el tiempo en concreto, seleccione la tarea desde la que desea restaurar los datos, haga clic en **Restaurar Datos por Fecha** en el menú **Tarea de Restauración** y a continuación siga estos 3 pasos.



Restaurar Datos por Fecha

1. Seleccione el archivo de copia de la fecha que desee. Se mostrará un comentario debajo del mismo.
2. En la ventana **Seleccionar Ubicación de la Restauración** puede seleccionar la ubicación original de los datos o indicar una ubicación diferente.

Haga clic en **Explorar** para seleccionar dónde desea guardar los datos en su archivo de copia.



Nota

No olvide hacer clic en **Restaurar** para empezar o en **Cancelar** para cancelar la restauración.

Para ajustar su configuración, haga clic en **Opciones**.

Cuadro de Diálogo de Opciones de Restauración

Las opciones de restauración permiten indicar las acciones que realizará la Copia de Seguridad de BitDefender si los archivos a restaurarse ya existen en el destino, o modificar la fecha de modificación de cada archivo restaurado.



Cuando los archivos a restaurar ya existen

- **Reemplazar Antiguos** BitDefender reemplazará sólo los archivos antiguos. La antigüedad de los archivos se determina a partir de la fecha en la que fueron modificados por última vez.

Fecha de Modificación del Archivo

Si la opción está marcada, BitDefender cambiará la fecha de última modificación de los archivos y carpetas restaurados a la fecha actual. Sino, la fecha de modificación corresponderá a la del momento en que se hizo la copia de seguridad.

Estructura de Carpetas

Esta opción sólo se activa cuando decide realizar la restauración en una ubicación diferente a la original. Con esta opción conservará la estructura de carpetas de sus datos.

Control de Tareas

Existen 3 maneras de monitorizar una tarea: pausar tarea, detener tarea y detener todo.

Pausar

Para pausar una tarea haga clic en el botón **Pausar Tarea** en el menú **Control de Tareas**.

Parar

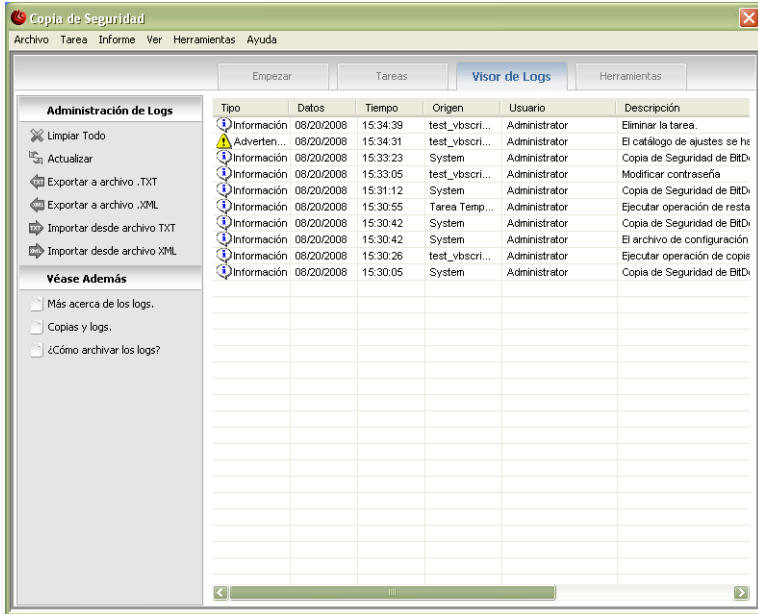
Para detener una tarea haga clic en el botón **Detener Tarea** en el menú **Control de Tareas**.

Parar Todo

Si hay más de una tarea ejecutándose, no hay necesidad de detenerlas una por una. Haga clic en el **Para Todo** en el menú **Control de Tareas**.

Visor de Logs

En este apartado se explica como ver, importar, exportar y limpiar logs. Los Logs sirven para recordar los datos que se ha copiado o restaurado, la fecha de realización y las posibles alertas o errores de la operación. Por ejemplo, si se produce un error durante una copia, BitDefender lo registra en forma de mensaje de advertencia.



Visor de Logs

Puede acceder al **Visor de Logs** siguiendo alguno de estos pasos:

- Haga clic en **Visor de Logs** en la **Barra de Navegación**.
- Haga clic en **Ver** en la **Barra de Menú** y seleccione **Visor de Logs**.
- Utilice el método abreviado pulsando **CTRL+Alt+L**.

Ver Logs

El visor de logs le permite analizar lo ocurrido durante la operación y encontrar la causa en caso de algún fallo o error.

Los logs de la Copia de Seguridad de BitDefender contienen los siguientes elementos:

Tipo

Los elementos de los logs se clasifican en según su gravedad. Existen 4 grados de gravedad en la Copia de Seguridad de BitDefender:



- **Fatal:** Se trata de un problema significativo que impide el correcto funcionamiento de la Copia de Seguridad de BitDefender. Por ejemplo, si el archivo de configuración de BitDefender Backup ha sido dañado.
- **Error:** Se trata de algún problema que provoca un fallo en la operación. Por ejemplo, si realiza una copia online pero no puede accederse al servidor.
- **Advertencia:** Se trata de un problema que no afecta a la operación, pero que más tarde podría clasificarse como un evento. Por ejemplo, un archivo que no ha podido leerse mientras se realizaba la copia.
- **Información** Describe una operación realizada con éxito. Por ejemplo, si se ha podido eliminar una tarea.

Fecha

La fecha en la que se ha producido el elemento del log.

Hora

La hora local en la que se ha producido el elemento del log.

Origen

El origen dónde se ha registrado el elemento, que puede ser una tarea o el programa Copia de Seguridad de BitDefender.

Usuario

El nombre del usuario en uso cuya acción ha sido registrada.

Descripción

Presenta el contenido en detalle del elemento registrado en el log.

Limpiar Logs

Puede limpiar los logs de la Copia de Seguridad de BitDefender de dos maneras: automáticamente y manualmente.



Importante

Una vez elimine las entradas del log, no podrán recuperarse. En consecuencia, es mejor exportar todos los logs a un archivo, y así poder consultarlos posteriormente.

Borrar Automáticamente

Cuando inicia Copia de Seguridad de BitDefender, éste compara el tamaño de los logs existentes con el tamaño predeterminado. BitDefender Backup eliminará automáticamente todos los logs que superen el tamaño predeterminado.



Nota

Para ver o modificar el tamaño predeterminado de los logs, siga estos pasos:

1. Haga clic en **Herramientas** en la **Barra de Menú**.



2. Haga clic en **Opciones** y seleccione **Informes y Logs**.
3. Introduzca la limitación de tamaño que desee (en MB) en el campo correspondiente. Cuando el tamaño del log alcance ese límite, la Copia de Seguridad de BitDefender borrará todos los logs.

Borrar Manualmente

Siga estos pasos para borrar los logs manualmente.

1. Haga clic en **Limpiar Todo** en el menú **Administración de Logs**.
2. Haga clic en **Aceptar** para exportar algunos logs antes de borrarlos, o haga clic en **No** si no desea conservar ningún log.

Importar y Exportar Logs

La Copia de Seguridad de BitDefender permite importar y exportar archivos en dos formatos: .TXT y .XML.



Nota

Recomendamos exportar y guardar los logs en un archivo antes de limpiarlos.

Para exportar los logs a un archivo, siga estos pasos:

1. Haga clic en **Exportar a TXT** o **Exportar a XML** en el menú **Administración de Logs**.
2. Introduzca el nombre del archivo y seleccione la ubicación donde desea guardarlo.
3. Haga clic en **Guardar**.

Para importar logs desde un archivo, siga estos pasos:

1. Haga clic en **Importar desde archivo TXT** o **Importar desde archivo XML** en el menú **Administración de Logs**.
2. Busque su archivo.
3. Haga clic en **Abrir**.



Nota

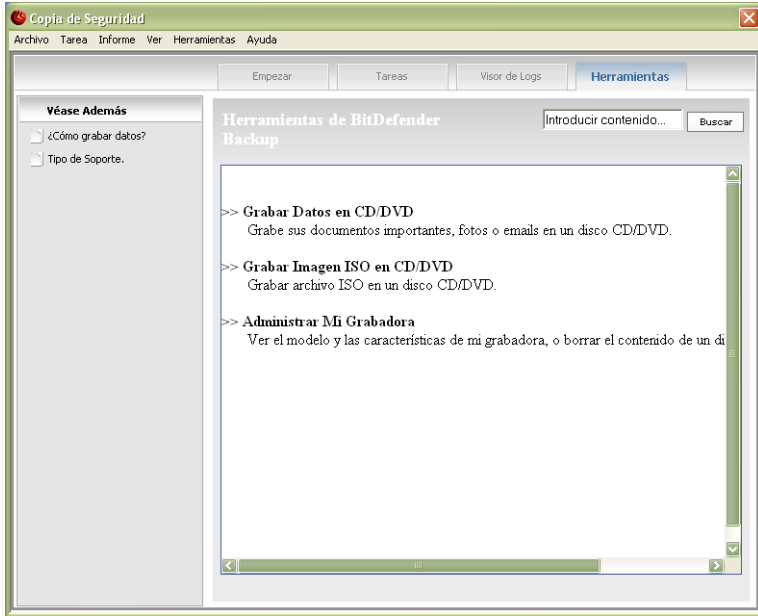
Haga clic en el botón **Actualizar** en el menú **Administración de Logs** para asegurarse que visualiza los últimos informes generados.

Herramientas

Este apartado muestra cómo usar la Copia de Seguridad de BitDefender para grabar datos en un CD/DVD o para grabar un archivo de Imagen ISO. Se incluyen temas



como la grabación de CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL y la conservación de los datos copiados offline.



