bitdefender
ANTIVIRUS v10

10th anniversary

Guía de usuario

Antivirus

Antispyware

bitdefender
secure your every bit

BitDefender Antivirus v10

Guía de usuario

BitDefender

publicado 2007.04.12
Version 10.2

Advertencia legal


bitdefender
secure your every bit

Tabla de contenidos

Licencia y garantía ix

Prólogo xiii

1. Convenciones utilizadas en este libro xiii
   1.1. Convenciones Tipográficas xiii
   1.2. Advertencias xiv
2. La Estructura del Manual xiv
3. Petición de Comentarios xv

Acerca de BitDefender 1

1. ¿Quién es BitDefender? 3
   1.1. ¿Por qué BitDefender? 3

Instalación del Producto 7

2. Instalación de BitDefender Antivirus v10 9
   2.1. Requisitos del Sistema 9
   2.2. Pasos de la Instalación 9
   2.3. Asistente de Configuración Inicial 12
      2.3.1. Paso 1/8 - Bienvenido al Asistente de Configuración Inicial 13
      2.3.2. Paso 2/8 - Registrar BitDefender Antivirus v10 13
      2.3.3. Paso 3/8 - Crear una cuenta de BitDefender 14
      2.3.4. Paso 4/8 - Introducir Detalles de la Cuenta 15
      2.3.5. Paso 5/8 - Aprender sobre RTVR 16
      2.3.6. Paso 6/8 – Seleccionar la Tarea a Ejecutar 17
      2.3.7. Paso 7/8 - Esperar a que Finalicen las Tareas 18
      2.3.8. Paso 8/8 - Resumen 19
   2.4. Actualización de la versión del Producto 19
   2.5. Eliminando, reparando o modificando BitDefender 20

Descripción y Características 21

3. BitDefender Antivirus v10 23
   3.1. Antivirus 23
   3.2. Antispyware 24
   3.3. Otras características 24

4. Módulos BitDefender 27
   4.1. Módulo General 27
   4.2. Módulo Antivirus 27
   4.3. Módulo Antispyware 27
   4.4. Módulo Actualización 28

Consola de Administración 29

5. General 31
5.1. Bandeja del sistema 32
5.2. La barra de actividad del análisis 33

6. Módulo General 35
6.1. Administración Central 36
6.1.1. Tareas rápidas 36
6.1.2. Nivel de Seguridad 37
6.1.3. Estado de Registro 38
6.2. Configuración de la Consola de Administración 38
6.2.1. Configuración General 39
6.2.2. Configuración del Informe de Virus 40
6.2.3. Configuración del Skin 40
6.2.4. Importar/Exportar Configuración 40
6.3. Eventos 41
6.4. Registro del Producto 42
6.4.1. Asistente de Registro 42
6.5. Acerca de 47

7. Módulo Antivirus 49
7.1. Análisis en Tiempo Real 49
7.1.1. Nivel de Protección 50
7.2. Análisis Bajo Demanda 55
7.2.1. Tareas de Análisis 55
7.2.2. Menú Rápido 57
7.2.3. Propiedades de la Tarea de Análisis 57
7.2.4. Tipos de Análisis Bajo Demanda 69
7.2.5. Análisis de Rootkits 72
7.3. Cuarantena 74

8. Módulo Antispyware 77
8.1. Estado Antispyware 78
8.1.1. Nivel de Protección 79
8.2. Configuración avanzada - Control de Privacidad 79
8.2.1. Asistente de Configuración 80
8.2.2. Administrando la Reglas 83
8.3. Configuración Avanzada - Control de Registro 84
8.4. Configuración avanzada - Control de Llamadas 86
8.4.1. Asistente de Configuración 88
8.5. Configuración avanzada - Control de las Cookies 90
8.5.1. Asistente de Configuración 91
8.6. Configuración avanzada - Control de Scripts 93
8.6.1. Asistente de Configuración 94
8.7. Información del Sistema 96

9. Módulo Actualización 97

9.1. Actualización automática 97
9.2. Actualización manual 98
9.2.1. Actualización manual con `weekly.exe` 99
9.2.2. Actualización manual con `archivos zip` 99
9.3. Configuración Actualización 101
9.3.1. Configuración de la Ubicación de las Actualizaciones 102
9.3.2. Opciones de la Actualización Automática 102
9.3.3. Configuración de la Actualización Manual 103
9.3.4. Opciones Avanzadas 103

Mejores Prácticas 105

10. Mejores Prácticas 107
10.1. Cómo Proteger Su Equipo contra las Amenazas de Malware 107
10.2. Cómo Configurar una Tarea de Análisis 108

CD de Rescate de BitDefender 109

11. General 111
11.1. Que es KNOPPIX? 111
11.2. Requisitos del Sistema 111
11.3. Software incluido 112
11.4. Soluciones de Seguridad BitDefender para Linux 112
11.4.1. BitDefender SMTP Proxy 112
11.4.2. BitDefender Remote Admin 113
11.4.3. BitDefender Linux Edition 113

12. Cómo utilizar LinuxDefender 115
12.1. Iniciar y salir 115
12.1.1. Iniciar LinuxDefender 115
12.1.2. Salir LinuxDefender 116
12.2. Configure la conexión de Internet 117
12.3. Actualizar BitDefender 118
12.4. Análisis de Virus 118
12.4.1. Como tener acceso a mis datos de Windows? 118
12.4.2. Como realizar un análisis antivirus? 119
12.5. Crear una protección de mail instantánea 119
12.5.1. Requisitos 120
12.5.2. Protección de email 120
12.6. Realice una auditoria de seguridad de la red 121
12.6.1. Compruebe la existencia de rootkits 121
12.6.2. Nessus - Analizador de Red 121
12.7. Compruebe el estado de la memoria RAM 122

Conseguir Ayuda 123

13. Soporte 125

13.1. Departamento de soporte 125
13.2. Ayuda On-line 125
13.2.1. BitDefender Knowledge Base 125
13.3. Información de contacto 126
13.3.1. Direcciones Web 126
13.3.2. Filiales 126

Glosario 129

Licencia y garantía

SI NO ESTÁ DE ACUERDO CON ESTOS TÉRMINOS Y CONDICIONES NO INSTALE EL SOFTWARE. AL SELECCIONAR "ACEPTO", "OK", "CONTINUAR", "SI" O AL INSTALAR O USAR EL SOFTWARE DE ALGÚN MODO, ESTÁ INDICANDO QUE HA ENTENDIDO POR COMPLETO Y HA ACEPTADO LOS TÉRMINOS DE ESTE ACUERDO.

Estos términos cubren las Soluciones y Servicios BitDefender dedicados al usuario doméstico incluidos en su licencia, tales como la información relacionada y cualquier actualización o mejora de las aplicaciones entregadas bajo los términos de la licencia comprada, o cualquier acuerdo de servicio relacionado según lo definido en la documentación y cualquier copia de estos artículos.

Esta licencia le concede el derecho de instalación sólo para uso doméstico.

Este Contrato de Licencia representa un acuerdo legal entre Usted (como persona física o jurídica) y SOFTWIN para la utilización del software de SOFTWIN identificado anteriormente, que incluye el software y servicio informático y puede incluir también soporte físico adjunto y materiales impresos, así como la documentación electrónica u “online” (designada aquí como “BitDefender”), todo lo cual está protegido por la legislación y tratados internacionales referentes al copyright. La instalación, copia u otra forma de utilización del producto BitDefender, significa que acepta los términos de este contrato.

Si no está de acuerdo con los términos de este acuerdo, no instale o use BitDefender.

Licencia BitDefender. BitDefender está protegido por las leyes de derechos de autor (el copyright), las leyes de la propiedad intelectual y otros tratados internacionales que sean de aplicación. El producto de software BitDefender es un producto con licencia. La licencia va junto con el producto y no se vende por separado.

CONCESIÓN DE LICENCIA: Por la presente, SOFTWIN le concede a usted y sólo la siguiente licencia no exclusiva, limitada, instransferible y con pago de derechos para el uso de BitDefender.

SOFTWARE DE APLICACIÓN. Usted puede instalar y usar BitDefender, en tantos de ordenadores como sea necesario considerando la limitación impuesta por el número total de usuarios autorizados. Usted puede hacer una copia adicional a modo de copia de seguridad.

LICENCIA DE USUARIO DOMÉSTICO: Esta licencia se aplica al software BitDefender que puede instalarse en un sólo equipo y que no proporcione servicios a la red. Cada usuario primario puede instalar este software sobre un sólo ordenador y puede hacer

una copia adicional para la reserva sobre un dispositivo diferente. El número de usuarios primarios permitidos es el número de los usuarios de la licencia.

TÉRMINOS DE LICENCIA. La licencia concedida a continuación comenzará en la fecha de adquisición de BitDefender y expirará al final del período para el cual compró la licencia.

VENCIMIENTO: El producto cesará en sus funciones inmediatamente después de la expiración de la licencia.

ACTUALIZACIONES DE PRODUCTO (UPGRADES): Si BitDefender tiene disponible una actualización de producto (update), debe ser un usuario registrado para usar el producto identificado por SOFTWIN para poder beneficiarse de dicha actualización. La actualización de BitDefender sustituye y/o complementa el producto básico con licencia. Puede usar el producto resultante actualizado conforme a los términos de este Acuerdo de licencia. Si hay alguna actualización de algún componente del paquete de software para el cual tiene licencia para un sólo producto, BitDefender puede ser transferido y usado sólo como parte del paquete de producto y no puede ser separada para usarse en más ordenadores de los autorizados por medio de la licencia. Los términos y condiciones de esta licencia reemplazan y sustituyen cualquier acuerdo previo que pueda haber existid entre usted y SOFTWIN respecto al producto original o el producto actualizado resultante.

COPYRIGHT. Todos los derechos, títulos y todos los beneficios como los derechos de copia acerca de BitDefender (incluyendo pero de forma no exclusiva a cualquier imagen, fotografía, logo, animación, vídeo, audio, música, texto y “applets” incorporados en BitDefender), los materiales impresos adjuntos y cualquier copia de BitDefender son propiedad de SOFTWIN. BitDefender está protegido por la legislación y tratados internacionales referentes al copyright. Así pues, Usted debe tratar a BitDefender como a cualquier otro producto con copyright. No debe copiar el material que acompaña al producto BitDefender. El comprador tiene la obligación de incluir todos los documentos originales de Copyright para todas las copias creadas independientemente del medio de grabación o en el BitDefender adquirido. Está prohibido entregar licencias y también alquilar, vender, o realizar "leasing" para el producto BitDefender. Tampoco debe rediseñar, recompilar, desensamblar, crear trabajos derivativos, modificar, traducir o realizar cualquier intento para descubrir el código fuente de BitDefender.

LÍMITES DE LA GARANTÍA. SOFTWIN garantiza el funcionamiento del programa BitDefender, de acuerdo con lo especificado en el manual y ayuda electrónica incluidas en el producto durante treinta días a partir de la fecha de recepción. Si el CD incluido en el paquete BitDefender, presenta defectos que impidan el buen funcionamiento del programa en este plazo, la empresa SOFTWIN garantiza al usuario la reparación, sustitución del producto o reembolso del importe económico pagado por la compra

del mismo, siempre que esté acompañado por el certificado de licencia y el comprobante de compra. SOFTWIN no garantiza que BitDefender será ininterrumpido, libre de errores o que los errores serán corregidos. SOFTWIN no garantiza que BitDefender cubrirá sus requisitos.

CON EXCEPCIÓN DE LO EXPLICITAMENTE DISPUESTO EN ESTE ACUERDO, SOFTWIN NIEGA CUALQUIER OTRA GARANTÍA, EXPLICITA O IMPLÍCITA, EN LO QUE CONCIERNE A LOS PRODUCTOS, MEJORAS, MANTENIMIENTO O SOPORTE RELACIONADO, ASI COMO CUALQUIER OTRO MATERIAL (TANGIBLE O INTANGIBLE) O SERVICIOS SUMINISTRADOS POR ÉL. SOFTWIN, POR LA PRESENTE, NIEGA EXPRESAMENTE CUALQUIER GARANTÍA Y CONDICION IMPLÍCITA, INCLUYENDO, SIN RESTRICCIÓN, LAS GARANTÍAS IMPLÍCITAS DE VALOR COMERCIAL, IDONEIDAD PARA UN OBJETIVO PARTICULAR, TÍTULO, NO INTERFERENCIA, EXACTITUD DE DATOS, EXACTITUD DE CONTENIDO INFORMATIVO, INTEGRACIÓN DEL SISTEMA, Y LA NO INFRACCIÓN DE DERECHOS DE UN TERCERO POR FILTRADO, DESHABILITACION, O ELIMINACIÓN DEL SOFTWARE DE DICHO TERCERO, SPYWARE, ADWARE, COOKIES, CORREO ELECTRÓNICO, DOCUMENTOS, PUBLICIDAD O SIMILARES, TANTO SI SURGE POR ESTATUTO, LEY, CURSO DEL TRATO, COSTUMBRE Y PRÁCTICA O USO COMERCIAL.

TÉRMINOS LEGALES. El usuario que analiza, prueba o evalúa BitDefender será responsable de los perjuicios que pudieran producirse por el uso incorrecto del producto. En ningún caso, SOFTWIN se hará responsable por ningún tipo de daño incluyendo, sin limitaciones, los daños directos o indirectos que deriven de la utilización del producto BitDefender aunque SOFTWIN haya sido advertido de la existencia o la posibilidad de aparición de tales daños. ALGUNOS ESTADOS NO PERMITEN LA LIMITACIÓN O EXCLUSIÓN DE RESPONSABILIDAD POR DAÑOS ACCIDENTALES O DERIVADOS, DE MODO QUE LA LIMITACIÓN O EXCLUSIÓN ANTERIOR PUEDE NO APICARSE EN USTED. EN NINGÚN CASO LA RESPONSABILIDAD DE SOFTWIN EXCEDERÁ EL PRECIO DE COMPRA PAGADO POR USTED POR LA COMPRA DE BITDEFENDER. Las condiciones estipuladas en esta sección se aplicarán tanto si acepta, utiliza, evalúa o prueba BitDefender.

AVISO IMPORTANTE A LOS USUARIOS. ESTE SOFTWARE PUEDE CONTENER ERRORES, Y NO ESTÁ INDICADO SU UTILIZACIÓN EN NINGÚN MEDIO QUE REQUIERA UN GRADO ALTO DE RIESGO Y QUE NECESITE ALTA ESTABILIDAD. ESTE PRODUCTO DE SOFTWARE NO ESTÁ DESTINADO A SECTORES DE LAS AREAS DE AVIACIÓN, CENTRALES NUCLEARES, SISTEMAS DE TELECOMUNICACIONES, ARMAS, O SISTEMAS RELACIONADOS CON LA SEGURIDAD DIRECTA O INDIRECTA DE LA VIDA. TAMPOCO ESTÁ INDICADO PARA APLICACIÓNES O INSTALACIONES DONDE UN ERROR DE

FUNCIONAMIENTO PODRÍA PROVOCAR LA MUERTE, DAÑOS FÍSICOS O DAÑOS CONTRA LA PROPIEDAD.

GENERAL. Este Contrato está gobernado por las leyes de Rumania y por la legislación y tratados internacionales relativos al copyright. La jurisdicción y venia exclusiva para adjudicar cualquier disputa que derive de esos Términos de Contrato pertenece a los juzgados de Rumania.

Los precios, gastos y tarifas del uso de BitDefender están sujetos a cambios sin previo aviso.

En caso de invalidez de cualquier cláusula de este Acuerdo, la invalidez no afectará la validez de las partes restantes de este Acuerdo.

BitDefender y los logos BitDefender son las marcas registradas por SOFTWIN. Todas otras marcas registradas usadas en el producto o en materiales asociados son la propiedad de sus respectivos dueños.

La licencia quedará rescindida inmediatamente sin previo aviso si usted viola cualquiera de sus términos y condiciones. Usted no tendrá derecho a un reembolso por parte de SOFTWIN o de ninguno de los distribuidores o revendedores de BitDefender como consecuencia de la rescisión. Los términos y condiciones acerca de la confidencialidad y restricciones sobre el uso permanecerán en vigor hasta después de cualquier rescisión.

SOFTWIN podrá revisar estos Términos en cualquier momento y los términos revisados se aplicarán automáticamente a las versiones correspondientes del Software distribuido con dichos términos revisados. Si cualquier parte de estos Términos fuera encontrado nulo o impracticable, la validez del resto de los Términos no se verá afectada, ya que seguirán siendo válidos y practicables.

En caso de controversia o inconsistencia entre las traducciones a otros idiomas de estos Términos, prevalecerá la versión en inglés emitida por SOFTWIN.

Haga clic en **Atrás** para volver al paso anterior o haga clic en **Cancelar** para abandonar el proceso de instalación. Si desea continuar de todos modos, haga clic sobre **Siguiente**.

Prólogo

Esta guía está dirigida a todos los usuarios que han elegido **BitDefender Internet Security v10** como solución de seguridad para sus ordenadores personales. La información presentada en este libro es apta no sólo para expertos en informática, sino para todo aquel capaz de trabajar bajo Windows.

Este manual le describirá el uso de BitDefender Internet Security v10, la compañía y el equipo que lo ha desarrollado le guiarán a través del proceso de instalación y le enseñarán a configurarlo. Descubrirá cómo utilizar BitDefender Internet Security v10, cómo actualizarlo, probarlo y personalizarlo. Aprenderá a sacarle el máximo provecho.

Le deseamos una provechosa y agradable lectura.

1. Convenciones utilizadas en este libro

1.1. Convenciones Tipográficas

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

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

1.2. Advertencias

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

Nota

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

Importante

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

Aviso

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

2. La Estructura del Manual

El libro consta de 7 partes, que describen los temas más importantes: Acerca de BitDefender, Instalación del Producto, Descripción y Características, Consola de Configuración, Mejores Prácticas, CD de Rescate de BitDefender y Ayuda. También se incluye un glosario y el apéndice para aclarar diferentes aspectos técnicos.

Acerca de BitDefender. Pequeña introducción a BitDefender.

Instalación del Producto. Instrucciones paso a paso para instalar BitDefender en una estación de trabajo. Se trata de un exhaustivo tutorial sobre la instalación de **BitDefender Antivirus v10**. Se le guía a través del proceso completo de instalación, empezando por los pre-requisitos para una correcta instalación. Finalmente, se describe el procedimiento de desinstalación en caso de que necesite desinstalar BitDefender.

Descripción y Características. Se le presentan los módulos y características de **BitDefender Internet Security v10**.

Consola de Administración. Descripción de los procesos básicos de administración y mantenimiento de BitDefender. El capítulo explica en detalle todas las opciones de **BitDefender Antivirus v10**, cómo registrar el producto, cómo analizar su equipo y cómo realizar las actualizaciones. Se le enseña a configurar y usar todos los módulos BitDefender.

Mejores Prácticas. Siga estas instrucciones para conseguir el mejor rendimiento de BitDefender.

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

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

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

3. Petición de Comentarios

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

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

Importante

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

Acerca de BitDefender

1. ¿Quién es BitDefender?

BitDefender es una compañía Europea pionera, dedicada al desarrollo de soluciones de seguridad para satisfacer los requisitos de protección del entorno informático actual. La compañía ofrece una de las líneas más rápidas y más efectivas de software de seguridad, creando nuevos estándares para la detección y mitigación oportuna de las amenazas. BitDefender ofrece productos y servicios a más de 41 usuarios en más de 180 países de todo el mundo. BitDefender dispone de oficinas en **Estados Unidos**, **Reino Unido**, **Alemania**, **España** y **Rumania**.

- Ofrece protección antivirus, cortafuego, antispyware y control parental a usuarios domésticos y corporativos;
- La gama de productos BitDefender está desarrollada para implementarse en estructuras TI complejas (estaciones de trabajo, servidores de ficheros, servidores de correos y puertas de enlace) en plataformas Windows, Linux y FreeBSD;
- Distribución a nivel mundial, productos disponibles en 18 idiomas;
- Fácil de usar, con un asistente de instalación que guía a los usuarios a través del proceso de instalación y realiza pocas preguntas;
- Productos certificados a nivel internacional: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, etc;
- Atención al cliente continua - el equipo de atención al cliente está disponible 24 horas al día, 7 días a la semana;
- Tiempo de respuesta rápido como un rayo ante los ataques a ordenadores nuevos;
- El mejor ratio de detección;
- Actualizaciones de las firmas de virus cada hora - acciones automáticas o programadas que le ofrecen protección ante los nuevos virus

1.1. ¿Por qué BitDefender?

Comprobado. El fabricante antivirus más reactivo. La rápida reacción de BitDefender en caso de epidemia de virus informáticos fue confirmada al comienzo de los últimos brotes de CodeRed, Nimda y Sircam, así como Badtrans.B u otros códigos maliciosos y de rápida propagación. BitDefender fue el primer fabricante en proporcionar antídotos contra estos códigos y en hacerlo de forma gratuita a través de Internet para toda la gente afectada. Ahora, con la extensión continua del virus

Klez en varias versiones, la protección antivirus inmediata se ha convertido una vez más en una necesidad crítica para cualquier sistema informático.

Innovador. Premiado por su innovación por la Comisión Europea y EuroCase. BitDefender ha sido proclamado ganador del European IST-Prize, premiado por la Comisión Europea y por representantes de 18 academias en Europa. Ahora, en su octavo año, el European IST Prize es un premio a los productos pioneros que representan a las mejores tecnologías europeas de innovación e información.

Exhaustivo. Cubre cada punto de su red, ofreciendo una completa seguridad. Las soluciones de seguridad BitDefender satisfacen los requisitos de protección de los entornos empresariales actuales, ofreciendo una solución efectiva contra las amenazas que hacen peligrar una red, desde pequeñas redes hasta multi-plataformas WAN.

La Protección Definitiva. La última frontera para cualquier amenaza posible que pueda afectar a su sistema informático. Dado que la detección de virus basada en el análisis del código no siempre ha ofrecido buenos resultados, BitDefender ha desarrollado una protección basada en el comportamiento, ofreciendo seguridad contra malware 'recién nacido'.

Estos son **los costes** que las organizaciones quieren evitar y los que los productos de seguridad están diseñados para prevenir:

- Ataques de Gusanos
- Pérdida de la comunicación a causa de e-mails infectados
- Fallo del sistema de e-mails
- Sistemas de limpieza y recuperación
- Pérdida de productividad experimentada por los usuarios finales porque los sistemas no están disponibles
- Hacking y accesos no autorizados que causan daños

Puede conseguir **mejoras y beneficios** simultáneamente al utilizar el paquete integrado de seguridad BitDefender:

- Mayor disponibilidad de la red al detener la propagación de ataques de código malicioso (p.ej., Nimda, caballos de Troya, DDoS).
- Protege a los usuarios remotos de ataques.
- Reducción de los costes de administración y rápida distribución gracias a las opciones de administración de BitDefender Enterprise Manager.
- Bloqueo de la propagación de malware a través del correo electrónico usando la protección de BitDefender en la puerta de enlace corporativa. Bloqueo temporal o permanente de las conexiones de aplicaciones no autorizadas, vulnerables o caras.

Puede obtener más información sobre BitDefender visitando: http://www.bitdefender-es.com

Instalación del Producto

2. Instalación de BitDefender Antivirus v10

El apartado **Instalación de BitDefender Antivirus v10** de esta guía contiene los siguientes temas:

- Requisitos del Sistema
- Pasos de la Instalación
- Asistente de Configuración Inicial
- Actualización de la versión del Producto
- Eliminando, reparando o modificando BitDefender

2.1. Requisitos del Sistema

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

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Pentium II 350 MHz o superior
- Mínimo 128 MB de RAM (256 MB recomendado)
- Mínimo 60 MB de espacio libre en disco
- Internet Explorer 5.5 (o superior)

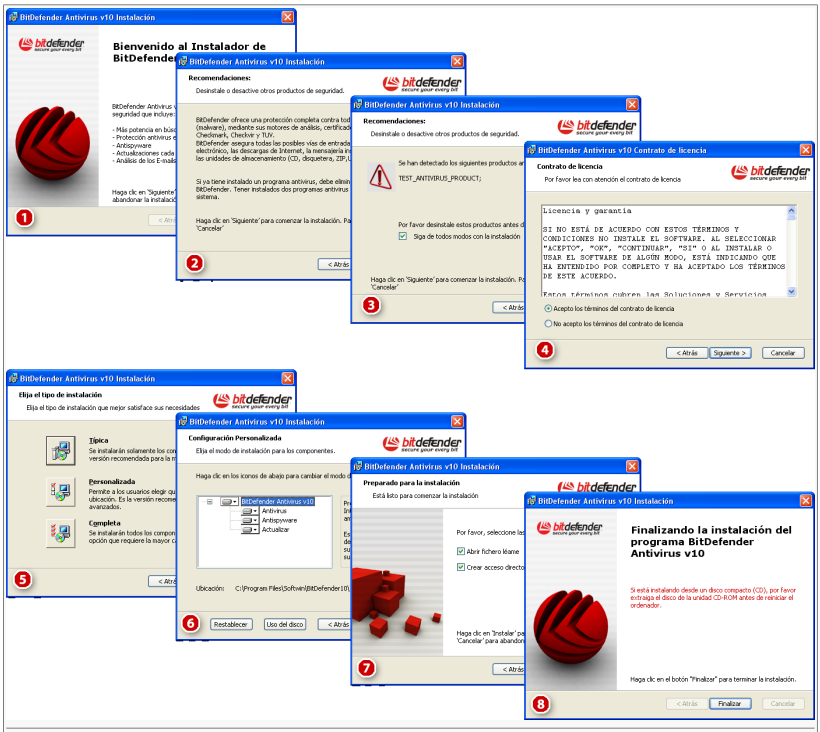
Microsoft Windows Vista 32-bit

- Procesador de 800 MHz o superior
- Mínimo 512 MB de RAM (1 GB recomendado)
- Mínimo 60 MB de espacio libre en disco

BitDefender Antivirus v10 está disponible para descargar y evaluar desde http://www.bitdefender-es.com el portal corporativo de SOFTWIN dedicado a la seguridad de datos.

2.2. Pasos de la Instalación

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



Pasos de la Instalación

1. Haga clic sobre **Siguiente** para continuar o haga clic en **Cancelar** si quiere abandonar el proceso de instalación.
2. Haga clic sobre **Siguiente** para continuar o haga clic en **Atrás** para volver al primer paso.
3. BitDefender Antivirus v10 le alertará si tiene otros productos antivirus instalados en su ordenador.

Aviso

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

Haga clic sobre **Atrás** para volver al paso anterior o haga clic en **Cancelar** para abandonar el proceso de instalación. Si desea continuar de todos modos, haga clic sobre **Siguiente**.

Nota

Si BitDefender Antivirus v10 no detecta otros productos antivirus en su sistema se omitirá este paso.

4. Por favor lea el Contrato de Licencia para el usuario final con atención y si está de acuerdo con las condiciones previstas, seleccione **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**. Si no está de acuerdo con las cláusulas de este contrato, haga clic en **Cancelar**. Abandonará el proceso y saldrá de la instalación.
5. Puede elegir el tipo de instalación que desee: típica, personalizada o completa.

   Típica
   El programa se instalará con las opciones más comunes. Recomendada para la mayoría de usuarios.

   Personalizada
   Puede elegir los componentes que quiere instalar. Se recomienda únicamente a usuarios avanzados.

   Completa
   Para la instalación completa del producto. Se instalarán todos los módulos de BitDefender.

   Si selecciona **Típica** o **Completa** se saltará el paso 6.
6. Si ha seleccionado la opción **Personalizada**,aparecerá una nueva ventana con un listado de todos los componentes de BitDefender en la que podrá seleccionar la instalación de los componentes que desee.

   Haciendo clic en cualquiera de los componentes aparecerá una breve descripción (espacio en disco necesario incluido) en la parte derecha. Seleccionando cualquiera de los iconos se le mostrará una ventana en la que podrá elegir si instalar o no el módulo seleccionado.

   Puede seleccionar la carpeta donde quiere instalar el producto. La carpeta predeterminada es `C:\Archivos de Programa\Softwin\BitDefender 10`.

   Si desea seleccionar otra carpeta haga clic en el botón **Explorar** y en la ventana que aparecerá, seleccione la carpeta deseada. Haga clic sobre **Siguiente**.
7. Tiene dos opciones configuradas por defecto:
   - **Abrir fichero léame** - para abrir el fichero léame al final de la instalación.

- **Crear acceso directo en el Escritorio** - para poner un acceso directo de BitDefender Antivirus v10 en el Escritorio al finalizar la instalación.
- **Desactivar Windows Defender** - para desactivar Windows Defender; esta opción sólo aparece en Windows Vista.

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

Importante

Durante el proceso de instalación aparecerá un Asistente. Este Asistente le ayudará a registrar **BitDefender Antivirus v10**, crear una cuenta de BitDefender y configurarlo para realizar tareas de seguridad importante.
Debe completar el proceso guiado por el Asistente para poder avanzar al siguiente paso.

8. Haga clic en **Finalizar** para completar la instalación del producto. Si ha aceptado la configuración predeterminada de la carpeta de instalación, se creará una nueva carpeta llamada `Softwin` en la carpeta `Archivos de Programa`, que contiene la subcarpeta `BitDefender 10`.

Nota

Es posible que sea necesario reiniciar el sistema para que se complete el proceso de instalación.

2.3. Asistente de Configuración Inicial

Durante el proceso de instalación aparecerá un Asistente. Este Asistente le ayudará a registrar su **BitDefender Antivirus v10**, crear una cuenta de BitDefender y configurar BitDefender para realizar tareas importantes de seguridad.

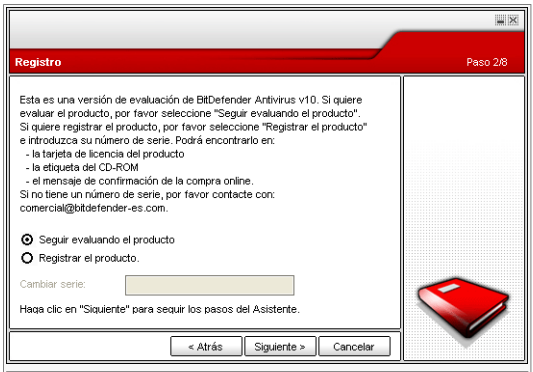
No es obligatorio completar este Asistente. Sin embargo, recomendamos hacerlo para así ganar tiempo y garantizar la seguridad de su sistema incluso antes que BitDefender Antivirus v10 esté instalado.

2.3.1. Paso 1/8 - Bienvenido al Asistente de Configuración Inicial

Ventana de Bienvenida

Haga clic sobre **Siguiente**.

2.3.2. Paso 2/8 - Registrar BitDefender Antivirus v10



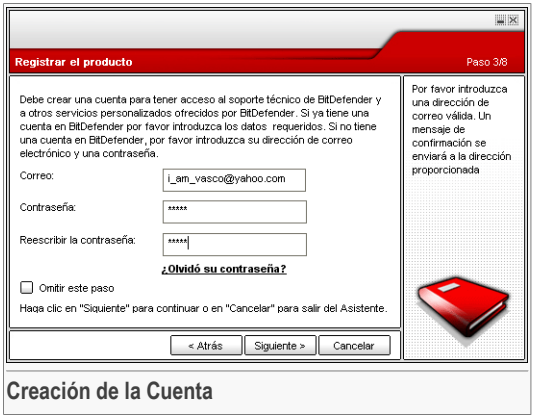
Registro

Seleccione **Registrar el Producto** para registrar **BitDefender Antivirus v10**. Escriba el número de licencia en el campo **Cambiar serie**.

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

Haga clic sobre **Siguiente**.

2.3.3. Paso 3/8 - Crear una cuenta de BitDefender



Creación de la Cuenta

No tengo una cuenta de BitDefender

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

Escriba una dirección de e-mail válida en el campo **Correo**. Piense en una contraseña y escríbala en el campo **Contraseña**. Vuelva a escribir la contraseña en el campo **Rescribir la contraseña**. Utilice la dirección de e-mail y la contraseña para iniciar su sesión en http://myaccount.bitdefender.com.

Nota

La contraseña debe contener 4 caracteres como mínimo.

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

Importante

Por favor, active su cuenta antes de continuar con el siguiente paso.

Si no quiere crear ninguna cuenta de BitDefender, haga clic en **Omitir este paso**. También omitirá el siguiente paso del asistente.

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

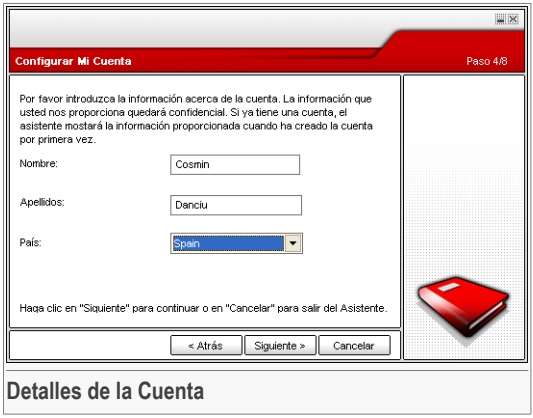
Ya tengo una cuenta de BitDefender

Si ya dispone de una cuenta activa, indique la dirección de e-mail y la contraseña de su cuenta. Si la contraseña indicada es incorrecta, se le volverá a solicitar cuando pulse en **Siguiente**. Haga clic en **Ok** para introducir de nuevo la contraseña o pulse en **Cancelar** para salir del Asistente.

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

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

2.3.4. Paso 4/8 - Introducir Detalles de la Cuenta



Detalles de la Cuenta

Nota

No visualizará este paso si ha seleccionado **Omitir este Paso** en el paso 3

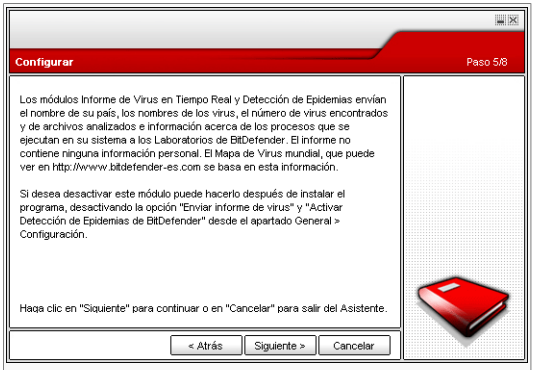
Escriba su nombre y apellido y seleccione su país de residencia.

Si ya tiene una cuenta, el asistente le mostrará la información introducida anteriormente, si la hay. Desde aquí puede modificar esta información si lo desea.

Importante
Los datos que introduzca aquí serán confidenciales.

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

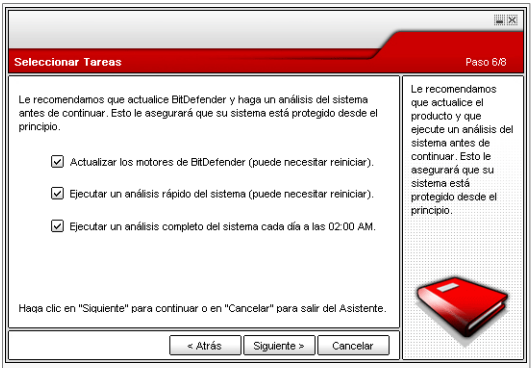
2.3.5. Paso 5/8 - Aprender sobre RTVR



Información RTVR

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

2.3.6. Paso 6/8 – Seleccionar la Tarea a Ejecutar



Selección de la Tarea

Configure BitDefender Antivirus v10 para que ejecute tareas importantes para la seguridad de su sistema.

Las siguientes opciones están disponibles:

- **Actualizar los motores de BitDefender Antivirus v10 (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 que BitDefender Antivirus v10 se asegure que los ficheros de las carpetas `Windows` y `Archivos de Programa` no están infectados.
- **Realizar un análisis completo del sistema cada día a las 2 AM** - ejecuta un análisis completo del sistema cada día a las 2 AM.

Importante

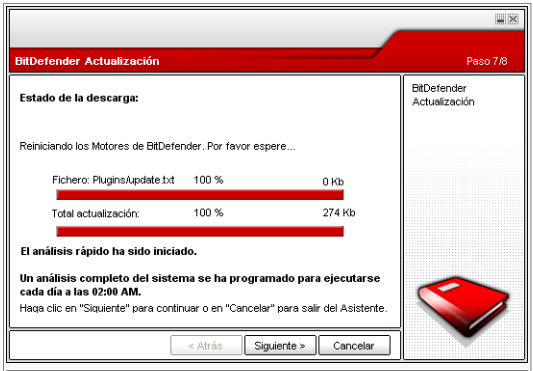
Recomendamos activar estas opciones antes de continuar con el siguiente paso para garantizar la seguridad de su sistema.

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

Puede realizar cualquier cambio volviendo a los pasos anteriores (haga clic en **Atrás**). Más adelante, el proceso será irreversible: si decide continuar, no podrá volver a los pasos anteriores.

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

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

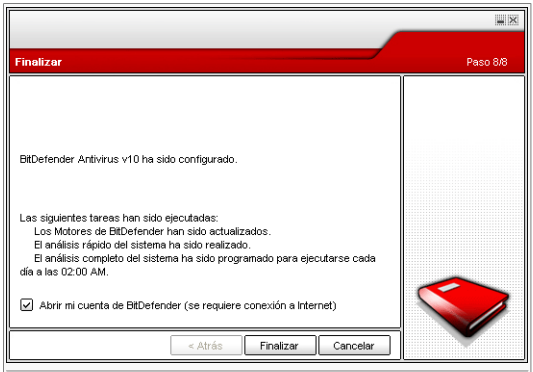


Estado de la Tarea

Esperar a que se complete(n) la(s) tarea(s). Puede comprobar el estado de las(s) tarea(s) seleccionadas en el paso anterior.

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

2.3.8. Paso 8/8 - Resumen



Finalizado

Este es el último paso del asistente de configuración.

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

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

2.4. Actualización de la versión del Producto

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

- **Instalar si desinstalar su versión anterior e instalar la nueva – para la v8 o superior, Internet Security excluido**

  Haga doble clic en el archive de instalación y siga el asistente descrito en la sección "*Pasos de la Instalación*" (p. 9).

  Importante

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

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

  Primero debe desinstalar su versión anterior, reiniciar el ordenador e instalar la nueva como se describe en el apartado "*Pasos de la Instalación*" (p. 9).

Importante

Si actualiza el producto desde la versión BitDefender 8 o posterior, le recomendamos guardar la Configuración de BitDefender. Cuando termine el proceso de actualización de producto podrá cargarla de nuevo.