Herramientas

Puede ver la **Herramientas** siguiendo cualquiera de estos pasos:

- Haga clic en **Herramientas** en la **Barra de Navegación**.
- Haga clic en el menú **Ver** de la **Barra de Menú** y seleccione **Herramientas**.
- Utilice el método abreviado pulsando **CTRL+Alt+T**.

Grabar a CD/DVD

Para grabar un CD/DVD manualmente, siga estos pasos:

1. Haga clic en **Copiar datos en CD/DVD**.
2. Haga clic en **Borrar** si desea reutilizar un disco regrabable. Si desea borrarlo rápidamente, haga clic en **Rápido**. Si necesita borrar la información de la pista completamente, haga clic en **Completo**, pero esta opción llevará más tiempo.



3. Haga clic en **Grabar con Diálogo**.

Desde aquí podrá elegir si desea expulsar el disco tras la grabación, finalizar el disco o grabar datos con el sistema de archivos Joliet.

4. Haga clic en **Archivo** o **Carpeta** en el cuadro de diálogo para añadir los datos que desee grabar.

5. Después de añadir los datos, seleccione la grabadora e introduzca el nombre que desea darle al disco. A continuación haga clic en **Grabar**.

Grabar Imagen ISO en un CD/DVD

Para grabar una imagen ISO en CD/DVD, siga estos pasos:

1. Haga clic en **Grabar Imagen ISO en CD/DVD**.

2. Haga clic en **Borrar** si desea reutilizar un disco regrabable. Si desea borrarlo rápidamente, haga clic en **Rápido**. Si necesita borrar la información de la pista completamente, haga clic en **Completo**, pero esta opción llevará más tiempo.

3. Haga clic en **Grabar con Diálogo**.

Desde aquí podrá seleccionar diferentes opciones: expulsar el disco tras la grabación, finalizar el disco (si desea compartir el disco con otros) o grabar los datos usando el sistema de archivo Joliet.

4. Haga clic en **Añadir**.

5. Seleccione una imagen ISO para grabar y haga clic en **Abrir**.

6. Haga clic en **Grabar**.

Administrar Mi Grabadora

Le ayudará a gestionar y a ver los dispositivos de grabación y medios del equipo. Contiene los siguientes enlaces:

- **Expulsar Dispositivo** Expulsa el dispositivo de grabación seleccionado.
- **Cerrar Dispositivo** Cierra el dispositivo de grabación seleccionado.
- **Info del Contenido** Le permite ver el contenido del medio de grabación seleccionado.
- **Info del Dispositivo** Permite ver información del dispositivo de grabación.
- **Características** Permite ver las características de los medios de grabación.
- **Borrar Contenido** Borra el contenido del disco.



21. Cifrado

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

21.1. Cifrado de Mensajería Instantánea (IM)

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

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



Importante

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

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



Nota

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



The screenshot shows the BitDefender Total Security 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, the "Cifrado de IM" (IM Encryption) settings are displayed. The "Blindaje" (Shield) tab is active. The "Cifrado de IM desactivado" (IM Encryption disabled) section has a checked checkbox. Below it, two sub-sections are visible: "Cifrado de Yahoo Messenger desactivado" and "Cifrado de Windows Live (MSN) Messenger desactivado", both with checked checkboxes. The "Exclusiones del Cifrado" (IM Encryption Exclusions) section contains an empty table with columns "ID de usuario" and "Programa de IM". Below this is the "Conexiones Actuales" (Current Connections) section, which contains a table with columns "ID de usuario", "Programa de IM", and "Estado del Cifrado". At the bottom of the interface, there is a 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.

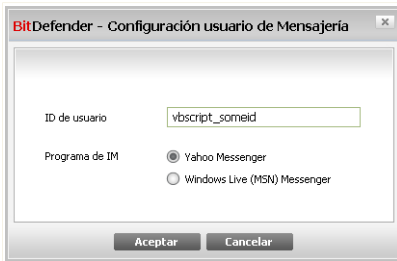


- Su contacto no tiene instalada ninguna versión de BitDefender que soporte el cifrado de IM.

21.1.1. Desactivando el Cifrado para Usuarios Específicos

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

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



Añadiendo Contactos

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

21.2. Blindaje de Archivos

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

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

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



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

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Cifrado de IM **Blindaje**

General
Antivirus
Antispam
Control Parental
Control de Privacidad
Cortafuego
Vulnerabilidad
Copia Seguridad

Cifrado
Optimizador
Modo Juego/Portátil
Red
Actualizar
Registro

Blindaje de Archivos activado

Blindajes en este equipo

Blindaje	Estado	Letra Unidad	Ruta Completa
miki	Bloq...		D:\Documents and Settings\Administrator\my documents\miki.bvd

Contenido del Blindaje

Ruta Completa	Tipo de Archivo
---------------	-----------------

Esta es una lista de los blindajes que se han encontrado en su equipo. Para buscar más blindajes, haga clic en el icono de la lupa situado en la esquina derecha. Haga clic derecho en los elementos para ver más opciones.

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

Blindaje de Archivos

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

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

21.2.1. Creando un Blindaje

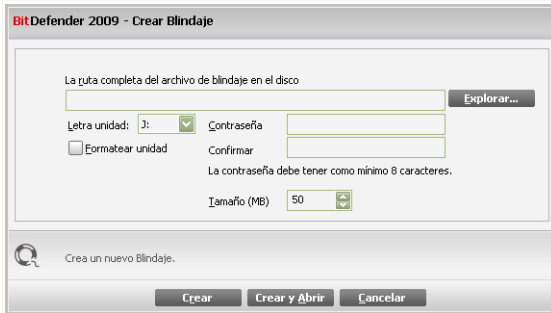
Para crear un nuevo blindaje, siga cualquiera de estos métodos:

- Haga clic en **Crear Blindaje**.



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

Aparecerá una nueva ventana.



Creación del Blindaje de Archivos

Siga estos pasos:


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



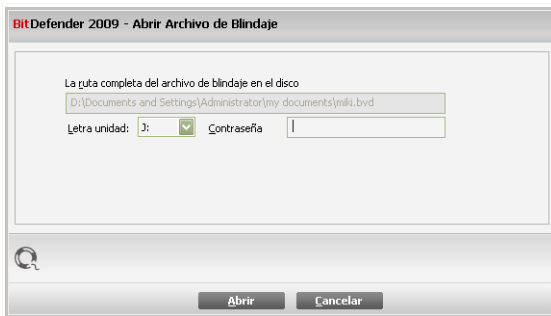
21.2.2. Abriendo un Blindaje

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

Para abrir un blindaje, use cualquiera de estos métodos:

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

Aparecerá una nueva ventana.



Abrir Blindaje de Archivos

Siga estos pasos:

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

21.2.3. Bloqueando un Blindaje

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

Para bloquear un blindaje, use cualquiera de estos métodos:



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

21.2.4. Cambiando la Contraseña del Blindaje

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

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

Aparecerá una nueva ventana.

BitDefender 2009 - Cambiar Contraseña

Cambia la contraseña existente del blindaje de archivos
D:\Documents and Settings\Administrator\my ...\miki.bvd

Contraseña Antigua

Nueva Contraseña

Confirmar Nueva Contraseña

La contraseña debe tener como mínimo 8 caracteres.

Aceptar Cancelar

Cambiar Contraseña del Blindaje

Siga estos pasos:

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



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



Nota

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

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

21.2.5. Añadiendo Archivos a un Blindaje

Para añadir archivos a un blindaje, siga estos pasos:

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



Nota

No puede añadir archivos ni aplicaciones del sistema al blindaje.

21.2.6. Eliminando Archivos de un Blindaje

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

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



Nota

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



Importante

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

22.1.1. 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

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

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

How do you prefer to solve this issue?

Force user to change password at next logon

Change the password yourself now

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
Yahoo! Messenger	8.1.0.421	8.1.0.241	Actualizado
Firefox	2.0.0.16 (en-US)	3.0 (en-US)	Página de Inicio

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

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

- Microsoft GDI+ Detection Tool (KB873374)
- Windows Genuine Advantage Validation Tool (KB892130)
- Windows Internet Explorer 7 For Windows XP
- Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB936181)
- Windows XP Service Pack 3 (KB936929)
- 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)
- Security Update for Windows XP (KB946648)
- Security Update for Windows XP (KB952954)
- Cumulative Security Update for Internet Explorer 6 for Windows XP (KB953838)
- Security Update for Windows XP (KB950974)
- Update for Windows XP (KB951072)
- Update for Windows XP (KB952287)

Buscar Actualizaciones Opcionales de Windows

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

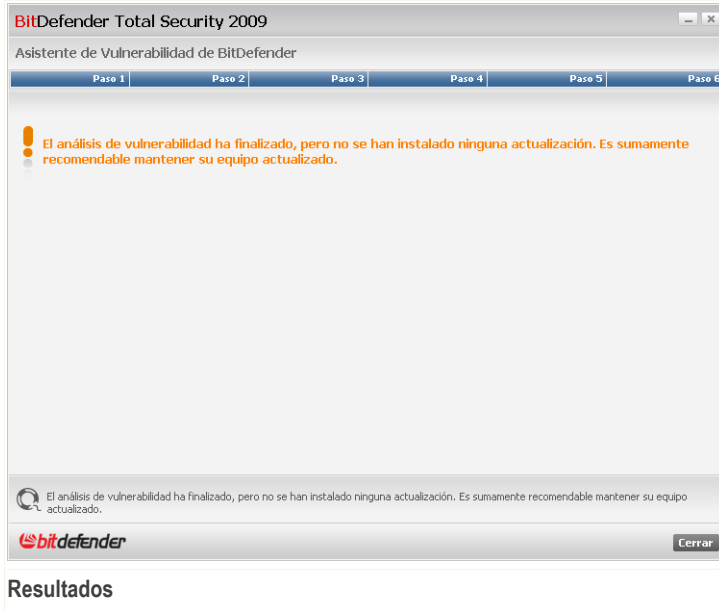
Actualizaciones de Windows

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**.



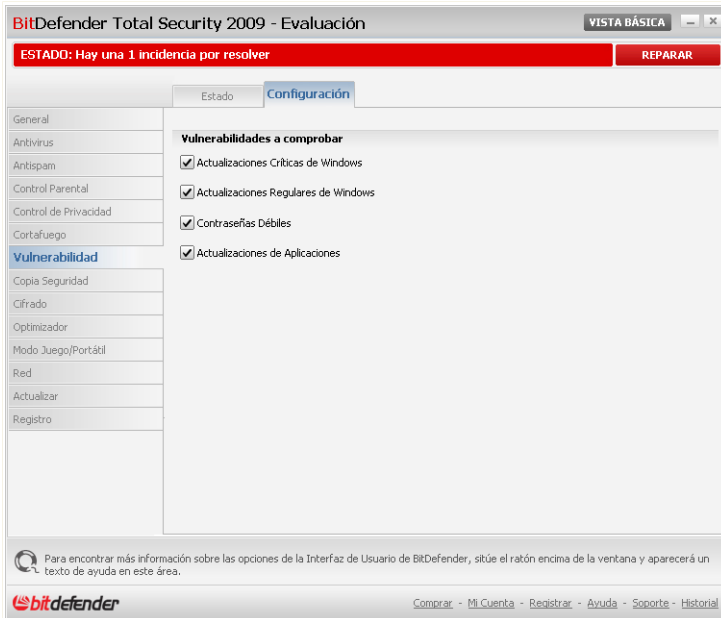
Paso 6/6 – Ver Resultados



Haga clic en **Cerrar**.

22.2. 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.



23. Optimizador

BitDefender incluye un módulo Optimizador que le ayudará a mantener la integridad de su sistema. Las herramientas de mantenimiento que se ofrecen son muy importantes para mejorar el rendimiento de su sistema y administrar eficientemente el espacio de los discos duros.

Para realizar operaciones de mantenimiento en su PC, diríjase al apartado **Optimizador** y utilice las herramientas incluidas.

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Optimizador

General

Antivirus

Antispam

Control Parental

Control de Privacidad

CortaFuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Desfragmentador del PC
Última Ejecución: Nunca Ejecutar

Limpiador del PC
Última Ejecución: Wednesday, August 20, 2008 4:28 PM Ejecutar

Destructor de Archivos
Ejecutar

Limpiador del Registro
Última Ejecución: Wednesday, August 20, 2008 4:27 PM Ejecutar

Recuperador del Registro
Ejecutar

Buscador de Duplicados
Última Ejecución: Wednesday, August 20, 2008 4:29 PM Ejecutar

Haga clic aquí para acceder a los componentes del Optimizador y ejecutarlos.

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

Optimizador

BitDefender incluye las siguientes herramientas de limpieza del PC:

- El **Desfragmentador del PC** reorganiza físicamente los datos del disco duro para que los fragmentos que componen cada archivo se almacenen juntos.



- El **Limpiador del PC** elimina los archivos temporales de Internet y cookies, archivos de sistema que no se utilizan y accesos directos a los documentos recientes.
- El **Destruccion de Archivos** elimina los archivos de forma permanente y sus rastros en el sistema. Utilice el Destruccion de Archivos para eliminar archivos en su sistema y asegurarse que nunca puedan recuperarse.
- El **Limpiador del Registro** identifica y elimina las referencias inválidas o huérfanas del Registro de Windows. Para mantener el Registro de Windows limpio y optimizado, recomendamos ejecutar el Limpiador del Registro mensualmente.
- El **Recuperador del Registro** puede restaurar las claves del registro que han sido eliminadas previamente en su equipo por el Limpiador del Registro de BitDefender.
- El **Buscador de Duplicados** busca y elimina aquellos archivos duplicados en su sistema.

Para utilizar cualquiera de estas herramientas, haga clic en el botón **Ejecutar** correspondiente y siga los pasos del asistente.

23.1. Desfragmentando los Discos Duros

Cuando copia un archivo con un tamaño superior al bloque de espacio libre más grande, se produce una fragmentación del archivo. Al no existir el espacio suficiente para almacenar el archivo de forma íntegra, éste se fragmenta en varios bloques. Cuando accede al archivo fragmentado, los datos se leen desde las diferentes ubicaciones donde se encuentran los bloques que forman el archivo.

La fragmentación de los archivos reduce la velocidad de acceso al archivo, disminuye el rendimiento del sistema y acelera el desgaste del disco duro.

Para reducir la fragmentación de los archivos debe desfragmentar los discos periódicamente. La desfragmentación reorganiza físicamente los datos del disco duro, ordenando los fragmentos de los archivos uno detrás de otro. También crea espacios de espacio disco para prevenir la desfragmentación de nuevos archivos.

Se recomienda desfragmentar el disco duro para:

- acceder a los archivos con más rapidez.
- mejorar el rendimiento global del equipo.
- prolongar la vida del disco duro.

Para desfragmentar el disco duro, siga estos pasos:



1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Desfragmentador del PC.
3. Siga el proceso guiado de tres pasos para completar el proceso.



Nota

La desfragmentación del disco puede llevar un tiempo, dado que implica mover porciones de datos almacenados de un sitio a otro. Recomendamos realizar la desfragmentación cuando no esté utilizando el ordenador.

23.1.1. Paso 1/3 - Analizando...

El Desfragmentador de Disco analizará el disco duro para determinar si es necesaria o no la desfragmentación.

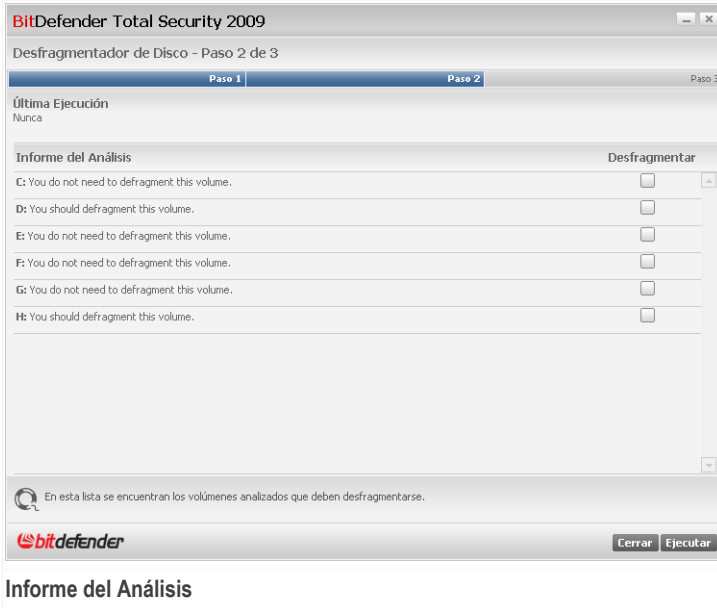


Espere a que el Desfragmentador de Disco finalice el análisis. Si desea cancelar la operación, haga clic en **Cancelar**.



23.1.2. Paso 2/3 - Ver Informe del Análisis

Una vez se ha completado el análisis, aparecerá una nueva ventana dónde podrá ver los resultados e iniciar la desfragmentación del disco, en caso necesario.



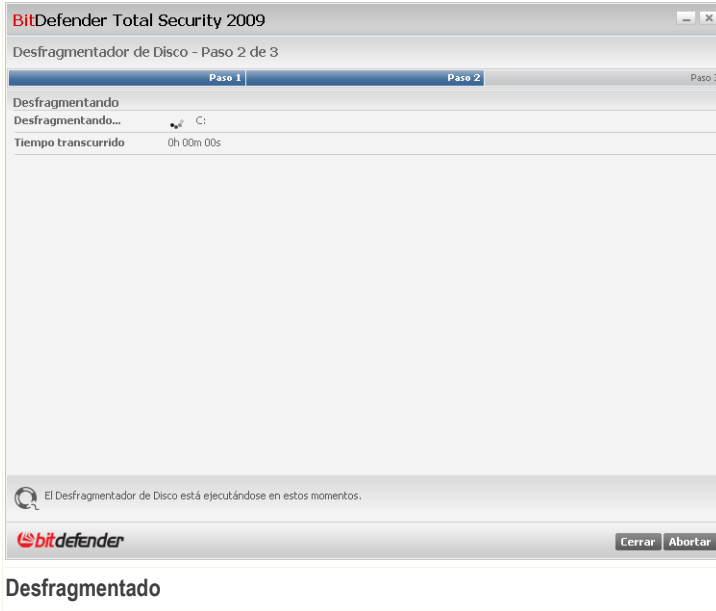
Compruebe el informe de análisis.

Si ningún volumen de disco necesita desfragmentación, haga clic en **Cerrar** para cerrar la ventana. De lo contrario, seleccione la opción **Desfragmentar** correspondiente al volumen de disco que necesita desfragmentación y haga clic en **Ejecutar** para iniciar la desfragmentación.



Nota

El Desfragmentador de Disco necesitará un 15% de espacio libre en el disco para poder funcionar correctamente. Si no hay espacio suficiente en el disco, la desfragmentación se cancelará.