2.5. Eliminando, reparando o modificando BitDefender

Si quiere modificar, reparar o eliminar **BitDefender Antivirus v10**, siga la ruta del menú Inicio de Windows: **Inicio → Programas → BitDefender 10 → Modificar, Reparar o Desinstalar**.

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

- **Modificar** - para añadir nuevos componentes del programa o para quitar componentes ya instalados.

  Nota

  Para aprender cómo completar el proceso de instalación, consulte sixth step en el apartado "*Pasos de la Instalación*" (p. 9).

- **Reparar** - para reinstalar todos los componentes del programa que se instalaron en la instalación anterior.

  Importante

  Antes de reparar el producto recomendamos guardar la configuración de BitDefender. Después de reparar el producto puede volver a cargar estos datos.

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

  Si decide eliminar BitDefender, dejará de estar protegido contra los virus, spyware y hackers. Si desea activar el Firewall de Windows y Windows Defender tras la desinstalación de BitDefender, seleccione las casillas correspondientes en el siguiente paso del asistente.

  Le agradeceríamos que se tome unos segundos para explicarnos las razones por las que ha decidido desinstalar BitDefender. Seleccione la casilla **Enviar FeedBack** y rellene el formulario online para transmitirnos sus sugerencias.

Para continuar el proceso de instalación, tendrá que seleccionar una de estas opciones. Recomendamos seleccionar la opción **Eliminar** para una reinstalación limpia. Después de la desinstalación, recomendamos eliminar la carpeta `Softwin` de la carpeta `Archivos de Programa`.

Descripción y Características

3. BitDefender Antivirus v10

¡La solución antivirus y antispyware ideal para su PC!

BitDefender Antivirus v10 es un producto antivirus y antispyware de alta seguridad, con funciones diseñadas especialmente para cubrir sus necesidades. Su facilidad de uso y las actualizaciones automáticas hacen de **BBitDefender Antivirus v10** un producto antivirus tipo 'instalar y olvidarse'.

3.1. Antivirus

La misión del módulo Antivirus es asegurar la detección y eliminación de todos los virus en circulación. BitDefender Antivirus usa potentes motores de análisis certificados por los ICSA Labs, Virus Bulletin, Checkmark, Checkvir y TÜV.

Detección Proactiva. B-HAVE (Behavioural Heuristic Analyzer in Virtual Environments) emula un ordenador virtual dentro de su ordenador, en el que se ejecutan fragmentos de software para comprobar si se trata de software malintencionado (malware). Esta tecnología, propiedad de BitDefender, representa una nueva capa de seguridad que mantiene el sistema operativo a salvo de virus desconocidos al detectar partes potencialmente dañinas de código para las cuales todavía no se han publicado las firmas.

Protección Antivirus Permanente. Los nuevos y superiores motores de análisis de BitDefender analizan y desinfectan los ficheros infectados en tiempo real, minimizando la pérdida de datos. Los documentos infectados ahora pueden ser recuperados en lugar de ser eliminados.

Detección y desinfección de Rootkits. Un nuevo módulo de BitDefender que analiza en busca de rootkits (programas maliciosos diseñados para controlar los ordenadores victima, mientras permanecen ocultos) y los elimina al detectarlos.

Análisis Web. El tráfico web es filtrado en tiempo real antes de que llegue al navegador, ofreciéndole una experciencia web agradable y segura.

Protección de Aplicaciones de Mensajería Instantánea y Peer-2-Peer. Análisis en busca de virus que se propagan por las aplicaciones de mensajería instantánea y las carpetas compartidas.

Protección completa del Correo Electrónico. BitDefender se ejecuta al nivel de los protocolos POP3 y SMTP, filtrando los mensajes entrantes y salientes independientemente del cliente de correo utilizado (Outlook™, Outlook Express™ /

/ Windows Mail™, The Bat!™, Netscape®, etc.) sin necesidad de configuración adicional.

3.2. Antispyware

BitDefender monitoriza y bloquea las amenazas potenciales de spyware en tiempo real, antes de que puedan dañar a su sistema. Este módulo utiliza una amplia base de datos de firmas de spyware para conseguir que su ordenador permanezca libre de spyware.

Antispyware en Tiempo-Real. BitDefender monitoriza docenas de puntos clave en su sistema en los que el spyware puede actuar, y verifica cualquier cambio realizado en su sistema o software. Las amenazas Spyware también se bloquean en tiempo real. Las amenazas de spyware conocidas también se bloquean en tiempo real.

Análisis y Desinfección de Spyware. BitDefender puede analizar su sistema, o parte de él, en busca de amenazas spyware conocidas. El análisis utiliza una base de datos de firmas de spyware actualizada en todo momento.

Protección de Privacidad. El guardián de privacidad monitoriza el tráfico saliente HTTP (web) y SMTP (correo electrónico) para detectar qué información podría ser personal - como números de tarjetas de crédito, números de la Seguridad Social u otros datos definidos por el usuario (ej. bits de las contraseñas).

Anti-Dialer. Dispone de un anti-dialer configurable que ofrece protección contra las aplicaciones maliciosas que cambian su conexión a Internet incrementando su factura telefónica.

Control de las Cookies. El antispyware filtra las cookies entrantes y salientes, manteniendo la confidencialidad de su identidad y preferencias mientras navega por Internet.

Control del contenido activo. Bloquea cualquier potencial aplicación maliciosa como: ActiveX, Java Applets o Java Scripts.

3.3. Otras características

Implementación y Uso. Justo después de la instalación se iniciará un Asistente de Configuración que permite a los usuarios elegir la configuración más adecuada para las actualizaciones, implementar un horario para los análisis y le ofrece una forma fácil y cómoda de registrar y activar el producto.

Experiencia del Usuario. BitDefender ha rediseñado la experiencia web, centrándose en la facilidad de uso y evitando confundir al usuario. En consecuencia, muchos

módulos de BitDefender v10 requieren menos interacción por parte del usuario, gracias al uso óptimo de la automatización y del aprendizaje de las máquinas.

Actualizaciones cada hora. Su copia de BitDefender se actualizará 24 veces al día a través de Internet; directamente o a través de un servidor proxy. El programa se puede auto-reparar descargando a través de Internet los ficheros eliminados o dañados.

Soporte 24x7. Brindado por un equipo de profesionales; también le ofecemos una base de datos online con las respuestas a las preguntas más frecuentes.

CD de Rescate. BitDefender Antivirus v10 se distribuye conjuntamente con un CD de auto-arranque. Este CD puede utilizarse para analizar/reparar/desinfectar un sistema que no se puede iniciar.

4. Módulos BitDefender

BitDefender Antivirus v10 incorpora los módulos: **General**, **Antivirus**, **Antispyware** y **Actualización**.

4.1. Módulo General

BitDefender viene totalmente configurado para su máxima seguridad.

Información esencial sobre el estado sobre todos los módulos BitDefender se muestra en el módulo General. Aquí puede registrar su producto y puede configurar el comportamiento general de BitDefender.

4.2. Módulo Antivirus

BitDefender le protege contra los virus, spyware y otras amenazas analizando sus archivos, mensajes, descargas y o cualquier tipo de contenido que entre en su sistema.

La protección que ofrece BitDefender está dividida en dos apartados:

- El análisis en Tiempo Real - impide el acceso de los nuevos virus, spyware y otras amenazas a su sistema. También puede contar con un módulo residente, que analiza los archivos al accederlos. Por ejemplo, BitDefender podrá analizar un documento al abrirlo o un mensaje de correo al recibirlo. BitDefender analiza los ficheros mientras los utiliza, al acceder.
- El análisis Bajo Demanda - detecta los virus, spyware u otras amenazas ya instaladas y residentes en su sistema. Se trata del análisis antivirus clásico, iniciado por el usuario, en el que elige los elementos que serán analizados por BitDefender: unidad, carpeta o fichero.

4.3. Módulo Antispyware

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. Es efectivo bloqueando troyanos u otras herramientas instaladas por hackers, que intentan comprometer su privacidad y enviar su información personal (como números de tarjetas de crédito) desde su equipo al del hacker.

4.4. Módulo Actualización

Cada día se encuentra e identifica nuevo software malintencionado. Por este motivo es tan importante mantener BitDefender actualizado con las últimas firmas de malware. Por defecto, BitDefender busca actualizaciones cada hora.

Las actualizciones se presentan de las siguientes maneras:

- **Actualización de los motores antivirus** - a medida que se detecten nuevas amenazas, los ficheros que incluyen las firmas de virus deberán actualizarse para asegurar una protección permanente contra los éstos. Este tipo de actualización también se conoce como **Actualización de las firmas de virus**.
- **Actualizaciones para los motores antispyware** - se añadirán nuevas firmas de spyware a la base de datos. Esta actualización también es conocida como **Actualización Antispyware**.
- **Actualizaciones del producto** - cuando aparece una nueva versión del producto, se introducen nuevas características y técnicas de análisis para mejorar el rendimiento del producto. Este tipo de actualización es conocido como **Actualización del producto**.

Además, desde el punto de vista de la intervención del usuario, podemos tener en cuenta:

- Actualización automática - BitDefender contacta automáticamente los servidores de actualizaciones para comprobar si hay nuevas actualizaciones para descargar. Si existen, BitDefender se actualizará automáticamente. La actualización automática puede realizarse en el cualquier momento haciendo clic en el botón **Actualizar** dentro del módulo Actualización.
- Actualización manual - tendrá que descargar e instalar las últimas firmas de amenazas manualmente.

Consola de Administración

5. General

BitDefender Antivirus v10 ha sido diseñado con una consola de administración centralizada, la cual permite la configuración de las opciones de protección de todos los módulos BitDefender. Basta con abrir la consola de administración para tener acceso a cualquiera de los módulos BitDefender: **Antivirus**, **Antispyware** y **Actualización**.

Para acceder a la consola de administración debe hacer clic en el menú Inicio de Windows y luego seguir la ruta **Inicio → Programas → BitDefender 10 → BitDefender Antivirus v10**, o de manera más rápida, haciendo doble clic en **el icono de BitDefender** de la bandeja del sistema.

Consola de Administración

En el lado izquierdo de la consola de administración puede seleccionar los módulos:

- General - en este apartado puede configurar el nivel de seguridad global y ejecutar tareas de seguridad esenciales. Aquí también puede registrar el programa y ver un resumen de todas las configuraciones principales, detalles acerca del producto e información de contacto.

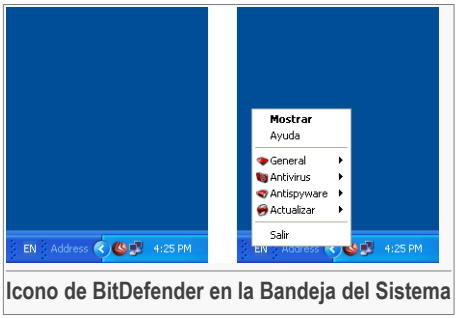
- Antivirus - en este apartado puede configurar el módulo **Antivirus**.
- Antispyware - en este apartado puede configurar el módulo **Antispyware**.
- Actualización - en este apartado puede configurar el módulo **Actualización**.

En la parte derecha de la consola de administración puede ver información sobre el apartado que en el se encuentra. La opción **Más ayuda**, ubicada en la parte inferior derecha, le mostrará el fichero de **Ayuda**.

5.1. Bandeja del sistema

Al minimizar la consola de administración, aparecerá un icono en la bandeja del sistema.

Haciendo doble clic sobre este icono se abrirá la consola de administración. Si en su lugar hace clic con el botón derecho, aparecerá un menú contextual. Este menú le permite administrar BitDefender rápidamente:



Icono de BitDefender en la Bandeja del Sistema

- **Mostar/Cerrar** - abre la consola de administración o la minimiza en la bandeja del sistema.
- **Ayuda** - abre la ventana de ayuda.
- **General** - administración del módulo General.
  - **Cambiar serie** - inicia el Asistente de Registro que le guiará durante el proceso de registro.
  - **Editar cuenta** - inicia un asistente que le ayudará a crear una cuenta de BitDefender.
- **Antivirus** - administración del módulo Antivirus.
  - **La protección en tiempo real está activada/desactivada** - muestra el estado de la protección en tiempo real (activado / desactivado). Haga clic en esta opción para desactivar o activar la protección en tiempo real.
  - **Análisis** - abre un submenú en el que puede seleccionar la ejecución de una de las tarea de análisis disponibles en el apartado Análisis.
- **Antispyware** - administración del módulo Antispyware.
  - **Análisis de Comportamiento Antispyware activado / desactivado** - muestra el estado de la análisis de comportamiento antispyware (activado/desactivado). Haga clic en esta opción para desactivar o activar la protección antispyware.
  - **Opciones avanzadas** - le permite configurar las opciones del antispyware.
- **Actualización** - administración del módulo Actualización.

- **Actualizar** - realiza una actualización inmediata.
- **Actualización automática está activada/desactivada** - muestra el estado de la Actualización automática (enabled / disabled). Haga clic en esta opción para desactivar o activar Actualización automática.

- **Salir** - cierra la aplicación. Seleccionando esta opción, el icono de la barra de tareas desaparecerá y para acceder de nuevo a la consola de administración tendrá que iniciarla de nuevo desde el menú Inicio de Windows.

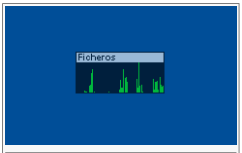
Nota

El icono se irá convirtiendo en negro si desactiva uno o más de los módulos BitDefender. De esta manera sabrá si algunos módulos están desactivados sin tener que abrir la consola de administración.
El icono parpadeará cuando haya actualizaciones disponibles.

5.2. La barra de actividad del análisis

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

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



Barra de Actividad

Nota

La **Barra de Actividad de Análisis** le avisará si el Residente o el Cortafuego están desactivados, marcando una X en las zonas correspondientes (**Ficheros**). De esta manera sabrá si está o no protegido sin entrar en la consola de administración.

Para ocultar esta ventana haga un clic derecho de ratón y elija **Ocultar**.

Nota

Para ocultar completamente esta ventana, deseleccione la opción **Activar barra de actividad** (desde el módulo **General**, sección Configuración).

6. Módulo General

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

- Administración Central
- Configuración de la Consola de Administración
- Eventos
- Registro del Producto
- Acerca de

Nota

Para más detalles acerca del módulo **General** consulte la descripción del "*Módulo General*" (p. 27).

6.1. Administración Central

Administración Central

En este apartado puede configurar el nivel de seguridad global y ejecutar tareas importantes de BitDefender. También puede registrar el producto y ver la fecha de vencimiento.

6.1.1. Tareas rápidas

BitDefender le facilita el acceso a las tareas esenciales de seguridad. Usando estas tareas puede mantener su BitDefender actualizado, analizar su sistema o bloquear el tráfico.

Para analizar todo el sistema sólo haga clic en **Analizar**. Se le mostrará la ventana del análisis y se iniciará un análisis completo del sistema.

Importante

Le recomendamos realizar un análisis completo de su sistema al menos una vez por semana. Para más información acerca de las tareas de análisis y el proceso de análisis vaya al apartado Análisis de esta Guía del Usuario.

Antes de analizar su sistema, le recomendamos que actualice Bitdefender para que pueda detectar las últimas amenazas. Para actualizar BitDefender sólo haga clic en **Actualizar**. Espere unos segundos para que la actualización se finalice o, mejor, verifique en el apartado Actualización el estado de la actualización.

Nota

Para más detalles acerca del proceso de actualización vaya al apartado Actualización automática de esta Guía de Usuario.

6.1.2. Nivel de Seguridad

Puede elegir el nivel de seguridad que mejor cumple con sus necesidades de protección. Arrastre el deslizador a lo largo de la escala para elegir el nivel de seguridad deseado.

Hay 3 niveles de seguridad:

Nivel de Seguridad	Descripción
Mantenimiento	No ofrece protección. Sólo la **Actualización automática** está activada. Sólo actualiza BitDefender. Aunque sea no ofrece ninguna protección, este nivel de seguridad podría ser útil para los administradores de sistema.
Sistema Local	Ofrece protección antivirus. Especialmente recomendado para ordenadores sin acceso a una red o a Internet. El nivel de consumo de recursos es muy bajo. Los archivos a los que accede se analizarán en busca de virus y spyware.
Sistema Local Plus	Ofrece protección antivirus y antispyware, especialmente recomendado para ordenadores sin acceso a una red o a Internet. El nivel de consumo de recursos es bajo. Los archivos a los que se accede serán analizados por virus y spyware.

BitDefender Antivirus v10 es recomendable para los ordenadores sin conexión a Internet.

Puede personalizar el nivel de seguridad haciendo clic en **Personalizado**. En la ventana que aparecerá, seleccione las opciones de protección de BitDefender que desea activar, y haga clic en **Aceptar**.

Haga clic en **Por Defecto** para situar el control deslizante en el nivel por defecto.

6.1.3. Estado de Registro

Puede ver información acerca del estado de su licencia de BitDefender. Aquí puede registrar su producto y visualizar la fecha de caducidad.

Para introducir un nuevo número de serie haga clic en **Cambiar serie**. Complete el Asistente de registro para registrar BitDefender correctamente.

Nota

Para más detalles acerca del proceso de registro vaya al apartado Registro del Producto de esta Guia de Usuario.

6.2. Configuración de la Consola de Administración

Configuración de la Consola de Administración

En esta sección 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.

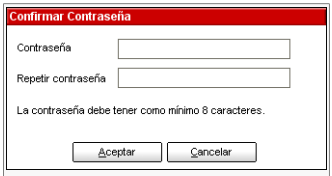
6.2.1. Configuración General

- **Activar protección por contraseña** - activa la configuración de una contraseña para proteger la configuración de la Consola de Administración de BitDefender.

Nota

Si no es el único usuario con derechos administrativos en utilizar este ordenador, es recomendado que proteja su configuración de BitDefender por una contraseña.

Si selecciona esta opción, aparecerá la siguiente ventana:



Confirmar contraseña

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

De ahora en adelante, si quiere cambiar la configuración de BitDefender, se le pedirá que introduzca la contraseña.

Importante

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

- **Mostrar Noticias de BitDefender (noticias relacionadas con la seguridad)** - muestra de vez en cuando noticias acerca de las epidemias de virus, enviadas desde los servidores de BitDefender.
- **Mostrar pop-ups (notas en pantalla)** - muestra pop-ups acerca del estado del producto.
- **Cargar BitDefender al iniciar Windows** - carga BitDefender automáticamente al iniciar el sistema.

Nota

Recomendamos mantener esta opción seleccionada.

- **Activar barra de Actividad del Análisis** - activa/desactiva la Barra de Actividad del Análisis.

- **Minimizar consola al iniciar** - minimiza la consola de administración de BitDefender después de haberse cargado al incio del sistema. Sólo el Icono de BitDefender aparecerá en la Bandeja del Sistema.

6.2.2. Configuración del Informe de Virus

- **Enviar informe de virus** - permite enviar automáticamente alertas acerca de estos virus a los Laboratorios BitDefender. 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, y no serán empleados con fines comerciales. Los datos proporcionados incluirán solamente el nombre del país y del virus y serán utilizados exclusivamente para crear informes y estadísticas.

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

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

6.2.3. Configuración del Skin

Le permite seleccionar el color de la Consola de Administración. La apariencia representa la imagen en la ventana de la interfaz. Para seleccionar una nueva apariencia haga clic en el correspondiente marco.