Espere a que la desfragmentación del disco finalice. Puede cancelar la desfragmentación del disco en cualquier momento haciendo clic en **Abortar**.

23.1.3. Paso 3/3 - Ver Informe de la Desfragmentación

Una vez se complete la desfragmentación del disco, aparecerá una nueva ventana dónde podrá ver las estadísticas de la desfragmentación.



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

23.2. Limpiando su PC

Cada vez que visita una página web se almacenan archivos temporales de Internet que permiten visualizar la página más rápidamente durante la próxima visita. A pesar de tratarse de archivos temporales, éstos no se eliminan después de cerrar el navegador. Esto podría considerarse como un fallo de privacidad, ya que cualquier persona que acceda a su ordenador podría ver estos archivos. Con el tiempo, estos archivos acaban ocupando un espacio considerable en su disco y consumen espacio libre.

Las cookies también se almacenan en su ordenador cuando visita una página web. Las cookies son pequeños archivos que contienen información sobre sus preferencias de navegación. También pueden suponer un problema de privacidad, ya que pueden analizarse por los anunciantes para determinar sus intereses y preferencias al navegar.

El Limpiador del PC le ayuda a liberar espacio en su disco y proteger su privacidad, al eliminar aquellos archivos que han dejado de ser útiles.



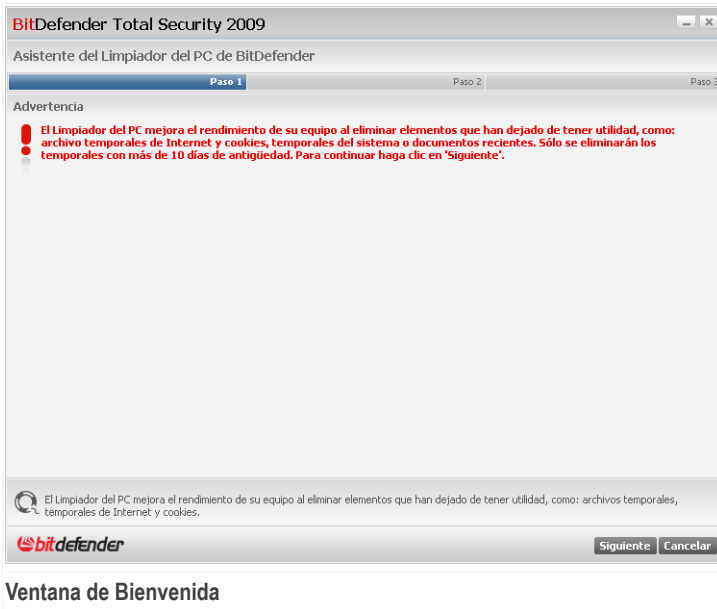
- archivos temporales de Internet y cookies de Internet Explorer.
- archivos temporales de Internet y cookies de Mozilla Firefox.
- archivos temporales del sistema creados por Windows durante sus operaciones.
- accesos directos a los documentos recientes creados por Windows cuando abre un archivo.

Para limpiar los archivos temporales de Internet y cookies, archivos temporales del sistema y accesos directos a los documentos recientes, siga estos pasos:

1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Limpiador del PC.
3. Siga el proceso guiado de tres pasos para completar el proceso.

23.2.1. Paso 1/3 – Iniciar Eliminación

Desde aquí puede iniciar la limpieza de sus archivos temporales de Internet y cookies.

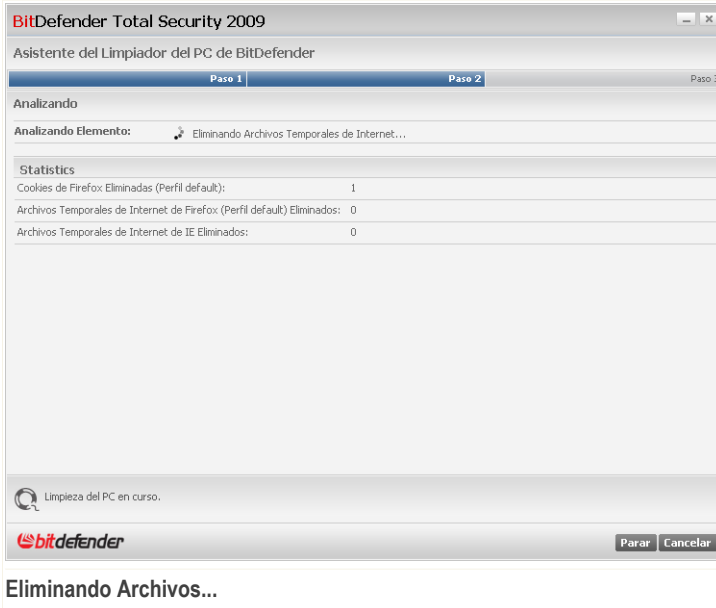




Haga clic en **Siguiente**.

23.2.2. Paso 2/3 - Eliminando Archivos...

El limpiador empezará a eliminar los archivos temporales de Internet y cookies.



Espere a que el Limpiador finalice la limpieza de los archivos temporales de Internet y las cookies. Si desea cancelar la operación, haga clic en **Cancelar**.

23.2.3. Paso 3/3 - Ver Resumen de Resultados

Una vez finalice la limpieza de los archivos, aparecerá una nueva ventana dónde podrá ver los resultados.



Puede ver las estadísticas de los objetos eliminados.

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

23.3. Eliminando Archivos de Forma Permanente

Cuando elimina un archivo, ya no podrá volver acceder al mismo como lo hacía habitualmente. Sin embargo, el archivo continúa estando almacenado en su disco hasta que no se sobrescriba al copiar archivos nuevos.

Incluso cuando elimina un archivo, éste puede recuperarse utilizando programas especializados. Esto podría representar una amenaza para su privacidad si alguien intenta obtener sus datos privados.

Para impedir la recuperación de datos confidenciales después de eliminarlos, puede utilizar BitDefender. BitDefender eliminará de forma permanente estos datos, al suprimirlos físicamente del disco duro.

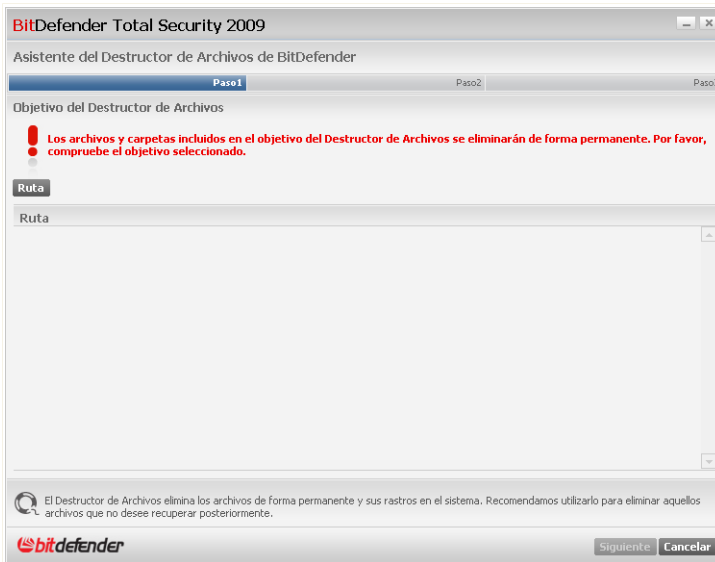
Para eliminar archivos de forma permanente, siga estos pasos:



1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Destructor de Archivos.
3. Siga el proceso guiado de tres pasos para completar el proceso.

23.3.1. Paso 1/3 - Seleccionar Objetivo

Aquí puede especificar los archivos y carpetas que se eliminarán de forma permanente.



Objetivo

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



Nota

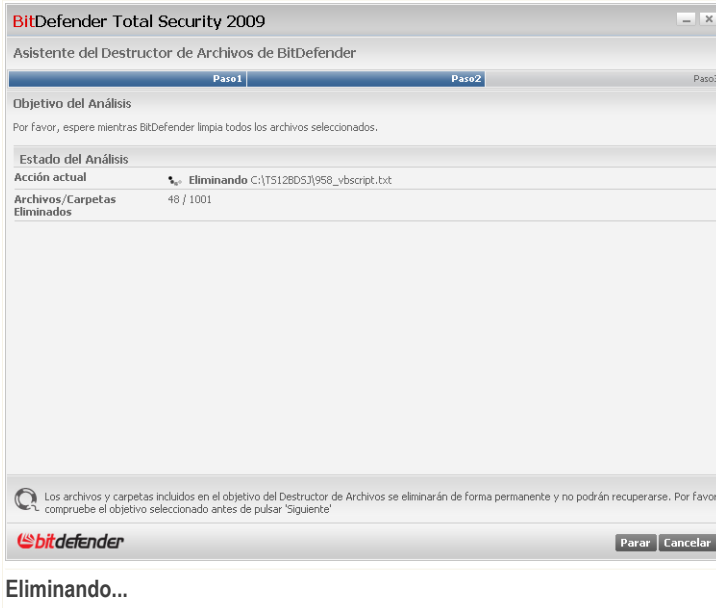
Puede seleccionar una o varias ubicaciones.



Haga clic en **Siguiente**.

23.3.2. Paso 2/3 - Eliminando Archivos...

BitDefender eliminará de forma permanente los archivos de las ubicaciones indicadas.



Espera a que la operación de destrucción de archivos se complete. Si desea cancelar la operación, haga clic en **Cancelar**.

23.3.3. Paso 3/3 - Ver Resumen de Resultados

Una vez se hayan eliminado los archivos, aparecerá una nueva ventana donde podrá ver los resultados.



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

23.4. Limpiando el Registro de Windows

El Registro de Windows es una parte importante de los sistemas operativos Windows. Se trata de una base de datos que contiene información y configuración del hardware y aplicaciones instaladas, usuarios, preferencias de su equipo, entre otra información

Muchas aplicaciones escriben claves en el Registro de Windows cuando se instalan. Pero al desinstalarse, algunas de las claves asociadas no pueden eliminarse y permanecen en el Registro de Windows, ralentizando su ordenador o incluso causando fallos de estabilidad. Lo mismo ocurre cuando elimina accesos directos a determinados archivos, o si existen controladores corruptos.

Utilice el Limpiador del Registro para limpiar el Registro de Windows y mejorar el rendimiento de su sistema. El Limpiador del Registro analiza el Registro de Windows y elimina las claves inválidas.

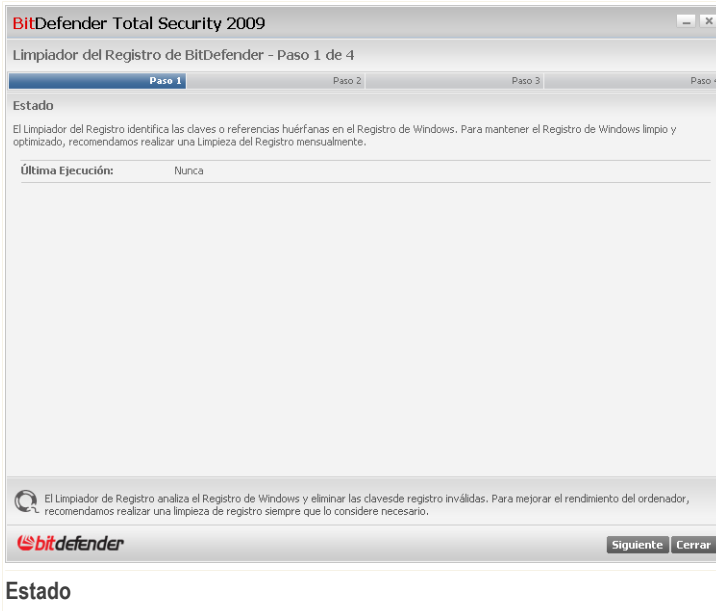
Para crear limpiar el Registro de Windows, siga estos pasos:



1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Limpiador del Registro.
3. Deberá completar un asistente guiado de cuatro pasos.

23.4.1. Paso 1/4 - Iniciar Análisis

Desde aquí puede iniciar el análisis del Registro.

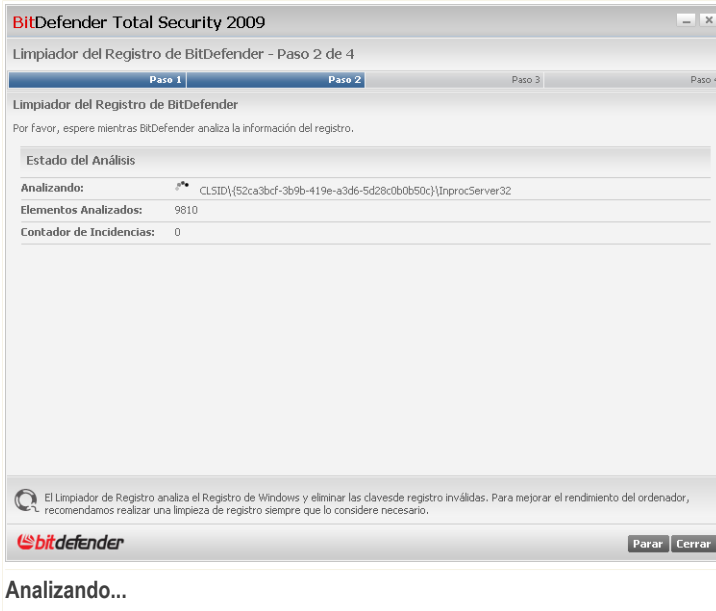


Puede ver cuándo se inició el Limpiador del Registro por última vez y las recomendaciones de BitDefender.

Haga clic en **Siguiente**.

23.4.2. Paso 2/4 - Analizando...

El Limpiador del Registro iniciará el análisis del registro.



Analizando...

Puede ver la última clave del registro analizada y estadísticas relacionadas con el análisis.

Espere a que el Registro de Windows finalice el análisis de claves. Si desea cancelar la operación, haga clic en **Cancelar**.



Nota

Si desea detener el análisis, haga clic en **Parar**. El asistente saltará al siguiente paso.

23.4.3. Paso 3/4 – Seleccione la acción

Una vez finalice el análisis de claves del registro, aparecerá una nueva ventana dónde podrá ver los resultados



Nota

Si no se ha detectado ninguna incidencia o ha decidido detener el análisis, se omitirá este paso del asistente.



BitDefender Total Security 2009

Limpiador del Registro de BitDefender - Paso 3 de 4

Paso 1 Paso 2 Paso 3 Paso 4

Acción General

Elija la acción que se debe aplicar a estas claves. Puede configurar la acción general o la acción para cada clave.

Seleccionar categoría Todas las Categorías ▾

Eliminar todas las claves (esta acción sobrescribirá la acción seleccionada en cada clave)

Acción por Clave

<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{3C4F38E7-47EB-101B-A3C9-08002B2F49FB}\InprocServer32
	Valor de la Clave: Nombre del valor:(Por defecto)
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{C27CE3C-8596-11D1-B16A-00C0F0283628}\InprocServer32
	Valor de la Clave: Nombre del valor:(Por defecto)
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{DFC09BAE-8185-31F2-AC1C-C4E437101217}\InprocServer32
	Valor de la Clave: Nombre del valor:CodeBase
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\CLSID>{DFC09BAE-8185-31F2-AC1C-C4E437101217}\InprocServer32\4.2.8.2
	Valor de la Clave: Nombre del valor:CodeBase
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls
<input checked="" type="checkbox"/>	Nombre de la Clave: HKCR\Installer\Products\0E23E40C6140D434FA9B96967D309AFE\SourceList
	Valor de la Clave: Nombre del valor>LastUsedSource
	El riesgo de eliminar este elemento: baja Categoría: Custom Controls

El Limpiador de Registro analiza el Registro de Windows y eliminar las claves de registro inválidas. Para mejorar el rendimiento del ordenador, recomendamos realizar una limpieza de registro siempre que lo considere necesario.

Siguiente Cerrar

Acciones

Podrá ver todas las claves del registro inválidas o huérfanas detectadas. Se le mostrará información detallada sobre cada clave (nombre, valor, prioridad, categoría).

Las claves del registro están agrupadas en función de su ubicación en el Registro de Windows.

Categoría	Descripción
Ubicaciones del Software	Claves del registro que contienen información sobre la ruta en la que están instaladas las aplicaciones de su equipo. Las claves inválidas tienen asignada una prioridad baja, lo cual significa que puede eliminarlas sin apenas riesgo alguno.
Controles Personalizados	Claves del registro que contienen información sobre las extensiones registradas en su equipo. Estas claves normalmente se utilizan para mantener las asociaciones de los archivos (para asegurarse que se inicia la



Categoría	Descripción
	<p>aplicación correcta al abrir un archivo desde el Explorador de Windows). Por ejemplo, una clave de este tipo le permitiría abrir un archivo .doc con Microsoft Word.</p> <p>Las claves inválidas tienen asignada una prioridad baja, lo cual significa que puede eliminarlas sin apenas riesgo alguno.</p>
DLLs Compartidas	<p>Claves del registro que contienen información sobre la ubicación de DLLs compartidas (Librerías de Conexión Dinámica). Las DLLs contienen funciones que las aplicaciones utilizan para realizar algunas tareas. Algunas DLLs se comparten para reducir los requisitos de espacio y memoria.</p> <p>Estas claves del registro dejan de ser válidas cuando la DLL a la que apuntan cambia de ubicación o se elimina (por ejemplo, al desinstalar un programa).</p> <p>Las claves del registro inválidas tienen asignadas una prioridad media, lo cual significa que eliminarlas puede afectar de forma negativa al sistema.</p>

Para realizar el proceso de limpieza de una forma más sencilla, seleccione una categoría del menú.

Puede elegir entre eliminar todas las categorías o sólo determinadas claves inválidas dentro de la categoría seleccionada. Si marca **Eliminar todas las claves**, todas las claves detectadas serán eliminadas. Si desea eliminar únicamente unas claves específicas, marque la opción **Eliminar** situada junto a la respectiva clave.



Nota

Por defecto, se eliminarán todas las claves inválidas detectadas.

Haga clic en **Siguiente**.

23.4.4. Paso 4/4 - Ver Resumen de Resultados

Aquí puede ver los resultados del análisis realizado por el Limpiador del Registro.



BitDefender Total Security 2009

Limpiador del Registro de BitDefender - Paso 4 de 4

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

Resumen de los Resultados

Debajo puede ver los resultados de la Limpieza del Registro.

Incidencias detectadas:	47
Claves eliminadas:	47
Claves omitidas:	0

Este es el resumen del proceso de limpieza del registro. Aquí puede ver el número de incidencias detectadas y el número de claves eliminadas o ignoradas.

Finalizar

Resumen de Resultados

Si ha decidido no eliminar todas las claves del registro, aparecerá una advertencia. Recomendamos revisar las incidencias correspondientes.

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

23.5. Recuperando Claves Eliminadas

En algunas ocasiones, después de la limpieza del registro, puede notar que su sistema no funciona correctamente o que algunas aplicaciones fallan a causa de claves registro que han sido eliminadas. Para solucionar el problema, debe recuperar las claves del registro eliminadas.