6.2.4. Importar/Exportar Configuración

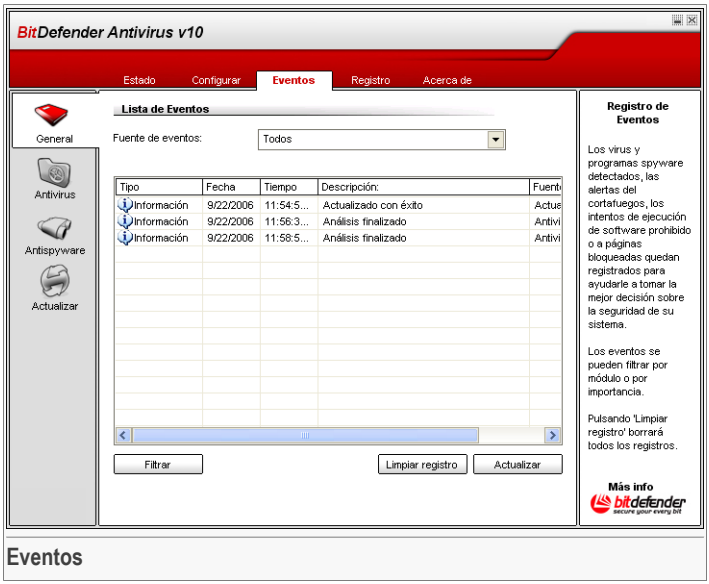
Utilice los botones **Guardar las configuraciones** / **Cargar las configuraciones** para guardar/importar las configuración hechas para BitDefender a otro destino. De este modo podrá utilizar las mismas configuraciones después de reinstalar o reparar el programa BitDefender.

Importante

Sólo los usuarios con derechos administrativos pueden guardar y cargar las configuraciones.

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

6.3. Eventos



Eventos

En esta sección se muestran todos los eventos generados por BitDefender.

Hay 3 tipos de eventos: **Información**, **Advertencia** y **Crítico**.

Ejemplos de eventos:

- **Información** - cuándo fue escaneado un e-mail;
- **Advertencia** - cuándo fue detectado un archivo sospechoso;
- **Crítico** - cuándo fue detectado un archivo infectado.

Para cada evento se le ofrece la siguiente información: la fecha y la hora en la que ocurrió un evento, una pequeña descripción de su fuente (**Antivirus**, **Cortafuego**, **Antispyware** or **Actualización**). Haga doble clic en un evento para ver sus propiedades.

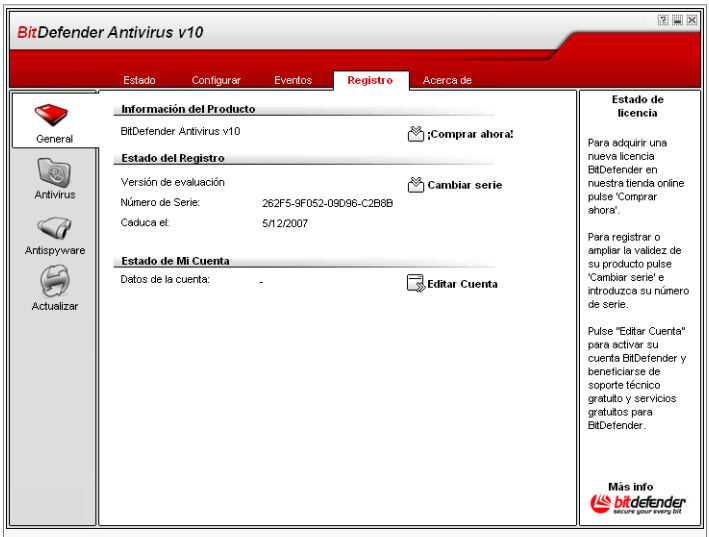
Puede filtrar estos eventos de dor formas (por tifo o por fuente):

- Haga clic en **Filtrar** para seleccionar qué tipo de eventos mostrar;
- Seleccione la fuente del evento desde el menú desplegable;

Si la Consola de gestión está abierta en la sección de **Eventos** y al mismo tiempo ocurre un evento, debe hacer clic en **Actualizar** para ver ese evento.

Para eliminar todos los eventos de la lista haga clic en **Limpiar registro**, y a continuación haga clic en **Si** para confirmar su elección.

6.4. Registro del Producto



Registro del Producto

Esta sección contiene información acerca de su producto BitDefender (estado del registro, ID del producto, fecha de caducidad) y de su cuenta de BitDefender. Aquí puede registrar su producto y configurar su cuenta de BitDefender.

Haga clic en el botón **Comprar ahora** para obtener un número de serie desde la tienda online de BitDefender.

Haciendo clic en **Cambiar Serie** puede registrar el producto, cambiar el número de serie o los detalles de su cuenta. Para configurar su cuenta de BitDefender haga clic en **Editar Cuenta**. En ambos casos, se iniciará el Asistente de Registro.

6.4.1. Asistente de Registro

El asistente de registro consta de 5 pasos.

Paso 1/5 - Bienvenido al Asistente de Registro de BitDefender

Ventana de Bienvenida

Haga clic sobre **Siguiente**.

Paso 2/5 - Registrar BitDefender

Registro

Seleccione **Registrar el Producto** para registrar **BitDefender Antivirus v10**. Escriba el número de licencia en el campo **Cambiar serie**.

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

Haga clic sobre **Siguiente**.

Paso 3/5 - Crear una cuenta de BitDefender

Creación de la Cuenta

No tengo una cuenta de BitDefender

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

Escriba una dirección de e-mail válida en el campo **Correo**. Piense en una contraseña y escríbala en el campo **Contraseña**. Vuelva a escribir la contraseña en el campo **Rescribir la contraseña**. Utilice la dirección de e-mail y la contraseña para iniciar su sesión en http://myaccount.bitdefender.com.

Nota

La contraseña debe contener 4 caracteres como mínimo.

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

Importante

Por favor, active su cuenta antes de continuar con el siguiente paso.

Si no quiere crear ninguna cuenta de BitDefender, haga clic en **Omitir este paso**. También omitirá el siguiente paso del asistente.

Haga clic en **Siguiente** para continuar.

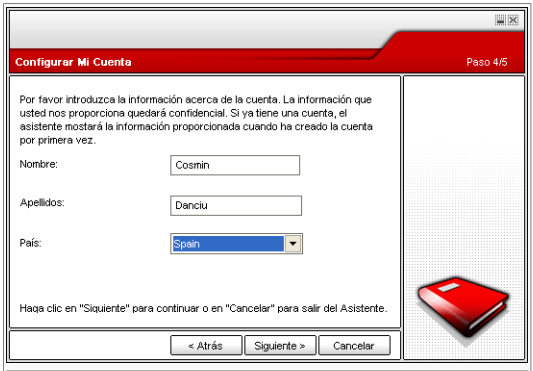
Ya tengo una cuenta de BitDefender

Si ya dispone de una cuenta activa, indique la dirección de e-mail y la contraseña de su cuenta. Si la contraseña indicada es incorrecta, se le volverá a solicitar cuando pulse en **Siguiente**. Haga clic en **Ok** para introducir de nuevo la contraseña o pulse en **Cancelar** para salir del Asistente.

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

Haga clic en **Siguiente** para continuar.

Paso 4/5 - Introducir los Detalles de la Cuenta



Detalles de la Cuenta

Nota

No realizará este paso si ha seleccionado **Omitir este paso** en el tercer paso.

Escriba su nombre y apellido y seleccione su país.

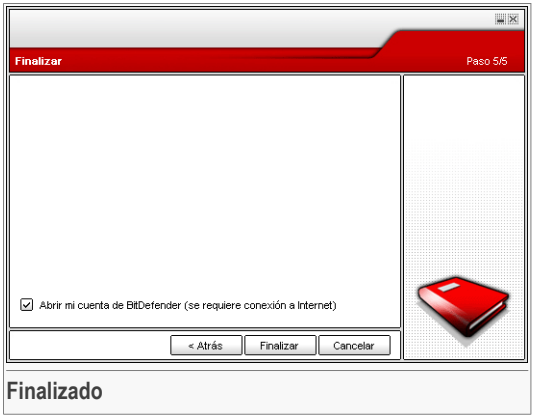
Si ya tiene una cuenta, el asistente mostrará la información que ha proporcionado anteriormente, en caso de que exista. Aquí también puede modificar esta información si lo desea.

Importante

Los datos que introduzca aquí serán confidenciales.

Haga clic sobre **Siguiente**.

Paso 5/5 - Ver Resumen



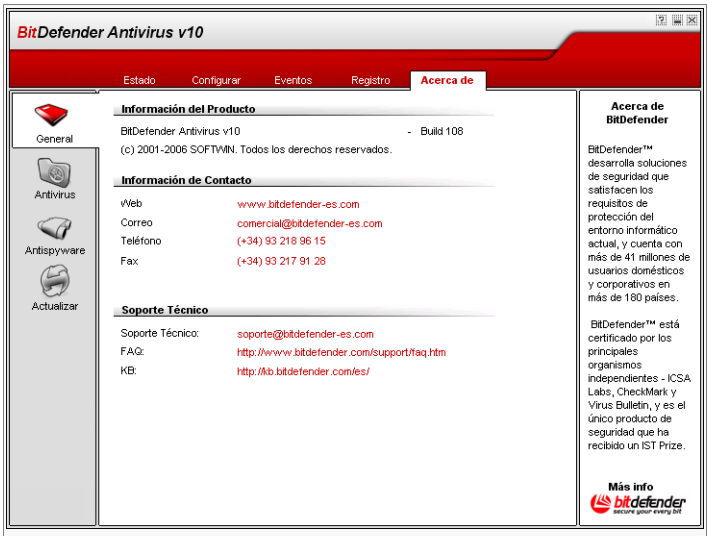
Finalizado

Este es el último paso del asistente de configuración. Puede realizar cualquier cambio volviendo a los pasos anteriores (haga clic en **Atrás**).

Si no quiere hacer ningún cambio haga clic en **Finalizar** para salir del asistente.

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

6.5. Acerca de



Información general

Aquí puede encontrar la información de contacto y detalles acerca del producto.

BitDefender™ es un fabircante pionero que desarrolla de soluciones de seguridad para satisfacer los requisitos de protección del entorno informático actual. La compañía ofrece una de las líneas más rápidas y más efectivas de software de seguridad, creando nuevos estándares para la detección y mitigación oportuna de las amenazas. BitDefender™ ofrece productos y servicios a más de 41 usuarios en más de 180 países de todo el mundo.

BitDefender™ Antivirus está certificado por los más prestigiosos laboratorios del mundo - **ICSA Labs**, **CheckMark** y **Virus Bulletin**, y es el único producto de seguridad premiado por la **Comisión Europea de TI**.

Puede obtener más información sobre BitDefender visitando: http://www.bitdefender-es.com

7. Módulo Antivirus

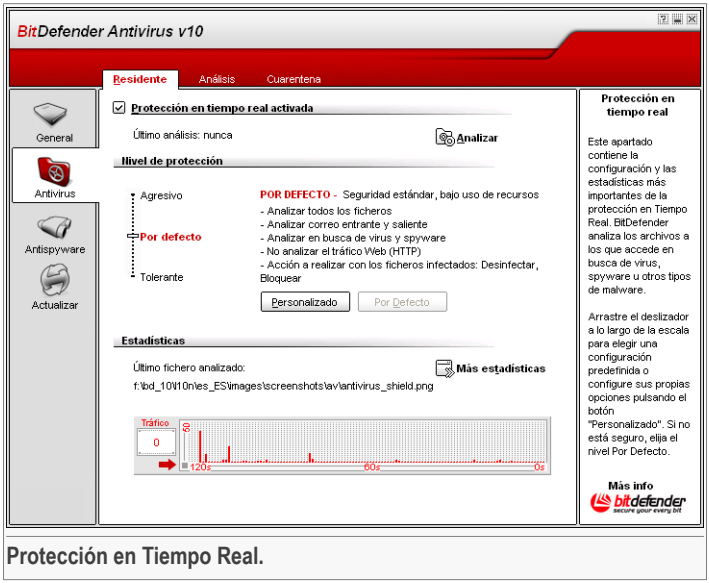
El apartado **Antivirus** de esta guía comprende los siguientes temas:

- Análisis en Tiempo Real
- Análisis Bajo Demanda
- Cuarentena

Nota

Para más detalles acerca del módulo **Antivirus** consulte la descripción del "*Módulo Antivirus*" (p. 27).

7.1. Análisis en Tiempo Real



Protección en Tiempo Real.

En este apartado puede configurar la **Protección en Tiempo Real** y puede visualizar información acerca de su actividad. La **Protección en Tiempo Real** mantiene su ordenador seguro analizando los mensajes de correo electrónico, las descargas y todos los archivos a los que se accede.

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

En la parte inferior de esta sección podrá ver las estadísticas de la **Protección en Tiempo Real** acerca de los ficheros y los mensajes de correo analizados. Haga clic en **Más estadisticas** si quiere ver una ventana con más explicaciones acerca de estas estadísticas.

7.1.1. Nivel de Protección

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

Hay 3 niveles de seguridad:

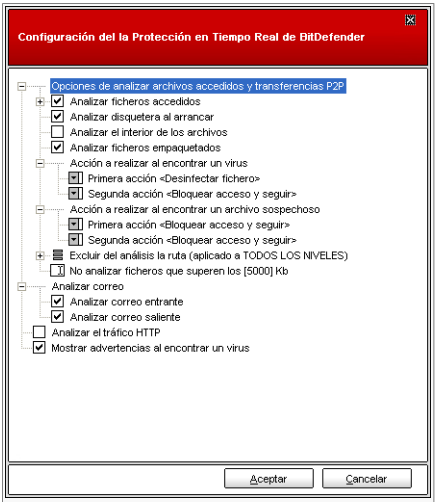
Nivel de Protección	Descripción
Tolerante	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. Los programas y los correos entrantes son analizados sólo por virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se encuentran 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 correos entrantes&salientes son analizados por virus y spyware. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se encuentran 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 y correos entrantes&salientes y el tráfico de web se analiza por virus y spyware. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las

Nivel de Protección	Descripción
	acciones que se realizan cuando se encuentran 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**.

Los usuarios avanzados querrán aprovechar las opciones de análisis que BitDefender ofrece. El análisis puede excluir extensiones de ficheros, carpetas o archivos que Usted sabe que son inofensivos. Esto puede reducir mucho la duración del análisis y mejorar el grado de reacción de su ordenador durante el análisis.

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



Configurar el Residente BitDefender

Las opciones de análisis están organizadas en la forma de un menú que se puede extender de una manera similar a los de exploración de Windows.

Haga clic en la casilla marcada con “+” para extender una opción o en aquella marcada con “-“ para restringir una opción.

Observará que ciertas opciones de análisis, aunque aparezca la seña "+" correspondiente, no se pueden extender debido a que estas opciones no han sido todavía seleccionadas. Notará que al seleccionarlas, se podrán extender.

- **Analizar ficheros accedidos y transferencias P2P** - analiza los ficheros accedidos y las comunicaciones mediante aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). Luego seleccione el tipo de ficheros a analizar.

Opción		Descripción
Analizar ficheros accedidos	**Analizar todos los ficheros**	Todos los ficheros serán analizados, independientemente de su tipo.
	Analizar sólo programas	Solamente los ficheros programa serán analizados. Es decir solamente los ficheros con las siguientes extensiones: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` y `.nws`.
	Analizar extensiones definidas	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".
	Excluir extensiones en el análisis: [ ]	Los archivos con las extensiones mencionadas por el usuario NO serán analizados. Dichas extensiones deben ser separadas por ";".
	Analizar en busca de software de riesgo	Analiza en busca de software de riesgo. Estos ficheros se tratarán como ficheros infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada. Seleccione **Omitir dialers y aplicaciones en el análisis** si quiere excluir este tipo de archivos del análisis.
Analizar disquetera en Tiempo Real		Analiza la disquetera cuando se accede a ella.
Analizar en el interior de los archivos		Para el análisis en el interior de los archivos. Con esta opción activada su ordenador será ralentizado.
Analizar ficheros empaquetados		Para el análisis de los ficheros empaquetados.

Opción		Descripción
Primera acción		Seleccione desde el menú desplegable la primera acción que desea que se realice al encontrar archivos infectados o sospechosos.
	Bloquear acceso y seguir	Si se detecta un fichero infectado, se le denegará accederlo.
	Desinfectar fichero	Para desinfectar el fichero.
	Eliminar fichero	Borra los ficheros infectados inmediatamente y sin previa advertencia.
	Mover fichero a la cuarentena	Los ficheros infectados serán transferidos a la zona de cuarentena.
Segunda acción		Seleccione desde el menú desplegable la segunda acción que desea que se realice al encontrar archivos infectados, en caso de que la primera accion falle.
	Bloquear acceso y seguir	Si se detecta un fichero infectado, se le denegará accederlo.
	Eliminar fichero	Borra los ficheros infectados inmediatamente y sin previa advertencia.
	Mover fichero a la cuarentena	Los ficheros infectados serán transferidos a la zona de cuarentena.
No analizar ficheros que superen los [x] Kb		Introduzca el tamaño máximo de los archivos que desea que sean analizados. Si el tamaño es 0 Kb, todos los archivos serán analizados, independientemente de su tamaño.
Excluir ruta en el análisis (aplicado a TODOS LOS NIVELES)		Haga clic en el "+" correspondiente a esta opción para especificar la carpeta que será excluida del análisis. La consecuencia de este hecho será que la opción hará visible una nueva opción `Nuevo elemento`. Haga clic en la casilla correspondiente al nuevo elemento y, desde la ventana de exploración seleccione la carpeta que quiere excluir en el análisis. Los objetos seleccionados aquí se excluirán del análisis, independientemente del nivel de

Opción	Descripción
	protección seleccionado (no sólo para el nivel **Personalizado**).

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

  Las siguientes opciones están disponibles:

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

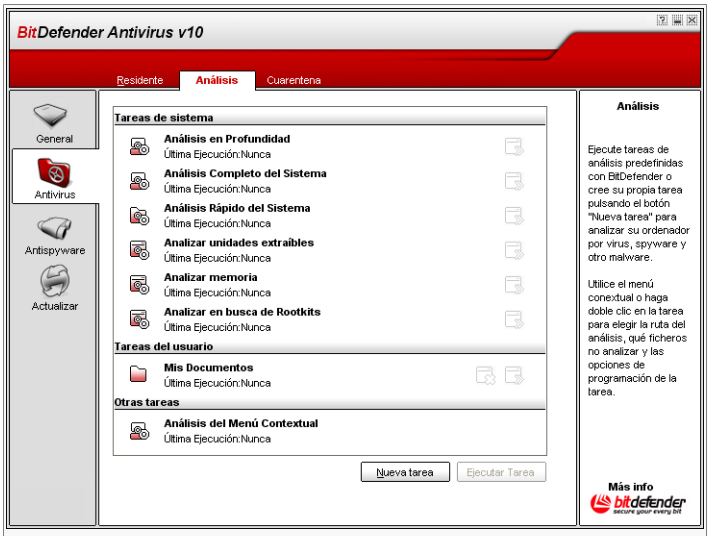
- **Analizar el tráfico HTTP** - analiza el tráfico HTTP.
- **Mostrar advertencias al encontrar un virus** - mostrará una ventana de advertencia al detectarse un virus en un fichero o correo electrónico.

  Para ficheros infectados, la ventana de advertencias contiene el nombre del virus, la ubicación, la acción realizada por BitDefender y un link a la página web donde podrá encontrar más información acerca del virus. Para mensajes infectados se mostrará también información sobre el remitente y el destinatario del correo.

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

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

7.2. Análisis Bajo Demanda



Tareas de Análisis

En este apartado puede configurar BitDefender para que analice su ordenador.

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

Sin embargo, queda un riesgo: que algún virus haya ingresado al sistema, antes de instalar BitDefender. Por esta misma razón le recomendamos analizar su ordenador inmediatamente después de instalar BitDefender. A todo esto, también consideramos que le resultaría útil efectuar análisis periódicos.

7.2.1. Tareas de Análisis

El análisis Bajo Demanda está basado en tareas de análisis. El usuario puede analizar el ordenador utilizando las tareas predeterminadas o crear sus propias tareas de análisis.

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 todo el sistema, incluso archivos comprimidos, en busca de virus y spyware.
Análisis Completo de Sistema	Analiza todo el sistema, excluyendo archivos comprimidos, en busca de virus y spyware.
Análisis Rápido del Sistema	Analiza todos los programas en busca de virus y spyware.
Análisis de unidades extraíbles	Analiza unidades extraíbles en busca de virus y spyware.
Analizar Memoria	Analiza la memoria en busca de amenazas de spyware conocidas.
Analizar en busca de Rootkits	Analiza la memoria en busca de malware oculto.

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

  Se le ofrece una tarea llamada `Mis Documentos`. Utilice esta tareas para analizar sus documentos de la carpeta `Mis Documentos`.

- **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.

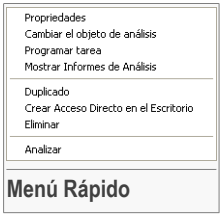
Hay tres botones disponibles en la parte derecha de cada tarea:

- **Tarea Programada** - indica que la tarea seleccionada está programada para después. Haga clic en este botón para ir al apartado Programador desde la ventana **Propiedades** donde puede modificar esta configuración.
- **Eliminar** - elimina la tarea seleccionada.

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

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

7.2.2. Menú Rápido



Menú Rápido

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

El menú rápido dispone de los siguientes comandos:

- **Analizar** - ejecuta la tarea seleccionada, iniciando inmediatamente el análisis.
- **Cambiar el Objeto de Análisis** - abre la ventana de **Propiedades**, pestaña **Ruta de Análisis**, donde puede cambiar el objeto de análisis para la tarea seleccionada.
- **Programar Tarea** - abre la ventana de **Propiedades**, pestaña **Programador**, donde puede programar la tarea seleccionada.
- **Mostrar Informes de Análisis** - abre la ventana de **Propiedades**, pestaña **Informes de Análisis**, donde puede ver los informes generados después de haberse ejecutado la tarea.
- **Duplicar** - duplica la tarea seleccionada.

Nota

Esto es muy útil a la hora de crear nuevas tareas, ya que puede modificar las opciones de la tarea duplicada.

- **Crear un Acceso Directo en el Escritorio** - crea un acceso directo de la tarea seleccionada en el Escritorio.
- **Eliminar** - elimina la tarea seleccionada.

Nota

No está 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.

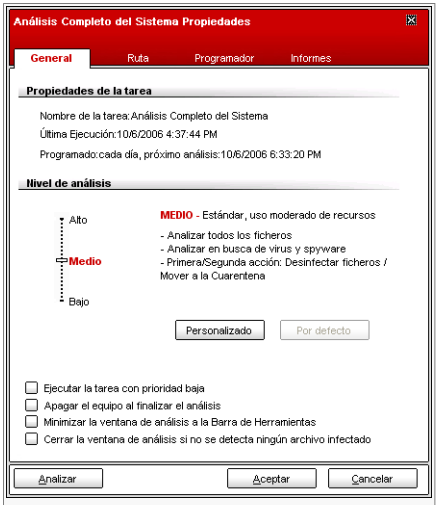
Importante

Debido a su naturaleza particular, sólo las opciones **Propiedades** y **Ver Informes de Análisis** están disponibles en la categoría **Otras tareas**.

7.2.3. Propiedades de la Tarea de Análisis

Cada tarea de análisis tiene su ventana de **Propiedades**, dónde puede configurar las opciones de análisis, el objeto de análisis, programar la tarea o ver los informes. Para abrir esta ventana seleccione la tarea y haga clic en **Propiedades** (o clic con el botón derecho encima de la tarea y después clic en **Propiedades**).

Opciones de análisis



Opciones de análisis

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

Nivel de Análisis

Antes que nada, tiene que elegir el nivel del análisis. Arrastre el deslizador a lo largo de la escala para elegir el nivel de análisis adecuado.

Hay 3 niveles de análisis:

Nivel de Protección	Descripción
Bajo	Ofrece un nivel razonable de eficacia de la detección. El nivel del consumo de recursos es bajo. Sólo los programas se analizan en busca de virus. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico. Las acciones que se realizan al encontrar archivos infectados son las siguientes: desinfectar archivo/trasladar a cuarentena.

Nivel de Protección	Descripción
Medio	Ofrece un nivel bueno de eficacia de la detección. El nivel del consumo de recursos es moderado. Todos los archivos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico. Las acciones que se realizan al encontrar archivos infectados son las siguientes: desinfectar archivo/trasladar a cuarentena.
Alto	Ofrece un nivel alto de eficacia de la detección. El nivel del consumo de recursos es alto. Todos los archivos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico. Las acciones que se realizan al encontrar archivos infectados son las siguientes: desinfectar archivo/trasladar a cuarentena.

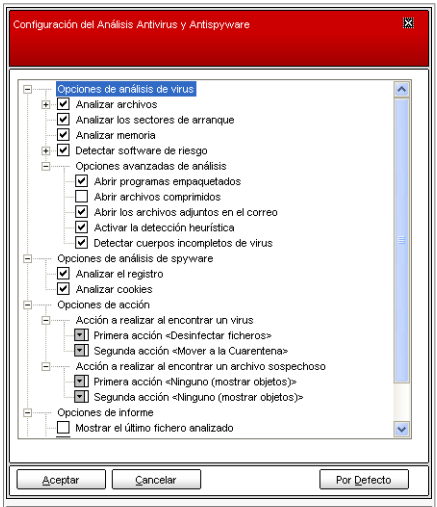
Importante

La tarea **Analizar en busca de rootkits** tiene los mismo niveles de análisis. Sin embargo, las opciones son diferentes:

- **Bajo** - Sólo se analizarán los procesos. No se realizará ninguna acción sobre los objetos detectados.
- **Medio** - Se buscarán objetos ocultos entre los ficheros y procesos. No se realizará ninguna acción sobre los objetos detectados.
- **Alto** - Se buscarán objetos ocultos entre los ficheros y procesos. Los objetos detectados serán renombrados.

Los usuarios avanzados querrán aprovechar las opciones de análisis que BitDefender ofrece. El análisis puede excluir extensiones de ficheros, carpetas o archivos que Usted sabe que son inofensivos. Esto puede reducir mucho la duración del análisis y mejorar el grado de reacción de su ordenador durante el 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 la forma de un menú que se puede extender de una manera similar a los de exploración de Windows.

Las opciones de análisis se agrupan en cinco categorías:

- **Opciones de análisis de virus**
- **Opciones de análisis de spyware**
- **Opciones de acción**
- **Opciones de informe**
- **Otras opciones**

Haga clic en la casilla marcada con “+” para extender una opción o en aquella marcada con “-“ para restringir una opción.

Importante

Para la tarea de **análisis de Rootkits** hay 3 categorías: **Opciones de análisis de rootkits**, **Opciones de Informe**, **Otras opciones**. En la primera categoría puede elegir qué analizar (ficheros, memoria o ambos) y puede especificar la acción a realizar con objetos detectados (**Ninguno (mostrar objetos)/Renombrar ficheros**). Las dos últimas opciones son idénticas a las descritas a continuación.

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

Opción		Descripción
Analizar archivos	**Analizar todos los ficheros**	Todos los ficheros serán analizados, independientemente de su tipo.
	Analizar sólo programas	Para analizar todos los ficheros programa. Es decir, solamente los ficheros con las siguientes extensiones: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` and `nws`.
	Analizar extensiones definidas	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".
	Excluir extensiones definidas	Los archivos con las extensiones mencionadas por el usuario NO serán analizados. Dichas extensiones deben ser separadas por ";".
Analizar los sectores de arranque		Para analizar el sector de arranque del sistema.
Analizar Memoria		Analiza la memoria en busca de virus y otro malware.
Detectar software de riesgo		Analiza en busca de amenazas que no son virus, como dialers y adware. Estos ficheros se tratarán como ficheros infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada. Seleccione **Excluir aplicaciones y dialers** si quiere excluir este tipo de archivos del análisis.
Opciones avanzadas de análisis	**Abrir programas empaquetados**	Para analizar en el interior de los programas empaquetados.

Opción	Descripción
Abrir archivos	Para analizar en el interior de los archivos.
Abrir los archivos adjuntos en el correo	Para analizar en el interior de los archivos de correo electrónico.
Activar la detección heurística	Para activar el análisis heurístico de los ficheros. El propósito de este tipo de análisis es identificar nuevos virus a base de ciertos elementos y algoritmos antes de que su aparición sea de conocimiento. Considerando que este método no es 100% seguro, pueden aparecer alarmas falsas. Al detectar un fichero de este tipo, se clasificará como sospechoso. En estos casos, le recomendamos enviar el fichero para ser analizado en los laboratorios de BitDefender.
Detectar los cuerpos incompletos de virus	Detecta los cuerpos incompletos de virus.

- Determina el objetivo del análisis (registro y memoria). El análisis se realiza con las opciones definidas en la categoría **Opciones de análisis de spyware**.

Opción	Descripción
Analizar el registro	Analiza las entradas del registro.
Analizar cookies	Analiza los archivos de cookies.

- Specifica la acción sobre los ficheros infectados o sospechosos. Haga clic en la seña " + " correspondiente a la categoría **Opciones de acción** para extenderla y vea todas las acciones posibles sobre los ficheros infectados.

  Seleccione las acciones que se realizarán al detectar un fichero infectado o sospechoso. Puede definir diferentes acciones a realizar con los ficheros infectados y los ficheros sospechosos. También puede seleccionar una segunda acción en caso que la primera falle.

Acción	Descripción
Ninguno(mostrar objetos)	No se realizará ninguna acción con los ficheros infectados. Estos ficheros aparecerán en el informe de análisis.
Preguntar al usuario	Al detectarse un fichero infectado, aparecerá una ventana en la cual el usuario tiene que seleccionar la acción sobre aquel fichero. Según la importancia de aquel fichero, puede optar por su desinfección, su aislamiento en la cuarentena o su eliminación.
Desinfectar ficheros	Para desinfectar el fichero.
Eliminar ficheros	Borra los ficheros infectados inmediatamente y sin previa advertencia.
Mover ficheros a la Cuarentena	Para trasladar los archivos infectados a la cuarentena.
Renombrar ficheros	Para cambiar la extensión de los ficheros infectados. La nueva extensión de los ficheros infectados será `.vir`. Cambiando el nombre de los ficheros infectados, la posibilidad de ejecutar y, por consiguiente, de propagar la infección es eliminada. En este momento estos ficheros pueden ser guardados para análisis ulteriores.

Importante

Renombrar ficheros tiene un efecto similar en los ficheros ocultos (rootkits). La nueva extensión de los ficheros detectados será `.bd.ren`. Renombrando los ficheros detectados se elimina la posibilidad de ejecución y de propagación de una infección potencial, a la vez que puede guardar los ficheros para su examinarlos y analizarlos posteriormente.

- Specifica las opciones de creación de los ficheros de informe. Abra la categoría **Opciones de Informe** para ver todas las opciones disponibles.

Opción	Descripción
Mostrar todos los ficheros analizados	Aparecerá un listado de todos los ficheros analizados, infectados o no, y su estado. Con esta opción activada su ordenador será ralentizado.
Eliminar informes anteriores a [x] días	Éste es un campo editable que le permite indicar el tiempo máximo que debe conservarse un informe en

Opción	Descripción
	el apartado Informes . Seleccione esta opción e inserte un nuevo intervalo de tiempo. El intervalo predeterminado es de 180 días.

Nota
Los informes del análisis pueden verse el apartado Informe del módulo **Antivirus**.

- Definir las otras opciones. Abra la categoría **Otras opciones** desde la que podrá seleccionar las siguientes opciones:

Opción	Descripción
Enviar ficheros sospechosos al Laboratorio BitDefender	Se le preguntará si quiere enviar todos los ficheros sospechosos a BitDefender una vez finalice el análisis.

Si hace clic en **Por Defecto** cargará la configuración por defecto.

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

Otras Opciones

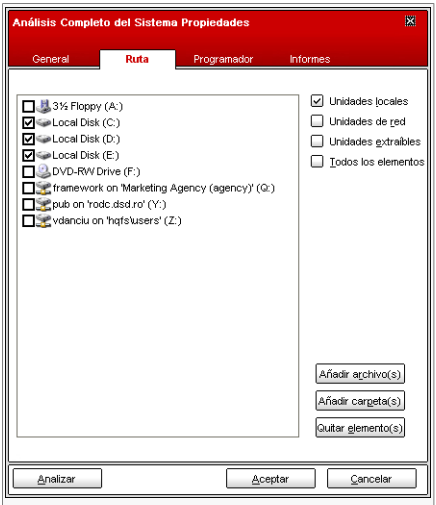
También hay disponibles una serie de opciones generales para el proceso de análisis:

Opción	Descripción
Ejecutar el análisis con prioridad baja	Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
Apagar el equipo al finalizar el análisis	Con esta opción se apagará el sistema una vez haya finalizado el proceso de análisis.
Enviar ficheros sospechosos al Laboratorio BitDefender	Se le preguntará si quiere enviar todos los ficheros sospechosos a BitDefender una vez finalice el análisis.
Minimizar ventana de análisis a la barra de tareas	Minimiza la ventana de análisis a la barra de tareas. Para visualizar la ventana haga doble clic en el icono.

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

Objetivo del Análisis

Seleccione la tarea, haga clic en **Propiedades** y a continuación haga clic en la pestaña **Ruta de análisis** para entrar a este apartado.



Objetivo del Análisis

Aquí puede indicar el objetivo del Análisis.

La sección contiene los siguientes botones:

- **Añadir archivo(s)** - abre una ventana de exploración desde la que podrá seleccionar el/los archivo(s) que desea analizar.
- **Añadir carpeta(s)** - como en el caso del botón Añadir archivo(s), haciendo clic sobre éste se abrirá una ventana de exploración desde la que podrá seleccionar la(s) carpeta(s) que quiere analizar.

Nota

También puedee arrastrar y soltar ficheros y carpetas para añadirlos a la lista.

- **Eliminar elementos** - borra del listado de análisis el fichero / directorio seleccionado anteriormente.

Nota

Solamente los ficheros y carpetas añadidos posteriormente se podrán borrar, pero no aquellos "vistos" automáticamente por BitDefender.

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

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

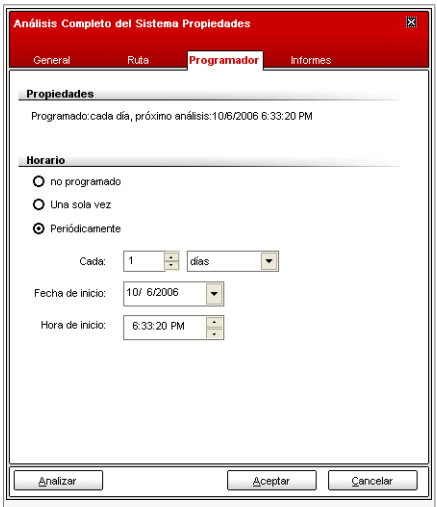
Nota

Si quiere analizar todo su sistema por 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**.

Programador

Seleccione la tarea, haga clic en **Propiedades** y a continuación haga clic en la pestaña **Programador** para entrar a este apartado.



Programador

Aquí puede ver si la tarea está programada o no, y puede modificar esta opción.

Importante

Considerando que el análisis durará cierto tiempo y que funcionará mejor si ha cerrado todos los otros programas, es aconsejable que programe este tipo de tareas con antelación, para hacerlo en aquel momento en el que no esté usando el ordenador y éste se encuentre inactivo.

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

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

Informes del análisis

Seleccione la tarea, haga clic en **Propiedades** y a continuación haga clic en la pestaña **Informes** para entrar a este apartado.

Informes del análisis

Aquí puede ver los ficheros de informe generados cada vez que se ejecuta una tarea. Cada fichero incluye información sobre su estado (infectado/desinfectado, la fecha y hora en que se realizó el análisis y un resumen (análisis finalizado).

Hay dos botones disponibles:

- **Mostrar informe** - para ver el fichero de informe seleccionado;
- **Eliminar informe** - para eliminar el fichero de informe seleccionado;

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

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

7.2.4. Tipos de Análisis Bajo Demanda

BitDefender acepta tres tipos de análisis bajo demanda:

- Análisis Inmediato - ejecutar una de las tareas de análisis de sistema o definidas por el usuario;
- Análisis Contextual - haga clic derecha en el fichero o la carpeta que quiere analizar y seleccione la opción BitDefender Antivirus v10;
- Análisis Seleccionar & Trasladar - seleccione y traslade un archivo o la carpeta sobre la zona gráfica ;

Análisis Inmediato

Para analizar su sistema o una parte puede usar las tareas de análisis predeterminadas o crear sus propias tareas de análisis. Hay 2 maneras de crear tareas de análisis:

- 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.

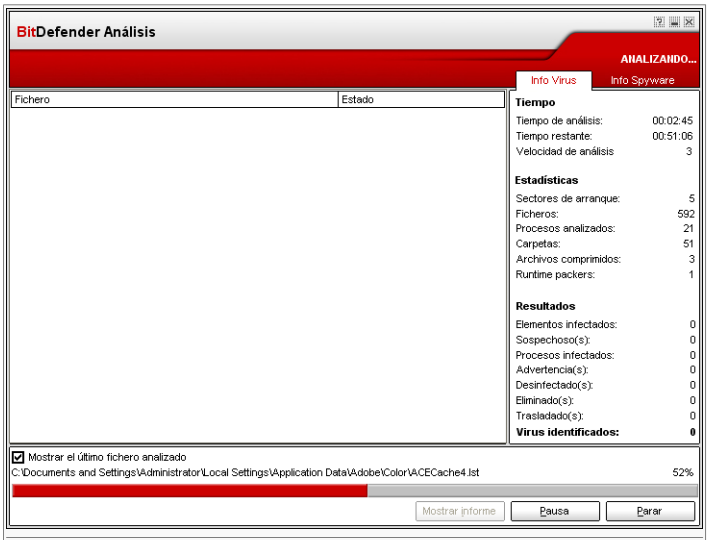
Para hacer un análisis completo de su sistema con BitDefender es necesario cerrar todos los programas abiertos. Especialmente, es importante cerrar su cliente de correo electrónico (por ejemplo: Outlook, Outlook Express o Eudora).

Antes de dejar BitDefender analizar su sistema tiene que asegurarse de que BitDefender tiene actualizadas las firmas de virus, puesto que nuevos virus son encontrados e identificados todos los días. Puede verificar cuando se ha hecho la última actualización en la parte de abajo del módulo Actualización.

Para iniciar el análisis, utilice uno de estos métodos:

- haga doble clic sobre 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 la ventana de Análisis.



Ventana de Análisis

Aparecerá un icono en la barra de tareas cuando el proceso se esté ejecutando.