Para recuperar las claves del registro eliminadas, siga estos pasos:

1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Recuperador del Registro.
3. Debe completar un asistente guiado de dos pasos.



Importante

Sólo los usuarios con permisos de administrador pueden recuperar las claves eliminadas.

23.5.1. Paso 1/2 - Iniciar Recuperador del Registro

Desde aquí puede iniciar la recuperación del registro.

BitDefender Total Security 2009

Recuperador del Registro - Paso 1 de 2

Paso 1

Estado

Última Ejecución: Wednesday, August 20, 2008 4:27 PM

Puntos de Recuperación

⚠ Antes de ejecutar el Asistente de Recuperación del Registro, tenga en cuenta que esta operación puede sobrescribir las claves el registro editadas desde la última Limpieza del Registro.

Por favor, seleccione la fecha en la que realizó la limpieza del registro para poder volver a este punto de restauración.

Wednesday, August 20, 2008 4:27 PM

El Recuperador del Registro permite restaurar las entradas que han sido eliminadas previamente en su equipo por el Limpiador del Registro de BitDefender.

bitdefender

Siguiente Cancelar

Estado

Podrá ver una lista de puntos en el tiempo en los que se realizó una Limpieza del Registro. Seleccione el punto en el tiempo sobre el que desea realizar la Recuperación del Registro.

Si está seguro que desea recuperar las claves eliminadas en ese momento, haga clic **Siguiente**.



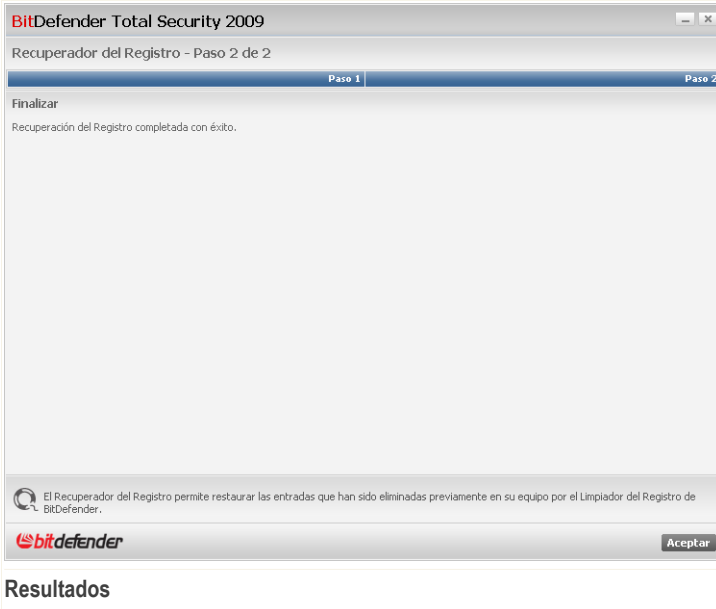
Aviso

La recuperación de las claves eliminadas puede suponer sobrescribir las claves editadas desde la última vez que realizó la limpieza.



23.5.2. Paso 2/2 - Ver Resultados

Aquí puede ver si la recuperación se ha realizado con éxito.



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

23.6. Buscar Duplicados

Los archivos duplicados consumen espacio en el disco duro. Piense qué ocurriría si tuviera el mismo archivo .mp3 almacenado en tres carpetas diferentes.

Para detectar y eliminar los archivos duplicados en su equipo puede utilizar el Buscador de Duplicados. De este modo conseguirá más espacio libre en sus discos duros.

Para buscar los archivos duplicados en su equipo, siga estos pasos:

1. En la Vista Avanzada, haga clic en el apartado **Optimizador** del menú de la izquierda.
2. Haga clic en el botón **Ejecutar** correspondiente al Buscador de Duplicados.



3. Deberá completar un asistente guiado de cuatro pasos.

23.6.1. Paso 1/4 – Seleccione el Objetivo de Búsqueda

Aquí puede indicar dónde buscar los archivos duplicados.



Haga clic en **Ruta** y seleccione la ubicación en la que el Buscador de Duplicados deberá buscar archivos duplicados. La rutas de los elementos seleccionados aparecerá en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento.



Nota

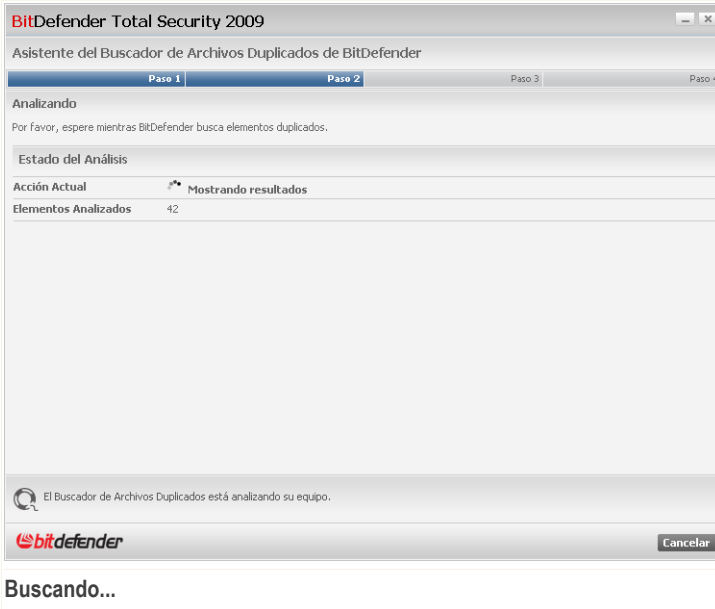
Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiente**.



23.6.2. Paso 2/4 - Buscando...

El Buscador de Duplicados iniciará la búsqueda de archivos duplicados.



Puede ver el estado de la búsqueda y las estadísticas.

Espere a que el Buscador de Duplicados complete la búsqueda. Si desea cancelar la operación, haga clic en **Cancelar**.

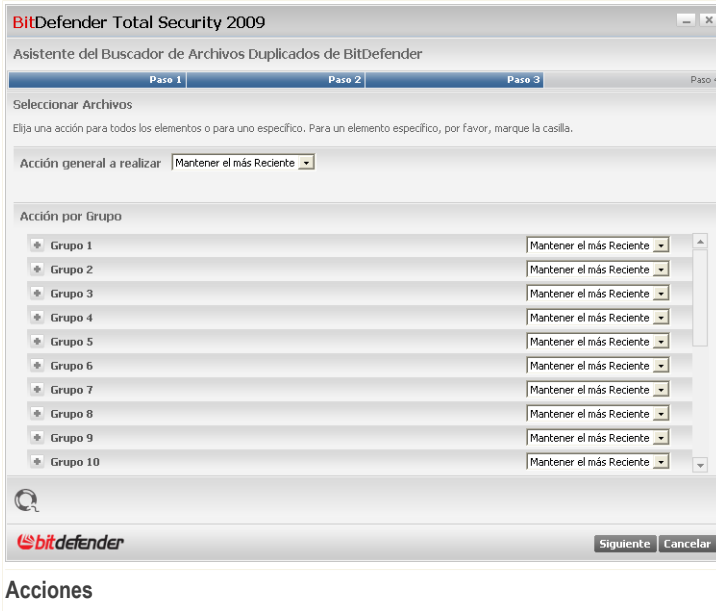
23.6.3. Paso 3/4 – Seleccione la acción

Una vez finalice la búsqueda, aparecerá una nueva ventana dónde podrá indicar las acciones a realizar con los archivos duplicados detectados.




Nota

Si no se encuentran archivos duplicados, puede saltarse este paso.



Acciones

Los archivos duplicados detectados están organizados en grupos. Si hace clic en el botón  situado junto a un grupo, verá información sobre los archivos duplicados (ruta completa, tamaño, fecha de creación y modificación).

Puede seleccionar una acción global que se aplicará a todos los archivos duplicados que se detecten, pero también puede seleccionar una acción para cada uno de los grupos. Dispone de las siguientes opciones en el menú:

Acción	Descripción
Guardar los más nuevos	Los archivos duplicados más recientes se mantendrán, mientras que los otros archivos duplicados se eliminarán.
Guardar los más antiguos	Los archivos duplicados de mayor antigüedad se mantendrán, mientras que los otros archivos duplicados se eliminarán.
Ninguna acción	No se aplicará ninguna acción sobre los archivos duplicados.



Si desea aplicar una acción global a todos los objetos del grupo, seleccione la acción deseada desde el menú correspondiente. Si sólo quiere eliminar algunos de los archivos del grupo, marque la casilla **Eliminar** cercana a cada uno de los archivos a eliminar.



Nota

La acción global no sobrescribirá la acción que ha elegido para algunos archivos o grupos en concreto. Por ejemplo, si selecciona **Guardar los más nuevos** como acción global, pero modifica la acción de un archivo o grupo, se aplicará la acción global a todos los archivos excepto en los que haya seleccionado una acción particular.

Haga clic en **Siguiente**.

23.6.4. Paso 4/4 - Ver Resumen de Resultados

Aquí podrá ver los resultados del análisis del Buscador de Duplicados.

The screenshot shows the 'Asistente del Buscador de Archivos Duplicados de BitDefender' window. It has a progress bar with four steps: Paso 1, Paso 2, Paso 3, and Paso 4 (selected). The main content area is titled 'Resumen de los Resultados' and contains the following text: 'No se ha eliminado ningún archivo. Abajo puede ver las estadísticas de esta tarea de buscador de duplicados. Puede ejecutar el asistente en cualquier momento desde el apartado Optimizador, Panel de tareas'.

Elementos analizados	2
Grupos de Archivos Duplicados	1
Archivos Duplicados	2

At the bottom of the window, there is a footer with the BitDefender logo and two buttons: 'Ejecutar de nuevo' and 'Cerrar'.