Mientras está analizando, BitDefender le mostrará su progreso y le alertará cuando se detecte alguna amenaza. A la izquierda puede ver las estadísticas sobre el proceso de análisis. Dependiendo del objetivo del análisis seleccionado aparecerá información acerca de virus y/o spyware. Si existe información para ambos, haga clic en la correspondiente pestaña para aprender más sobre el proceso de análisis antivirus y antispyware.

Seleccione la cajita correpondiente a **Mostrar el último fichero analizado** y sólo la información acerca del último fichero analizado será visible.

Nota

El análisis puede durar un poco, dependiendo del tamaño de la compejidad del análisis.

Hay tres botones disponibles:

- **Parar** - aparecerá una nueva ventana, desde la cual podrá terminar el análisis del sistema. Haga clic en **Si&Salir** para salir de la ventana de análisis.

Nota

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

- **Pausa** - el análisis se detiene temporalmente y podrá seguir pulsando **Reanudar**.
- **Mostrar informe** - se abrirá el informe del análisis.

Nota

Si hace clic derecha en una tarea en ejecución, se le mostrará un menú contextual que le permite administrar la ventana de análisis. Las opciones (**Pausar / Reanudar**, **Stop** y **Parar&Cerrar**) son similares a las de los botones de la ventana de análisis.

Si la opción **Preguntar al usuario** está configurada en la ventana Propiedades, se le mostrará una ventana de alerta que le solicitará elegir la acción a realizar al encontrar archivos infectados.

Podrá ver el nombre del fichero y el nombre del virus.

Podrá seleccionar una de las siguientes opciones:

- **Desinfectar** - para desinfectar los ficheros infectados;
- **Eliminar** - para borrar los ficheros infectados;
- **Mover a Cuarentena** - para mover los ficheros infectados a la cuarentena;
- **Omitir** - para ignorar la infección. En este caso no se realizará ninguna acción sobre los ficheros infectados.

Selección de la Acción

Si desea analizar un fichero - directorio y aplicar la misma acción para todos los ficheros infectados, seleccione **Aplicar a todos**.

Nota

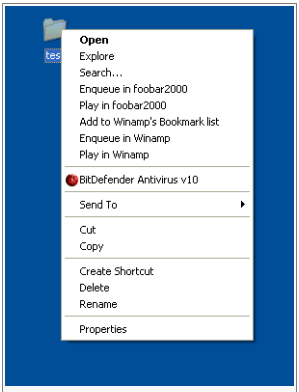
Si la opcióne **Desinfectar** no se activa, significa que el fichero no se puede desinfectar. En un caso así, la mejor solución es aislar el fichero en la cuarentena o borrarlo.

Haga clic en **Aceptar**.

Nota

El informe está guardado automáticamente en el apartado Informes del análisis de la ventana **Propiedades** de la tarea seleccionada.

Análisis contextual



Análisis contextual

Haga clic derecha en el fichero o la carpeta que quiere analizar y seleccione la opción **BitDefender Antivirus v10**.

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

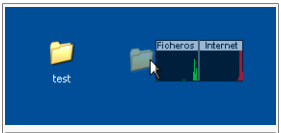
Análisis al Arrastrar&Soltar

Traslade el fichero o la carpeta que quiere analizar y suéltelo sobre la **Barra de actividad del análisis**, tal como se puede notar en las imágenes de abajo.

Trasladar el fichero

Si se detecta un fichero infectado una ventana de alerta aparecerá solicitando la acción a realizar con el fichero infectado.

En ambos casos (análisis contextual y análisis trasladar&soltar) se le mostrará la ventana de análisis



Soltar el fichero

7.2.5. Análisis de Rootkits

BitDefender quiere combatir las últimas amenazas de seguridad introduciendo un detector de rootkits conjuntamente con sus motores antivirus y antispam. Ahora

BitDefender es capaz de detectar rootkits al buscar ficheros, carpetas o procesos ocultos. Además, puede proteger a su sistema renombrando el malware que utilice técnicas rootkit.

Para analizar su ordenador en busca de rootkits, ejecute la tarea **Analizar en busca de Rootkits**. Aparecerá una ventana de análisis.

Importante

Cuando comprueba la existencia de rootkits, es sumamente recomendable configurar BitDefender para que no realice ninguna acción en los ficheros ocultos.

Al final de análisis podrá ver los resultados. Si se han detectado ficheros ocultos, márquelos con cautela: la presencia de ficheros ocultos puede indicar una posible intrusión.

Si está seguro que los ficheros detectados se tratan de malware, recomendamos cambiar la acción a **Renombrar ficheros** y ejecutar de nuevo la tarea **Analizar en busca de Rootkits**. De esta manera, los archivos ocultos quedarán bloqueados.

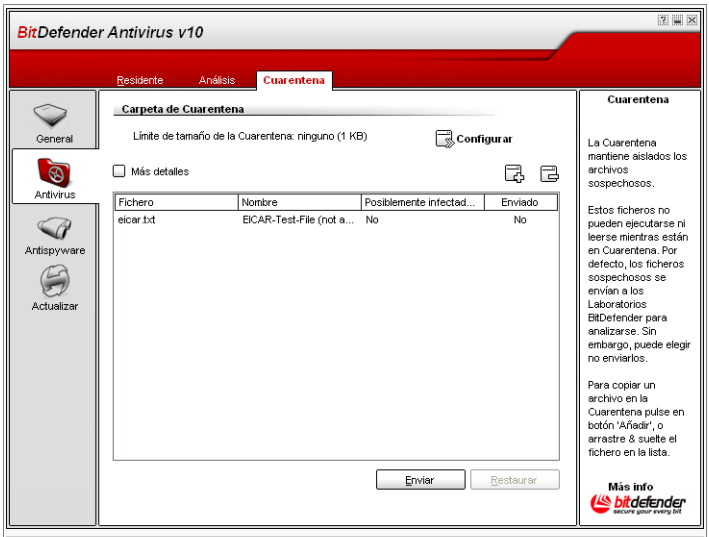
Aviso

¡NO TODOS LOS FICHEROS OCULTOS SON MALWARE! Antes de renombrar los ficheros, asegúrese que no pertenecen a ninguna aplicación válida ni al sistema. Renombrar este tipo de ficheros puede convertir su sistema inservible.

Importante

Si su sistema ha sido hackeado, sólo hay una manera segura de eliminar la intrusión: reinstalar el sistema.

7.3. Cuarentena



Cuarentena

BitDefender permite aislar los ficheros 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 ficheros para un análisis adicional en el laboratorio de BitDefender.

El componente que asegura la administración de los ficheros aislados es la zona **Cuarentena**, elemento proyectado con una función de envío automático de los ficheros infectados al laboratorio de BitDefender.

En la imagen se puede notar que la ventana **Cuarentena** contiene un listado de los ficheros aislados hasta el momento. Cada fichero contiene ciertos datos: nombre, tamaño, la fecha cuando fue aislado y respectivamente enviado al Laboratorio BitDefender. Si desea ver más información acerca de los ficheros en cuarentena, haga clic en **Más detalles**.

Nota

Cuando un virus está aislado en cuarentena no puede hacer daño alguno, al no poder ejecutar o leerlo.

Haga clic en el botón **Añadir** para añadir a la cuarentena un archivo que sospecha que es infectado. Se le mostrará una ventana y puede seleccionar el archivo desde su ubicación en el disco. De esta manera el archivo se copiará a la cuarentena. Si quiere trasladar el archivo a la cuarentena tiene que seleccionar la casilla correspondiente a **Eliminar ficheros desde la ubicación inicial**. Una manera más rápida de añadir archivos sospechosos a la cuarentena es arrastrar&soltar los archivos sobre la lista de la cuarentena.

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

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

Importante

Debe especificar algunos datos necesarios para hacer efectivo el envío de estos ficheros. Para ello, haga clic en **Configurar** y rellene los campos correspondientes a la sección **Configuración de envio**, tal como se describe a continuación.

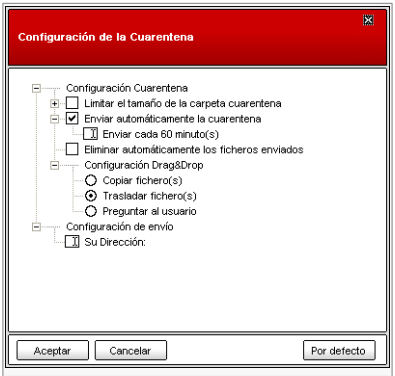
Haga clic en **Configuración** para visualizar las opciones avanzadas de la cuarentena. Aparecerá una nueva ventana:

Las opciones de la zona de cuarentena están divididas en dos categorías:

- **Configuración Cuarentena**
- **Configuración de envío**

Nota

Haga clic en la casilla marcada con "+" para extender una opción o en aquella marcada con "-" para restringir una opción.



Configurar la Cuarentena

Configuración Cuarentena

- **Limitar el tamaño de la carpeta Cuarentena** - mantiene bajo control el tamaño de la Cuarentena. El tamaño por defecto es de 12000 kB. Si desea cambiar este valor, escriba nuevo valor en la casilla correspondiente.

  Si selecciona la casilla correspondiente a **Eliminar automáticamente los ficheros antiguos**, cuando la Cuarentena esté llena y se añada un fichero nuevo, el fichero más antiguo se eliminará automáticamente para liberar espacio para el nuevo fichero.

Nota

Por defecto, la carpeta Cuarentena no tiene límite de tamaño.

- **Enviar automáticamente la cuarentena** - permite enviar automáticamente los ficheros de la cuarentena al Laboratorio BitDefender para análisis adicionales. En el campo **Enviar cada x minutos** podrá configurar el intervalo de tiempo entre dos envíos consecutivos en minutos.
- **Eliminar automáticamente los ficheros enviados** - para borrar automáticamente los ficheros de la cuarentena después de enviarlos al Laboratorio BitDefender para análisis adicionales.
- **Configuración Arrastrar&Soltar** - si utiliza el método Seleccionar & Trasladar para añadir ficheros a la cuarentena, podrá especificar la acción a realizar: copiar, trasladar o preguntar al usuario.

Configuración de envío

- **Su Dirección** - introduzca su dirección de correo si quiere recibir mensajes de parte de nuestros especialistas, acerca de los ficheros enviados para análisis.

Haga clic en **Aceptar** para guardar los cambios realizados o en **Por defecto** para cargar las configuraciones iniciales.

8. Módulo Antispyware

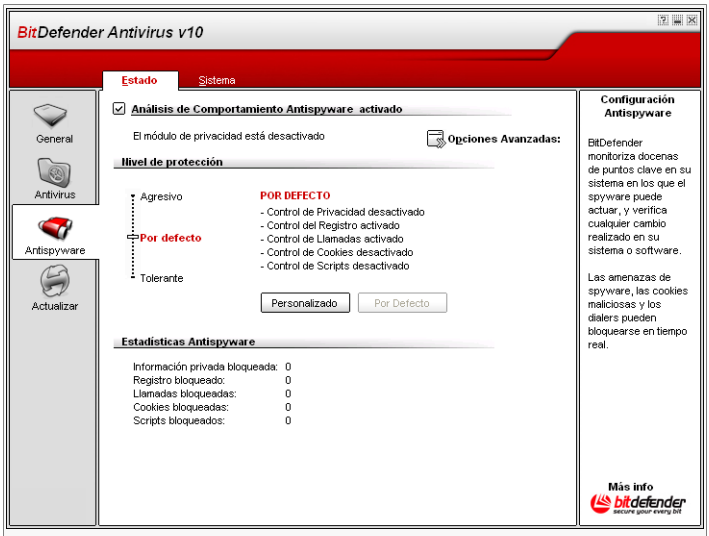
La sección **Antispyware** de esta guía del usuario contiene los siguientes temas:

- Estado Antispyware
- Configuración Avanzada - Control de Privacidad
- Configuración Avanzada - Control de Registro
- Configuración Avanzada - Control de Llamadas
- Configuración Avanzada - Control de las Cookies
- Configuración Avanzada - Control de Scripts
- Información del sistema

Nota

Para más detalles relativos al módulo **Antispyware** comrpuebe la descripción de "*Módulo Antispyware*" (p. 27).

8.1. Estado Antispyware



Estado Antispyware

En esta sección podrá configurar el módulo **Antispyware comportamental** y también podrá ver información relacionada a su actividad.

Importante

Para prevenir al spyware de que infecte su sistema mantenga el **Antispyware comportamental** habilitado.

En la parte inferior de la sección puede ver las **Estadísticas del Antispyware**.

El módulo **Antispyware** protege su equipo contra spyware a través de 5 controles de protección importantes:

- Control de Privacidad - protege sus datos confidenciales filtrando todo el tráfico HTTP y SMTP saliente según las reglas creadas en el apartado Privacidad.
- Control de Registro - se le pedirá permiso cada vez que un programa intente modificar un entrada de registro con el fin de ser ejecutada con el inicio de Windows.
- Control de Llamadas - se le pedirá permiso cada vez que un programa intente acceder al módem.

- Control de Cookies - se le pedirá permiso cada vez que una nueva página web intente guardar una cookie.
- Control de Scripts - se le pedirá permiso cada vez que una página web intente activar un script u otro contenido activo.

Para configurar las opciones para estos controles haga clic en Configuración Avanzada.

8.1.1. Nivel de Protección

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

Hay 3 niveles de seguridad:

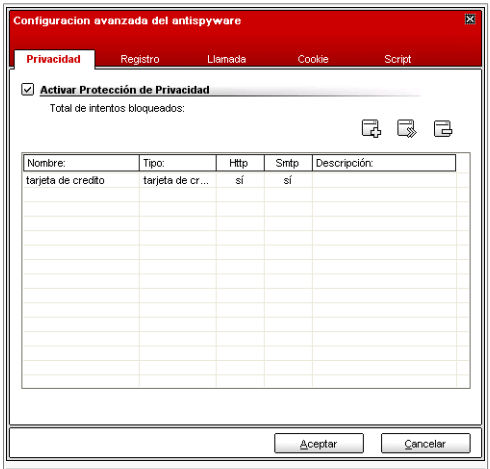
Nivel de Protección	Descripción
Tolerante	Sólo el **Control de Registro** está activado.
Por Defecto	El **Control de Registro** y **Control de Llamadas** están activados.
Agresivo	El **Control de Registro**, **Control de Llamdas** y **Control de Privacidad** están activados.

Puede personalizar el nivel de protección haciendo clic en **Personalizado**. En la ventana que aparecerá, seleccione las opciones de control Antispyware que desea activar, y haga clic en **Aceptar**.

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

8.2. Configuración avanzada - Control de Privacidad

Para acceder a este apartado haga clic en el botón **Configuración Avanzada** desde el módulo **Antispyware**, apartado Estado.



Control de Privacidad

Mantener seguros los datos confidenciales es nuestra mayor preocupación hoy en día. El robo de datos avanzó al mismo tiempo que el desarollo de la comunicación en Internet y utiliza nuevos métodos para engañar al usuario para enviar su información privada.

Independientemente de que sea su e-mail o su número de tarjeta de crédito, cuando caen en manos equivocadas, dicha información puede ser dañina para vd.: puede encontrarse a si mismo ahogandose en mensajes de spam o puede que se sorprenda al acceder a una cuenta bancaria vacia.

El **Control de Privacidad** le ayuda a mantener a salvo sus datos confidenciales. Analiza el tráfico HTTP o SMTP, o ambos, en busca de ciertos textos que usted ha configurado. Si se encuentra alguno de los textos, la página o el mensaje de correo se bloqueará.

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

8.2.1. Asistente de Configuración

El asistente de configuración es un proceso de 3 pasos.

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

Seleccionar el tipo y los datos de la regla

Introduzca el nombre de la regla en el campo editable.

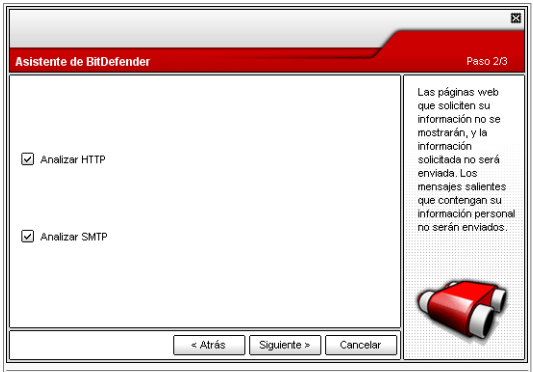
Tiene que configurar los siguientes parámetros:

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

Todos los datos que introduzca serán cifrados. Para más seguridad, no introduzca todos los datos que desee proteger.

Haga clic sobre **Siguiente**.

Paso 2/3 - Seleccionar Tráfico



Seleccionar Tráfico

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

- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea la información saliente que coincide con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (mail) y bloquea los mensajes salientes que coinciden con los datos de la regla.

Haga clic sobre **Siguiente**.

Paso 3/3 – Descripción de la regla

Describa la regla

Introduzca una corta descripción de la regla en el campo editable.

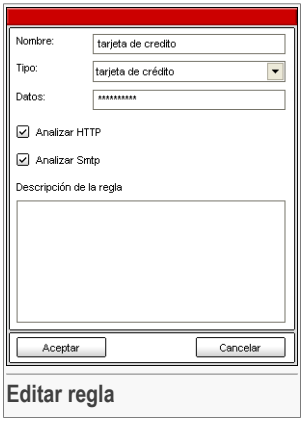
Haga clic en **Finalizar**.

8.2.2. Administrando la Reglas

Puede ver las reglas listadas en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para desactivar una regla temporalmente sin eliminarla, deseleccione la casilla correspondiente a la regla.

Para editar una regla, selecciónela y haga clic en el botón **Editar** o simplemente haga doble clic sobre la regla. Aparecerá una nueva ventana:



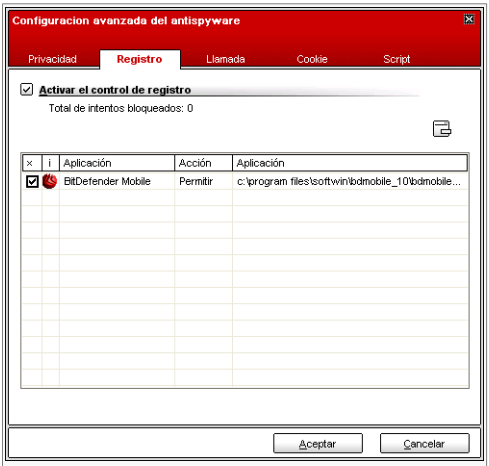
Editar regla

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

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

8.3. Configuración Avanzada - Control de Registro

Para acceder a este apartado abra la ventana **Configuración Avanzada del Antispyware** (vaya al módulo **Antispyware**, el apartado Estado y haga clic en **Configuración Avanzada**) y haga clic en la pestaña **Registro**.



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 es utilizado para definir los programas que se puedan lanzar automáticamente con cada inicio de Windows. Esta posibilidad es frecuentemente usada por los virus para lanzarse automáticamente cuando el usuario reinicie su ordenador.

El **Control del Registro** monitoriza toda la actividad del Registro Windows – acción que puede resultar muy útil para detectar Troyanos. Este módulo le advierte cada vez que un programa intenta modificar una entrada en el registro para poder ejecutarse con cada inicio del sistema.

Aviso de Registro

Para rechazar esta modificación del registro, pulse **No** o si quiere permitirla, elija **Sí**.

Si quiere que BitDefender guarde su respuesta, debe seleccionar la casilla: **Recordar esta respuesta**.

Nota

Sus respuestas serán inmediatamente incluidas en la base de datos con el listado de reglas.

Para borrar una entrada en el registro, simplemente selecciónela y pulse **Eliminar**. Para desactivar temporalmente un registro sin borrarlo, desactive la casilla correspondiente con un simple clic.