Resumen de Resultados

Haga clic en **Repetic** para iniciar una nueva búsqueda de archivos duplicados, o pulse **Aceptar** para cerrar la ventana.



24. Modo Juego / Portátil

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

- El **Modo Juego** 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.

24.1. Modo Juego

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

- Todas las alertas y ventanas emergentes de BitDefender quedan desactivadas.
- El nivel de protección en tiempo real de BitDefender queda fijado a **Permisivo**.
- El Cortafuego de BitDefender está configurado en modo **Permitir Todo**. Esto significa que todas las conexiones nuevas (tanto entrantes como salientes) se aceptarán de forma automática, independientemente del puerto y protocolo que utilicen.
- Por defecto, no se realizarán actualizaciones.



Nota

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

- Las tareas de análisis programadas se desactivarán de forma predeterminada.
- Las tareas de copia programadas están desactivadas de forma predeterminada.

Por defecto, BitDefender activa automáticamente el Modo Juego 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 Juego usando la combinación de teclas predeterminada, **Ctrl+Alt+Shift+G**. Es sumamente recomendable desactivar el Modo Juego cuando acabe de jugar (puede utilizar la misma combinación de teclas, **Ctrl+Alt+Shift+G**).



Nota

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

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

The screenshot shows the BitDefender Total Security 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, there are two tabs: "Modo Juego" (selected) and "Modo Portátil". The left sidebar contains a navigation menu with categories like General, Antivirus, Antispam, Control Parental, Control de Privacidad, Cortafuego, Vulnerabilidad, Copia Seguridad, Cifrado, Optimizador, and "Modo Juego/Portátil" (selected). Under "Modo Juego/Portátil", there are sub-items: Red, Actualizar, and Registro. The main content area is titled "Estado actual" and shows "Modo Juego desactivado" with an "Activar Modo Juego" button. Below this, there is a section for "Modo Juego Automático activado" with 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". A "Configuración" section follows, with "Opciones Avanzadas" button. It contains two checked tasks: "Tarea de Análisis" and "Tarea de Copia", each with radio buttons for "Omitir Tarea" and "Posponer Tarea". At the bottom, there is a note about applying the game list and a footer with the BitDefender logo and links for "Comprar", "Mi Cuenta", "Registrar", "Ayuda", "Soporte", and "Historial".

Modo Juego

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

24.1.1. Configurando el Modo Juego Automático

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

- **Usar la lista predeterminada de juegos de BitDefender** - para activar automáticamente el Modo Juego 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 juego al entrar en modo pantalla completa** - para activar automáticamente el Modo Juego 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 Juego la próxima vez que la inicie.

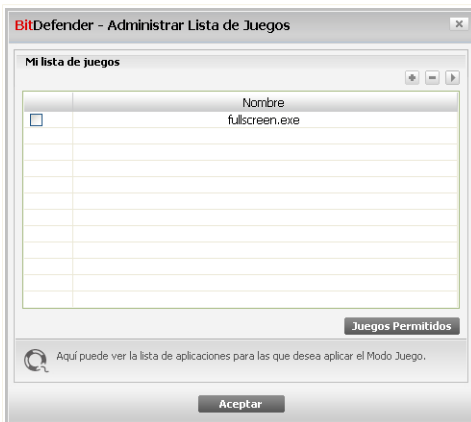


Nota

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

24.1.2. Administrando la Lista de Juegos

BitDefender activará automáticamente el Modo Juego 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.

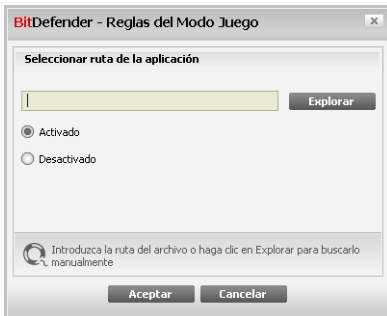
Si desea desactivar el Modo Juego Automático para una aplicación concreta de la lista, desmarque su casilla correspondiente. Debe desactivar el Modo Juego Automático para aquellas aplicaciones de uso habitual que utilizan el modo pantalla completa, como navegadores web o reproductores de vídeos y películas.

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 Juego al iniciar la aplicación seleccionada, seleccione **Desactivar**.



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

24.1.3. Modificando la Configuración del Modo Juego

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 Juego 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 Juego.

- **Tarea de Copia** - para impedir que las tareas de copia programadas se ejecuten mientras el Modo Juego 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 Juego.

Para desactivar automáticamente el Cortafuego cuando el Modo Juego esté activado, siga estos pasos:

1. Haga clic en **Opciones Avanzadas**. Aparecerá una nueva ventana.
2. Marque la casilla **No usar cortafuego**.
3. Haga clic en **Aplicar** para guardar los cambios.



24.1.4. Cambiando el Atajo de Teclado del Modo Juego

Puede activar manualmente el Modo Juego 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.



24.2. 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 Juego/Portátil > Modo Portátil** en la Vista Avanzada.

The screenshot shows the BitDefender Total Security 2009 - Evaluación interface. At the top, there is a status bar with the text "ESTADO: Hay 2 incidencias por resolver" and a "REPARAR TODAS" button. Below this, there are two tabs: "Modo Juego" and "Modo Portátil", with "Modo Portátil" selected. The main content area is divided into a left sidebar with various settings categories and a main panel for "Modo Portátil".

Modo Portátil

- Modo Portátil activado**
- Tarea de Análisis
 - Omitir Tarea
 - Posponer Tarea
- Tarea de Copia
 - Omitir Tarea
 - Posponer Tarea

Below the settings, there is a note: "Seleccione esta opción para omitir las tareas de análisis si el Modo Portátil está activado y así prolongar la duración de su batería."

At the bottom of the window, there is a footer with the BitDefender logo and navigation links: "Comprar - Mi Cuenta - Registrar - Ayuda - Soporte - Historial".



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.

24.2.1. Configurando las Opciones del Modo Portátil

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

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

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

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

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



25. Red

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

BitDefender Total Security 2009 - Evaluación

VISTA BÁSICA

ESTADO: Hay una 1 incidencia por resolver

REPARAR

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)

Unirse a/Crear Red

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

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.



25.1. 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**.

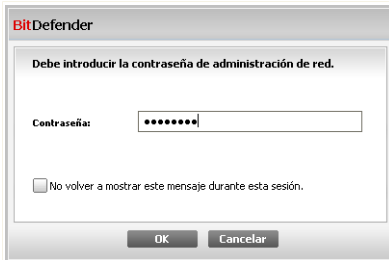
Podrá ver como el nombre del equipo aparece en el mapa de la red.

25.2. 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.

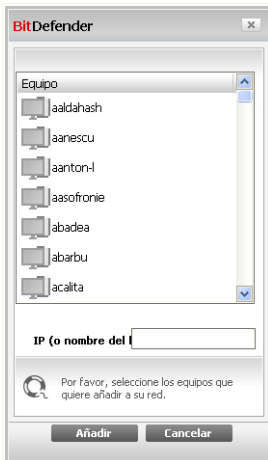
Para añadir un equipo a la red de administración de BitDefender, siga estos pasos:

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.




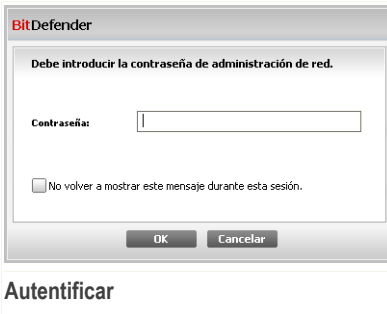
Añadir Equipo

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 label "Contraseña:" followed by a text input field. 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".

- 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.

25.3. 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 Total Security 2009 evaluation interface. At the top, a red banner indicates "ESTADO: Hay una 1 incidencia por resolver" and a "REPARAR" button. The main area is titled "Red" and displays a network diagram with "INTERNET" at the top and several devices below. A context menu is open over one device, listing actions such as "Registrar este equipo", "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", "Aplicar Perfil", "Iniciar una tarea de Optimizador en este equipo", and "Establecer como Servidor de Actualizaciones de esta Red".

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 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.



26. 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 de los motores antispam** - se añadirán nuevas firmas a los filtros Heurístico y URL, y nuevas imágenes al filtro de Imágenes. Este tipo de actualizaciones ayudarán a aumentar la efectividad del motor Antispam, y se conoce como **Actualización del Antispam**.
- **Actualizaciones para los motores antispware** - se añadirán nuevas firmas de spyware a la base de datos. Esta actualización también es conocida como **Actualización Antispware**.
- **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**.

26.1. Actualización automática

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



BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Actualizar Configuración

General

Antivirus

Antispam

Control Parental

Control de Privacidad

Cortafuego

Vulnerabilidad

Copia Seguridad

Cifrado

Optimizador

Modo Juego/Portátil

Red

Actualizar

Registro

Actualización automática activada

Última comprobación 20.08.2008 16:20:22

Última actualización Nunca Actualizar

Propiedades de las Firmas de Virus

Firmas de Virus 1571313 Lista de Virus

Versión del motor 7.20597

Estado de la Descarga

Se ha producido un error durante la actualización (HTTP error 404).
Si el problema persiste, contacte con el soporte de BitDefender (información de contacto disponible desde el apartado Acerca de)

Archivo:	0 %	0 kb
Total actualización	0 %	0 kb

Mantenga activada la actualización automática para asegurarse que las firmas de malware y su producto BitDefender se actualizan regularmente.

[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.



26.1.1. 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.

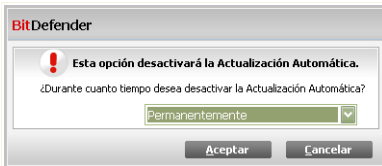


Nota

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

26.1.2. 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.

26.2. Configuración de la Actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy. Por defecto, BitDefender comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

Para modificar la configuración de la actualización y del proxy, haga clic en **Actualización > Configuración** en la Vista Avanzada.

Configuración de la Actualización

Las opciones de actualización están agrupadas en 4 categorías (**Configuración de la Ubicación de las Actualizaciones**, **Configuración de la Actualización Automática**, **Configuración de la Actualización Manual** y **Opciones Avanzadas**). Cada categoría se describirá por separado.



26.2.1. 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. 395).

26.2.2. 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.



26.2.3. 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.

26.2.4. 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 Juego está activado** - BitDefender no se actualizará mientras el modo juego esté activado. De esta manera podrá minimizar el impacto del producto en el rendimiento del sistema mientras juega.

26.2.5. 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.



27. Registro

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

BitDefender Total Security 2009 - Evaluación CAMBIAR A VISTA BÁSICA

ESTADO: Hay 2 incidencias por resolver REPARAR TODAS

Registro

General
Antivirus
Antispam
Control Parental
Control de Privacidad
CortaFuego
Vulnerabilidad
Copia Seguridad
Cifrado
Optimizador
Modo Juego/Portátil
Red
Actualizar
Registro

Información del Producto
BitDefender Total Security 2009
Versión: 12.0.10

Información de Registro
Registrado por testare.automata@live.com
Caduca en 30 días
Número de licencia: DBA3EE27571F96A3C7F2

Acciones
[Crear una cuenta](#)
[Registrar Ahora](#)

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.

[Comprar](#) - [Mi Cuenta](#) - [Registrar](#) - [Ayuda](#) - [Soporte](#) - [Historial](#)

Registro

Esta sección muestra:

- **Información del Producto:** el producto BitDefender product y la versión.
- **Información del Registro:** la dirección de correo utilizada para iniciar sesión con su Cuenta de BitDefender (si está configurada), la licencia actual y lo días restantes hasta que caduque la licencia.

27.1. Registrando BitDefender Total Security 2009

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



BitDefender Total Security 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: **DBA3EE27571F96A3C7F2**
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 Internet Total 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**.

27.2. 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 Total Security 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. 401)



- “Ya tengo una cuenta de BitDefender” (p. 401)

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



28. 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 suporte@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.

28.1. 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>.



28.2. Solicitando Ayuda

28.2.1. 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/>

28.2.2. 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/>



28.3. 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.

28.3.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Soporte técnico: soporte@bitdefender.es
Documentación: documentation@bitdefender.com
Programa de Partners: partners@bitdefender.es
Marketing: marketing@bitdefender.es
Relaciones con la Prensa: prensa@bitdefender.es
Oportunidades de Trabajo: jobs@bitdefender.es
Envío de Virus: virus@bitdefender.es
Envío de Spam: spam_submission@bitdefender.com
Notificar abuso: abuso@bitdefender.es
Página del producto: <http://www.bitdefender.es>
Productos en ftp: <ftp://ftp.bitdefender.com/pub>
Distribuidores locales: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: <http://kb.bitdefender.com>

28.3.2. Filiales

Las oficinas de BitDefender están listas para responder cualquier pregunta relativa a sus áreas de operación, tanto a nivel comercial como en asuntos generales. Sus direcciones y contactos están listados a continuación.

Estados Unidos

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Tel: 1-954-776-6262
Web: <http://www.bitdefender.com>

Soporte Técnico (Sólo para Usuarios Registrados):

- E-mail: support@bitdefender.com
- Tel (Llamada Gratuita):



- Estados Unidos: 1-888-868-1873
- Canadá: 1-866-947-1873

Servicio de Atención al Cliente (Sólo para Usuarios Registrados):

- E-mail: customerservice@bitdefender.com
- Tel (Llamada Gratuita):
 - Estados Unidos: 1-888-868-1873
 - Canadá: 1-866-947-1873

Alemania

BitDefender GmbH

Headquarter Europa Occidental

Saarlandstrasse 84

44139 Dortmund

Alemania

Tel: +49 (0)231 99 33 98 0

Email: info@bitdefender.com

Comercial: sales@bitdefender.com

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

Soporte Técnico: support@bitdefender.com

Reino Unido e Irlanda

Business Centre 10 Queen Street

Newcastle, Staffordshire

ST5 1ED

Tel: +44(0)1782664865

Email: info@bitdefender.com

Comercial: sales@bitdefender.com

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

Soporte técnico: soporte@bitdefender.es

España

BitDefender España, S.L

C/ Balmes 191, 2ª planta, 08006

Barcelona

Soporte Técnico: soporte@bitdefender.es

Comercial: comercial@bitdefender.es



Tel: +34 932189615
Fax: +34 932179128
Web: <http://www.bitdefender.es>

Rumania

BITDEFENDER

West Gate Park, Building H2, 24 Preciziei Street
Bucharest

Soporte técnico: soporte@bitdefender.es

Comercial: sales@bitdefender.com

Tel: +40 21 3001255

Tel: +40 21 3001254

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



BitDefender Total Security 2009

CD de Rescate de BitDefender



29. General

BitDefender Total Security 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/

29.1. 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.

29.2. 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](#) .



30. 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.

30.1. 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.

Espera 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

30.2. 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) (khsbpbkt) (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

30.3. ¿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**.

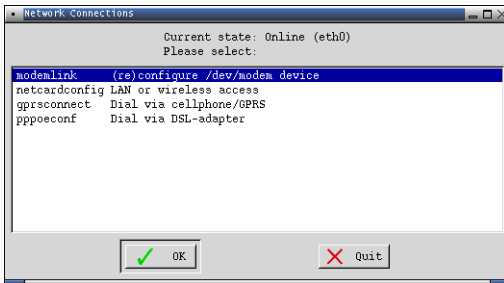
También puede utilizar el siguiente comando estando conectado como root en la terminal. El **Análisis Antivirus de BitDefender** comenzará a analizar los archivos y carpetas seleccionados.

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

30.4. ¿Cómo puedo configurar la conexión a Internet?

Si tiene una red con DHCP y tiene una tarjeta de red ethernet, Linux Defender debe detectar y configurar automáticamente la conexión de Internet. Para configurar manualmente la conexión de Internet debe seguir los pasos.

1. Haga doble clic en el acceso directo de Network Connections situado en el Escritorio. Aparecerá la siguiente ventana.



Network Connections (Conexiones de Red)

2. Seleccione el tipo de conexión que utiliza y haga clic en OK.



Conexión	Descripción
modemlink	Seleccione este tipo de conexión cuando utilice un módem y una línea de teléfono para acceder a Internet.
netcardconfig	Seleccione este tipo de conexión cuando utilice una conexión de área local (LAN) para acceder a Internet. Esta opción también es válida para conexiones Wi-Fi.
gprsconnect	Seleccione este tipo de conexión cuando acceda a Internet mediante un teléfono móvil y el protocolo GPRS (General Packet Radio Service). Utilice esta opción si en lugar de un teléfono móvil, utiliza un módem GPRS.
pppoeconf	Seleccione este tipo de conexión cuando utilice un módem DSL (Digital Subscriber Line) para acceder a Internet.

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



Importante

Tenga en cuenta que, al seleccionar las opciones mencionadas anteriormente, sólo activará el módem. Para configurar la conexión de red, siga estos pasos:

1. Haga clic derecho en el Escritorio y aparecerá el menú contextual del CD de Rescate de BitDefender.
2. Seleccione **Terminal (as root)**.
3. Introduzca el siguiente comando:

```
# pppconfig
```

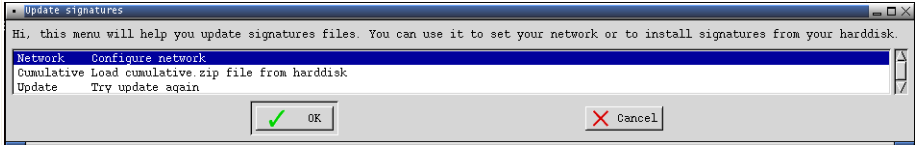
4. Siga las instrucciones que aparecen en pantalla. Si no está seguro de los datos que debe introducir, póngase en contacto con su administrador de sistema o red para más detalles.

30.5. ¿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**.

30.5.1. ¿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`.



30.6. 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 dónde el CD de Rescate de BitDefender resulta sumamente útil.

Para guardar sus datos del ordenador en un dispositivo extraíble, como una memoria USB, sólo tiene que seguir estos pasos:

1. Introduzca el CD de Rescate de BitDefender en la unidad de CD, la memoria USB en la ranura USB correspondiente, y reinicie el ordenador.



Nota

Si conecta una memoria USB en otro momento, deberá montar la unidad extraíble siguiendo estos pasos:

- a. Haga doble clic en el acceso directo de Terminal 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.



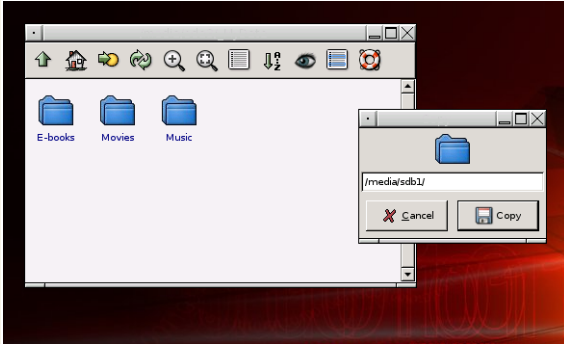
Importante

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.