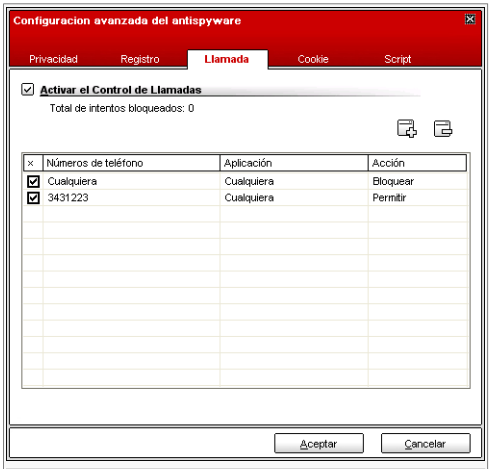
Nota

Generalmente, BitDefender le envía alertas cuando usted instala nuevos programas que deben ejecutarse después del próximo reinicio del ordenador. En la mayoría de los casos, estos programas son legítimos y de confianza.

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

8.4. Configuración avanzada - Control de Llamadas

Para acceder a este apartado abra la ventana **Configuración Avanzada de Antispyware** (vaya al módulo **Antispyware**, la pestaña Estado y haga clic en **Configuración Avanzada**) y después en la pestaña **Llamada**.



Control de llamadas

Los dialers son aplicaciones que usan los módems de los ordenadores para marcar distintos números de teléfono. Generalmente, los dialers se utilizan para acceder a varias ubicaciones tras realizar llamadas costosas.

Con el **Control de Llamadas** usted decidirá qué conexiones telefónicas desea permitir o bloquear. Esta función monitoriza todos los programas que intenten acceder al módem del ordenador y se le avisará inmediatamente, preguntándole si desea permitir o bloquear la acción:

Alerta de Llamada

Puede ver el nombre de la aplicación y el número de teléfono.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No** para crear una nueva regla de permiso, aplicada y listada en la tabla de reglas. No recibirá más esta notificación la próxima vez que la aplicación intente marcar el mismo número de teléfono.

Cada regla guardada puede ser modificada desde la sección **Llamar**.

Importante

Las reglas se muestran en el orden de sus prioridades comenzando por las más importantes. Puede cambiar este orden utilizando las opciones Arrastrar y Soltar.

Para eliminar una regla, simplemente selecciónela y pulse **Eliminar**. Para modificar los atributos de una regla, haga doble clic en el campo correspondiente. Para desactivar temporalmente una regla sin eliminarla, deseleccione la casilla correspondiente con un simple clic.

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

8.4.1. Asistente de Configuración

El asistente de configuración consta de 2 pasos.

Paso 1/2 - Seleccione la Aplicación y la Acción

Seleccionar la Aplicación y la Acción

Puede configurar los parámetros:

- **Seleccionar aplicación** - seleccione la aplicación para la cual desea crear una regla. Puede elegir una sola aplicación (clic en **Especificar aplicación**, luego en **Explorar** y seleccione la aplicación) o todas las aplicaciones (con un simple clic en **Cualquiera**).

- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La acción será permitida.
Bloquear	La acción será denegada.

Haga clic sobre **Siguiente**.

Paso 2/2 - Seleccione los Números de Teléfono

Seleccione los Números de Teléfono

Haga clic en **Especificar número de teléfono**, introduzca los números de teléfono para los cuales ha creado la regla et haga clic en **Añadir**.

Nota

Puede usar comodines en su listado de números bloqueados; Ej.: 1900* significa que todos los números que empiezan por 1900 serán bloqueados.

Haga clic en **Cualquiera** si quiere que la regla se aplique para cualquier número de teléfono. Si desea eliminar un número, selecciónelo y luego pulse **Eliminar**.

Nota

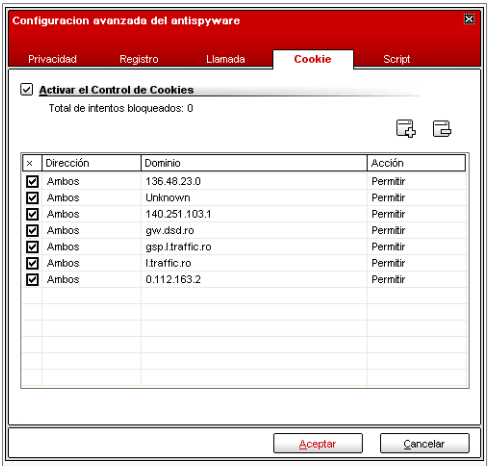
Asimismo, puede crear una regla que permita a un cierto programa marcar sólo algunos números de teléfono (como por ejemplo su Proveedor de Servicios de Internet o su servicio de fax).

Haga clic en **Finalizar**.

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

8.5. Configuración avanzada - Control de las Cookies

Para acceder a este apartado abra la ventana **Configuración Avanzada Antispyware** (vaya al módulo **Antispyware**, el apartado Estado y haga clic en **Configuración Avanzada**) y después en la pestaña **Cookie**.



Control de las cookies

Las Cookies son elementos muy comunes en Internet. Se trata de pequeños ficheros almacenados en su sistema – los sitios web, por ejemplo, crean estas cookies para recoger determinada información acerca de usted.

Las Cookies están hechas para hacerle la vida más fácil. Por ejemplo, pueden ayudar al sitio web “recordar” su nombre y preferencias, para que no tenga que introducir estos datos cada vez que visita aquella página.

Pero las cookies también pueden ser empleadas para comprometer su confidencialidad, al monitorizar sus preferencias mientras navega en Internet.

Para evitar estos casos, use nuestro **Control de cookie**. Si se lo mantiene activado, **Control de cookies** le pedirá la autorización cada vez que un nuevo sitio web intenta enviar una cookie:

Alerta de Cookie

Podrá ver el nombre de la aplicación que trata de enviar la cookie.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No** para crear una nueva regla de permiso, aplicada y listada en la tabla de reglas. No recibirá más esta notificación la próxima vez que se conecte a este mismo sitio web.

Esto le ayudará a decidir cuáles serán los sitios web de confianza.

Nota

Debido al gran número de cookies empleadas hoy por hoy en Internet, el **Control de cookies** puede resultar fastidioso de alguna manera. Recibiría muchas preguntas acerca de los sitios que intentan colocar cookies en su ordenador. Pero, en cuanto agregue los sitios de confianza al listado de reglas, el proceso de navegación en Internet volverá a ser tan fácil como antes.

Cada regla guardada puede ser modificada desde la sección **Cookies**.

Importante

Las reglas se muestran en el orden de sus prioridades comenzando por las más importantes. Puede cambiar este orden utilizando las opciones Arrastrar y Soltar.

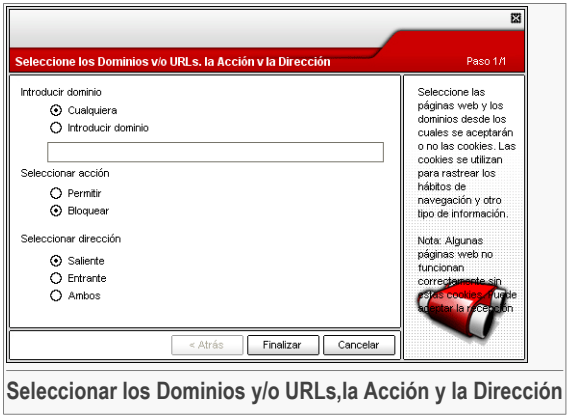
Para eliminar una regla, simplemente selecciónela y pulse **Eliminar**. Para modificar los atributos de una regla, haga doble clic en el campo correspondiente. Para desactivar temporalmente una regla sin eliminarla, deseleccione la casilla correspondiente con un simple clic.

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

8.5.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 - Seleccionar los Dominios y/o URLs,la Acción y la Dirección



Seleccionar los Dominios y/o URLs,la Acción y la Dirección

Puede configurar los parámetros:

- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

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

Tipo	Descripción
Saliente	La regla será aplicada sólo para las cookies enviadas al sitio web conectado.
Entrante	La regla será aplicada sólo para las cookies recibidas del sitio web conectado.
Ambos	La regla aplicará en ambas direcciones.

Haga clic en **Finalizar**.

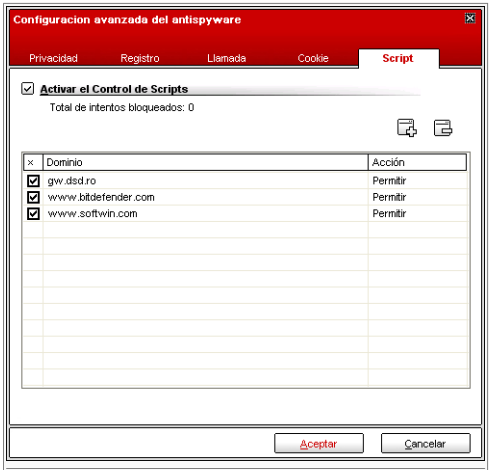
Nota

Puede aceptar cookies pero nunca enviarlas si cambia la acción a **Bloquear** y la dirección a **Saliente**.

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

8.6. Configuración avanzada - Control de Scripts

Para acceder a este apartado abra la ventana **Configuración Avanzada de Antispyware** (vaya al módulo **Antispyware**, pestaña Estado y haga clic en **Configuración Avanzada**) y después haga clic en la pestaña **Script**.

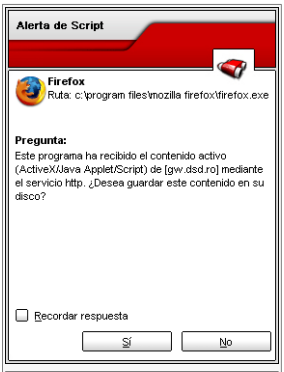


Control de script

Los Scripts y otros códigos, como los Controles ActiveX y los Applets de Java, se utilizan para crear páginas web interactivas, aunque 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 optar por ejecutar estos elementos o bien por bloquearlos.

Con el **Control del Script** usted decidirá cuáles serán los sitios web de confianza. BitDefender le pedirá una confirmación de permiso todas las veces que un sitio intente activar un script u otros contenidos activos:



Alerta de Script

Puede ver el nombre del recurso.

Seleccione la casilla **Recordar esta respuesta** y haga clic en **Si** o en **No** para crear una nueva regla de permiso, aplicada y listada en la tabla de reglas. A partir de este momento, no recibirá más notificaciones cuando el mismo sitio intente enviarle contenidos activos.

Cada regla guardada puede ser modificada desde la sección **Script**.

Importante

Las reglas se muestran en el orden de sus prioridades comenzando por las más importantes. Puede cambiar este orden utilizando las opciones Arrastrar y Soltar.

Para eliminar una regla, simplemente selecciónela y pulse **Eliminar**. Para modificar los atributos de una regla, haga doble clic en el campo correspondiente. Para desactivar temporalmente una regla sin eliminarla, deseleccione la casilla correspondiente con un simple clic.

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

8.6.1. Asistente de Configuración

El asistente de configuración consta de un paso.

Paso 1/1 - Seleccione la Dirección y la Acción

Seleccione la Dirección y la Acción

Puede configurar los parámetros:

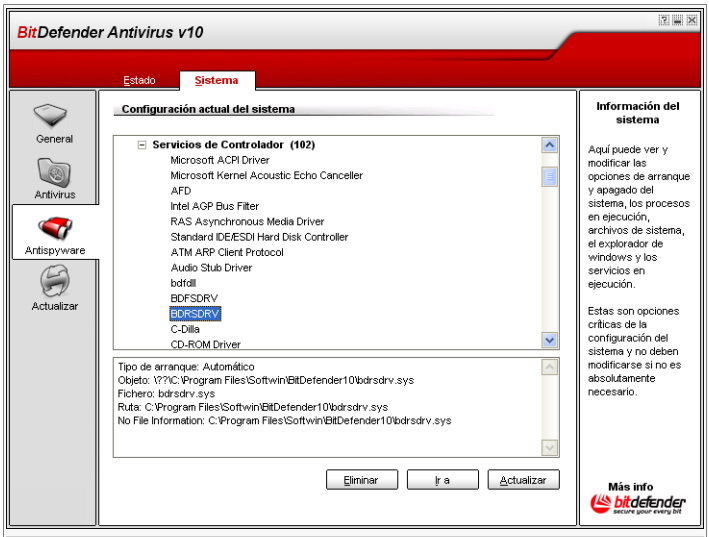
- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

Haga clic en **Finalizar**.

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

8.7. Información del Sistema



Información del Sistema

Aquí puede ver y cambiar las cofiguraciones clave de la información.

La lista contiene todos los objetos cargados cuando se inicia el sistema así como los objetos cargados por diferentes aplicaciones.

Hay tres botones disponibles:

- **Eliminar** - elimina el objeto seleccionado.
- **Ir a** - abre una ventana donde el objeto seleccionado es colocado (el **Registro** por ejemplo).
- **Actualizar** - re-abre el apartado **Sistema**.

9. Módulo Actualización

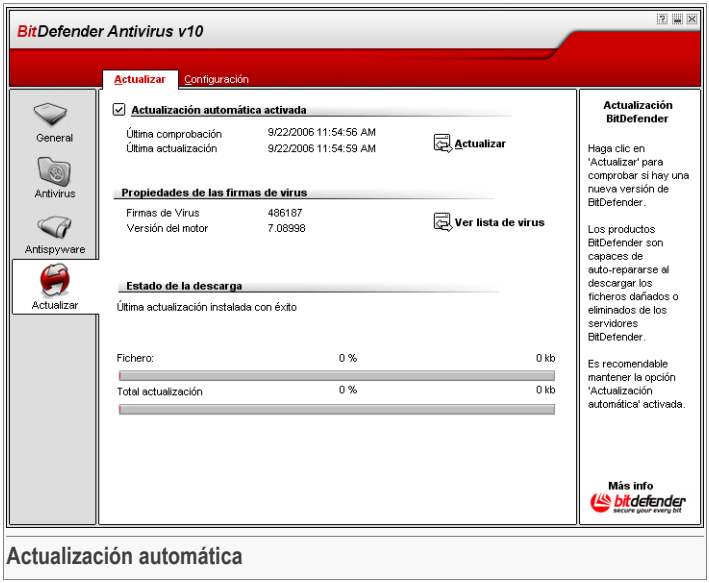
La sección **Actualización** de esta guía de usuario contiene los siguientes temas:

- Actualización automática
- Actualización manual
- Configuración de la Actualización

Nota

Para más detalles relativos al módulo **Actualización** compruebe la descripción del "*Módulo Actualización*" (p. 28).

9.1. Actualización automática



Actualización automática

En este apartado puede realizar actualizaciones o ver información relacionada con éstas.

Importante

Para estar protegido contra las últimas amenazas mantenga la **Actualización automática** activada.

Si está conectado a Internet a través de banda ancha o ADSL, BitDefender se ocupa él mismo de esto. Comprueba si hay nuevas firmas de virus cuando enciende su ordenador y cada **1 hora** después de eso.

Si se detecta alguna actualización, dependiendo de las opciones elegidas en la sección de Opciones de la Actualización Automática se le pedirá que confirme la actualización o la misma será realizada automáticamente.

La actualización automática también puede realizarse en cualquier momento haciendo clic en **Actualizar**. Este tipo de actualización también se conoce como **Actualización por petición del usuario**.

El módulo **Actualizar** se conectará al servidor de actualización de BitDefender y verificará si hay alguna actualización disponible. Si se detecta una actualización, dependiendo de las opciones elegidas en la sección de Configuración de la Actualización Manual se le pedirá que confirme la actualización o ésta será realizada automáticamente.

Importante

Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Recomendamos hacerlo lo más pronto possible.

Nota

Si está conectado a Internet a través de una connexion dial-up, entonces sería una Buena idea habituarse a actualizar BitDefender by user request.

BitDefender puede descargar las firmas de malware haciendo clic **Ver lista de virus**. Se creará un fichero HTML que contiene todas las firmas. Haga clic de nuevo en **Ver lista de virus** para ver la lista. Puede buscar la firma de un malware a través de la base de datos, haciendo clic **Lista de Virus de BitDefender** para ir a la base de datos online.

9.2. Actualización manual

Este método permite la instalación de las firmas de virus más recientes. Para instalar una actualización de la versón del producto a la versión más reciente utilice la Actualización automática.

Importante

Utilice la actualización manual cuando la actualización automática no pueda ser realizada o cuando el ordenador no estñe conectado a Internet.

Hay dos formas de realizar la actualización manual:

- Con el archivo `weekly.exe`;
- Con archivos `zip`.

9.2.1. Actualización manual con `weekly.exe`

El paquete de actualización `weekly.exe` es publicado cad viernes e incluye todas las firmas de virus y actualizaciones del motor de análisis disponibles hasta la fecha de la publicación.

Para actualizar BitDefender utilizando `weekly.exe`, siga estos pasos:

1. Descargue weekly.exe y guárdelo en su disco duro.
2. Localice el archivo descargado y haga doble clic en él para lanzar el asistente de actualización.
3. Haga clic sobre **Siguiente**.
4. Marque **Acepto los términos del contrato de licencia** y haga clic en **Siguiente**.
5. Haga clic en **Instalar**.
6. Haga clic en **Finalizar**.

9.2.2. Actualización manual con `archivos zip`

Se trata de archivos .zip del servidor de actualizaciones que contienen las actualizaciones de los motores de análisis y las firmas de virus: `cumulative.zip` y `daily.zip`.

- `cumulative.zip` se publica el lunes de cada semana e incluye todas las firmas de virus y actualizaciones de los motores de análisis hasta la fecha de publicación.
- `daily.zip` se publica cada día e incluye todas las firmas de virus y actualizaciones del motor de análisis desde el último cumulative.zip y hasta la fecha actual.

BitDefender utiliza un arquitectura basada en los servicios. Por ello, el procedimiento para reemplazar las firmas de virus es diferente dependiendo del sistema operativo:

- Windows NT-SP6, Windows 2000, Windows XP, Windows Vista.

- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Pasos a seguir:

1. **Descargue la actualización apropiada.** Si es lunes, por favor descargue el cumulative.zip y guárdelo en su disco duro. Si no es el caso, descargue el daily.zip y guárdelo en su disco duro. Si es la primera vez que actualiza utilizando el procedimiento manual, por favor descargue ambos archivos.
2. **Detenga la protección antivirus de BitDefender.**
   - **Salir de la Consola de Gestión de BitDefender.** Clic derecho en el icono de BitDefender de la System Tray y seleccione **Salir**.
   - **Abrir los Servicios.** Haga clic en **Inicio**, **Control Panel**, doble clic en **Administrative Tools** y clic en **Servicios**.
   - **Parar el servicio BitDefender Virus Shield.** Seleccione el servicio **BitDefender Virus Shield** de la lista y haga clic en **Parar**.
   - **Parar el servicio BitDefender Scan Server.** Seleccione el servicio **BitDefender Scan Server** de la lista y haga clic en **Parar**.
3. **Extraiga el contenido del archivo.** Empiece con el `cumulative.zip` cuando ambos archivos de actualización están disponibles. Extraiga el contenido en el directo `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` y acepte sobrescribir archivos existentes.
4. **Reinicie la protección antivirus de BitDefender.**
   - **Comienzo el servicio BitDefender Scan Server.** Seleccione el servicio **BitDefender Scan Server** de la lista y haga clic en **Start**.
   - **Comienzo el servicio BitDefender Virus Shield.** Seleccione el servicio **BitDefender Virus Shield** de la lista y haga clic en **Start**.
   - **Abra la Consola de Gestión de BitDefender.**

Nota

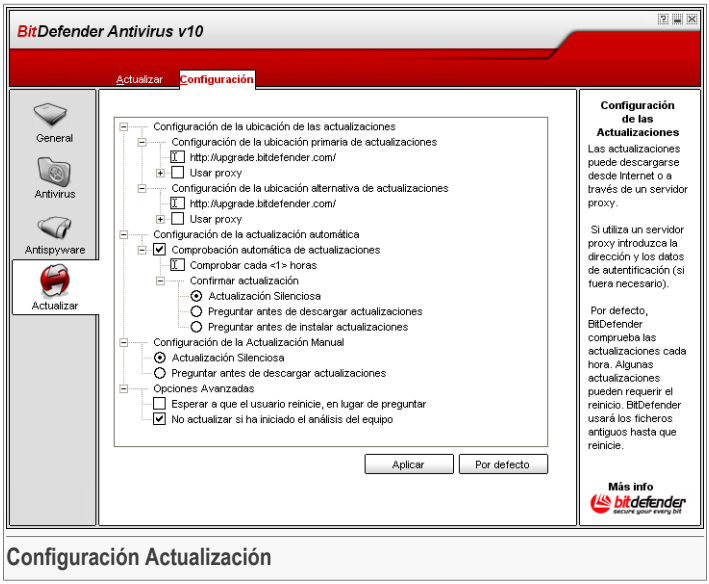
Si tiene Windows Vista instalado, se le solicitará la confirmación de la mayoría de estas acciones.

Windows 98, Windows Millennium

Pasos a seguir:

1. **Descargue la actualización apropiada.** Si es lunes, por favor descargue el cumulative.zip y guárdelo en su disco duro. Si no es el caso, descargue el daily.zip y guárdelo en su disco duro. Si es la primera vez que actualiza utilizando el procedimiento manual, por favor descargue ambos archivos.
2. **Extraiga el contenido del archivo.** Empiece con el `cumulative.zip` cuando ambos archivos de actualización están disponibles. Extraiga el contenido en el directo `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` y acepte sobrescribir archivos existentes.
3. **Reinicie el equipo.**

9.3. Configuración Actualización



Configuración Actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy.

La ventana con las opciones de actualización contiene 4 categorías (**Configuración de la Ubicación de las Actualizaciones**, **Opciones de la Actualización Automática**, **Configuración de la Actualización Manual** y **Opciones avanzadas**) organizadas en un menú extensible, similar a los de Windows.

Nota

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

9.3.1. Configuración de la Ubicación de las Actualizaciones

Para actualizaciones más rapidas y fiables, puede configurar dos localizaciones de descarga: una **Localización de descarga primaria** y una **Localización de descarga alternativa**. Para ambos debe configurar las siguientes opciones:

- **Localización de descarga** - Si está conectado a una red local que tiene firmas de virus colocadas localmente, puede cambiar la localización de las actualizaciones aquí. Por defecto esto es: http://upgrade.bitdefender.com.
- **Utilizar proxy** - En caso que la compañía utilice un servidor proxy marque esta opción. Las siguientes configuraciones deben ser especificadas:
  - **Configuración del proxy** - escriba la IP o el nombre del servidor proxy y el puerto que BitDefender utiliza para conectarse al servidor proxy.

    Importante

    Sintaxis: `nombre:puerto` o `ip:puerto`.

  - **Usuario** - introduzca un nombre de usuario reconocido por el proxy.

    Importante

    Sintaxis: `dominio\usuario`.

  - **Contraseña** - introduzca la contraseña válida para el usuario mencionado arriba.

9.3.2. Opciones de la Actualización Automática

- **Comprobar si hay actualizaciones automáticamente** - BitDefender comprueba nuestros servidores automáticamente para comprobar si hay actualizaciones nuevas disponibles.
- **Verificar cada x horas** - Define cada cuánto BitDefender comprueba si hay actualizaciones. El intervalo de tiempo por defecto son 1 hora.
- **Actualización silenciosa** - BitDefender descarga e implementa la actualización automáticamente.

- **Preguntar antes de descargar** - cada vez que hay una actualización disponible, será preguntado antes de descargarla.
- **Preguntar antes de instalar** - cada vez que una actualización haya sido descargada, se le preguntará antes de ser instalada.

Importante

Si selecciona **Preguntar antes de descargar** o **Preguntar antes de instalar** y vd. cierra&sale de la consola de gestión, la actualización automática no será realizada.

9.3.3. Configuración de la Actualización Manual

- **Actualización silenciosa** - BitDefender descarga e implementa la actualización automáticamente.
- **Preguntar antes de descargar** - cada vez que hay una actualización disponible, será preguntado antes de descargarla.

Importante

Si selecciona **Preguntar antes de descargar** y cierra&sale de la consola de gestión la actualización manual no será realizada.

9.3.4. Opciones Avanzadas

- **Esperar al reinicio, en lugar de preguntar al usuario** - Si una actualización requiere un reinicio, el producto continuará funcionando con los viejos archivos hasta que el sistema reinicie. No se le pedirá al usuario que reinicie, de forma que el proceso de actualización de BitDefender no interferirá con el trabajo del usuario.
- **No actualizar si ha iniciado el análisis del equipo** - BitDefender no se actualizará si se está realizando un análisis en ese momento. 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.

Haga clic en **Aplicar** para guardar los cambios realizados o en **Por defecto** para cargar las configuraciones iniciales.

Mejores Prácticas

10. Mejores Prácticas

El apartado **Mejores prácticas** de esta guía de usuario contiene los siguientes temas:

- Cómo proteger a su Ordenador de las Amenazas de Malware
- Cómo Configurar una Tarea de Análisis

10.1. Cómo Proteger Su Equipo contra las Amenazas de Malware

Siga estos pasos para proteger su equipo contra los virus, spyware y otro tipo de malware:

1. **Asistente de Configuración Inicial.** Durante el proceso de instalación aparecerá un Asistente. Este Asistente le ayudará a registrar su **BitDefender** y a crear una cuenta de BitDefender para beneficiarse del soporte técnico gratuito. También le ayudará a realizar tareas de seguridad importantes para su sistema.

   Importante

   Si dispone del CD de Rescate de BitDefender, analice su sistema antes de instalar BitDefender para asegurarse que no existe malware en su sistema.

2. **Actualice BitDefender.** Si no ha completado el asistente de configuración inicial durante el proceso de instalación, realice una actualización manual (diríjase al módulo **Actualización**, apartado Actualizar y haga clic en **Actualizar**).
3. **Realice un análisis completo de sistema.** Diríjase al módulo **Antivirus**, apartado Residente y haga clic en **Analizar**.

   Nota

   También puede iniciar un análisis completo del sistema desde el apartado Análisis. Seleccione la tarea **Análisis Completo del Sistema** y haga clic en **Ejecutar Tarea**.

4. **Prevenir Infección.** En el apartado **Residente**, mantenga activada la protección en tiempo real para estar protegido contra los virus, spyware u otro malware. Configure el nivel de protección del modo que mejor se ajuste a sus necesidades. Puede personalizar el nivel de protección cuando quiera haciendo clic en **Personalizar**.

Importante

Configure su BitDefender Antivirus v10 para analizar su sistema al menos una vez por semana programando la tarea **Análisis Completo del Sistema** desde el apartado Análisis.

5. **Mantenga su BitDefender actualizado.** En el módulo **Actualización**, apartado Actualizar, mantenga activada la opción **Actualización Automática** para estar protegido contra las últimas amenazas.
6. **Programe un análisis completo del sistema.** Diríjase al apartado **Análisis** y configure BitDefender para analizar su sistema al menos una vez por semana programando la tarea **Análisis Completo del Sistema**.

10.2. Cómo Configurar una Tarea de Análisis

Siga estos pasos para crear y configurar una tarea de análisis:

1. **Crear una nueva tarea.** Diríjase al apartado Análisis y haga clic en **Nueva Tarea**. Aparecerá la ventana de Propiedades.

Nota

También puede crear una nueva tarea duplicando una ya existente. Para hacerlo, haga clic con el botón derecho sobre una tarea y seleccione **Duplicar** desde el menú del acceso directo. Seleccione la copia y haga clic en el botón **Propiedades** para abrir la ventana de **Propiedades**.

2. **Establezca el nivel de análisis.** Diríjase al apartado **General** para establecer el nivel de análisis. Si lo desea, puede personalizar las opciones de análisis haciendo clic en el botón **Personalizado**.
3. **Seleccione los elementos a analizar.** Diríjase al apartado **Ruta** y elija los objetos que quiere analizar.
4. **Programe la tarea.** Si la tarea de análisis es compleja, es posible que necesite programarla para más tarde, cuando el ordenador esté inactivo. Esto ayudará a que BitDefender realice un análisis en profundidad del sistema. Diríjase al apartado **Programador** para programar la tarea.

CD de Rescate de BitDefender

BitDefender Antivirus v10 incluye un CD de autoarranque (CD de Rescate BitDefender basado en LinuxDefender) capaz de analizar y desinfectar todos los discos del equipo, antes de iniciarse el sistema operativo.

Puede utilizar el CD de rescate BitDefender cada evz que su sistema operativo no funciona correctamente debido a las infecciones de virus. Normalmente hay 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.

LinuxDefender está basado en la distribución Knoppix, e incluye las últimas soluciones de seguridad BitDefender for Linux ofreciendo protección antivirus/antispam SMTP instantánea y protección para puestos de trabajo, capaz de analizar y desinfectar todos los discos (incluyendo las particiones Windows NTFS), directorios compartidos en Samba/Windows o d puntos NFS. El CD incluye también una interfaz de configuración BitDefender.

11. General

Características principales

- Protección de correo instantánea (Antivirus & Antispam)
- Solución AntiVirus para analizar los discos
- Soporte de lectura NTFS (utilizando el proyecto Captive)
- Desinfección de los ficheros infectados para las particiones de Windows XP

11.1. Que es KNOPPIX?

Información de http://knopper.net/knoppix:

“ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

11.2. Requisitos del Sistema

Antes de iniciar LinuxDefender, debe comprobar si el equipo cumple con los siguientes requisitos.

Procesador

Compatible con procesadores x86, mínimo 166 MHz, pero no espere un gran redimiendo en este caso. Un procesador de generación i686, a 800 MHz, sería la mejor opción.

RAM

Mínimo aceptable 64MB, y recomendado más de 128 MB.

CD-ROM

LinuxDefender funciona desde el CD-ROM, y la BIOS debe permitir el incio desde el CD.

Conexión de Internet

Aunque LinuxDefender 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 poner actualizar la protección.

Resolución gráfica

Para la interfaz de administración se recomienda utilizar una resolución de 800x600.

11.3. Software incluido

El CD de Rescate BitDefender incluye los siguientes paquetes.

- BitDefender SMTP Proxy (Antispam & Antivirus)
- BitDefender Remote Admin (consola de configuración)
- BitDefender Linux Edition (analizador antivirus) + interfaz GTK
- BitDefender Documentation (en formato PDF & HTML)
- BitDefender Extras (Presentaciones, folletos)
- Linux-Kernel 2.6
- Proyecto de escritura NTFS Captive
- LUFS - Linux Userland File System
- Herramientas para la recuperación de datos y reparación del sistema
- Herramientas de seguridad de análisis de red
- Solución de copias de seguridad Amanda
- thttpd
- Analizador de tráfico de red Ethereal, IPTraf IP LAN Monitor
- Programa de auditoria de seguridad en red Nessus
- Soluciones para particiar el disco, redefinir particiones guardar y recuperar - QTParted
- Adobe Acrobat Reader
- El navegador Mozilla Firefox

11.4. Soluciones de Seguridad BitDefender para Linux

El CD LinuxDefender incluye el programa BitDefender SMTP Proxy Antivirus/Antispam for Linux, BitDefender Remote Admin (una interfaz web para configurar BitDefender SMTP Proxy) y BitDefender Linux Edition, un analizador antivirus bajo demanda.

11.4.1. BitDefender SMTP Proxy

La solución BitDefender for Mail Servers funciona bajo plataformas Linux y FreeBSD, y le proporciona seguridad de contenido a nivel de la puerta de enlace, analizando todo el tráfico de correo electrónico entrante y saliente en busca de códigos maliciosos

y spam. BitDefender for MailServers es compatible con la mayoría de las plataformas del correo electrónico existentes y certificado por “RedHat Ready".

Para configurar BitDefender SMTP Proxy, utilizando la consola BitDefender Remote Admin, debe seguir las instrucciones mencionadas a continuación.

11.4.2. BitDefender Remote Admin

Puede configurar y administrar los servicios BitDefender remotamente (una vez configurada la red) o en local siguiendo los pasos:

1. Inicie el navegador Firefox y cargue la dirección de BitDefender Remote Admin URL: https://localhost:8139 o doble clic en el acceso directo ubicado en el Escritorio de BitDefender Remote Admin)
2. Autentificarse con el usuario "bd" y la contraseña "bd"
3. Seleccione la opción "SMTP Proxy" en la parte izquierda de la ventana
4. Configure el servidor real SMTP y el puerto de escucha
5. Añadir los dominios de correo para realizar el relay
6. Añadir los dominios de red para realizar el relay
7. Seleccione "AntiSpam" para configurar los filtros
8. Seleccione "AntiVirus" para configurar las acciones a realizar al encontrarse un virus
9. Además puede configurar la opción de Advertencias por mail y las opciones de registro de log ("Logger")

11.4.3. BitDefender Linux Edition

El analizador antivirus incluido en LinuxDefender tiene un acceso directo directamente en el Escritorio. Esta versión tiene una interfaz gráfica basada en GTK+ .

Explore su disco (o unidades remotas montadas), haga clic con el botón derecho en un fichero o carpeta y seleccione "Scan with BitDefender". BitDefender Linux Edition analizará los objetos seleccionados y mostrará el historial. Para más información puede ver la documentación BitDefender ubicada en **/opt/BitDefender/lib/bdc**.

12. Cómo utilizar LinuxDefender

12.1. Iniciar y salir

12.1.1. Iniciar LinuxDefender

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 iniciarse desde el CD.

Espere que se inicie el equipo desde el CD LinuxDefender.

Ventana de inicio de Boot

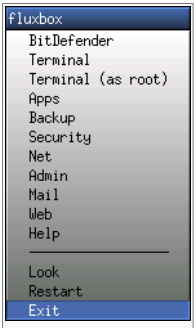
Presione F2 para más detalles. Presione F3 para más información en alemán. Presione F4 para más información en francés. Presione F5 para más detalles en español. Para comenzar el inicio rápido, con las opciones predeterminadas haga clic en ENTER.

Una vez finalizado el inicio del CD podrá ver el Escritorio y utilizar el programa LinuxDefender.

El Escritorio

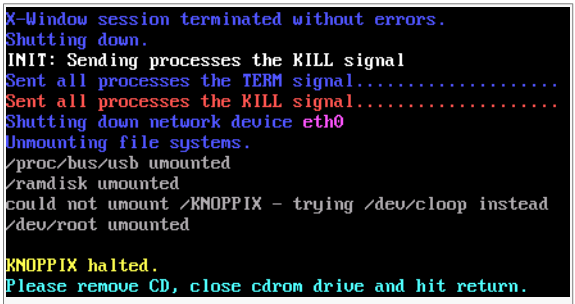
12.1.2. Salir LinuxDefender

Para salir de LinuxDefender recomendamos desmontar todas las particiones utilizando el comando **umount** umount o con clic derecho en los iconos de las particiones seleccione la opción **Unmount**. Después puede apagar el equipo seleccionando la opción **Salir** en la ventana de LinuxDefender (clic derecho en el ratón para abrirlo) o utilizando el comando **halt** en linea de comandos.



Seleccione "Salir"

Una vez finalizados los programas de LinuxDefender se mostrará una imagen similar a la siguiente. Puede extraer el CD para volver a iniciar su sistema operativo. Ahora ya puede apagar o reiniciar su equipo.



Espere este mensaje cuando apaga el equipo

12.2. Configure la conexión de 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. Abrir la ventana de LinuxDefender (clic derecho en el ratón) y seleccione la opción **Terminal** para abrir la consola.
2. Introduzca el comando **netcardconfig** para iniciar la herramienta de configuración de red.
3. Si la red utiliza DHCP, seleccione **yes** (si no está seguro pregunte a su administrador de la red). A continuación seguir con.
4. La conexión de red debe configurarse ahora automáticamente. Puede ver su IP y la configuración de red utilizando el comando **ifconfig**.
5. Si tiene una IP estática (no utiliza DHCP), seleccione la opción **No** en la pregunta sobre DHCP.
6. Siga las instrucciones que aparecen en pantalla. Si no está seguro sobre qué debe escribir, póngase en contacto con su administrador de sistema o red para más detalles.

Para comprobar que todo funciona correctamente puede hacer “ping” a nuestra web `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Si utiliza el modem para conectarse al Internet, seleccione la opción **pppconfig** desde la opción admin. de LinuxDefender. A continuación siga las instrucciones de configuración de las conexiones de Internet PPP .

12.3. Actualizar BitDefender

Los programas BitDefender incluidos en LinuxDefender utilizan el sistema ramdisk para actualizar los ficheros. De esta manera, puede actualizar todas las firmas de virus, los motores de análisis o la base de datos del módulo antispam cada vez que utiliza el CD LinuxDefender.

Asegúrense que tiene una conexión de Internet válida. Al principio debe abrir la consola BitDefender Remote Admin y seleccione la opción **Live! Update** en la parte izquierda de la ventana. Haga clic en **Actualizar ahora** para descargar todas las actualizaciones disponibles.

También puede ejecutar los comandos en línea de comandos.

```
# /opt/BitDefender/bin/bd  update
```

Todos los procesos se guardarán en el fichero predeterminado BitDefender log. Puede visualizarlo utilizando el siguiente comando.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Si para salir a Internet utiliza un servidor proxy, debe configurarlo en el apartado configuración Proxy en la ventana de **Live! Update**, sección **Configuración**.

12.4. Análisis de Virus

12.4.1. Como tener acceso a mis datos de Windows?

Soporte de escritura NTFS

El soporte de escritura NTFS es posible utilizando el proyecto Captive NTFS write project. Necesita dos controladores (driver) de instalación de Windows: `ntoskrnl.exe` y `ntfs.sys`. Actualmente, soporta sólo los controladores de Windows XP. Puede utilizar los mismos controladores para acceder a las particiones de Windows/2000/NT/2003.

Instalar los controladores NTFS

Para acceder a las particiones NTFS de Windows y tener permisos de escritura sobre ellas, necesita instalar primero los controladores de NTFS. Si no utilizan las particiones

NTFS, y utiliza las particiones FAT, necesita exclusivamente permisos de sólo lectura y puede acceder a los datos de manera similar a las particiones de Linux.

Para soportar las particiones NTFS debe instalar primero los controladores desde una ubicación segura como directorios de red compartidos, sticks USB, utilizando la opción Windows Update. También se puede actualizar en local pero no es recomendable ya que el Windows puede estar infectado.

Haga doble clic en el icono **Install NTFS Write Drivers** para ejecutar el instalador **BitDefender Captive NTFS Installer**. Seleccione la primera opción si desea instalar los controladores desde una ubicación local.

Si los controladores están en una ubicación habitual utilice la opción **Quick search** para encontrar los controladores.

También puede especificar donde encontrar los controladores. Puede descargar los ficheros desde Windows Update SP1.

Los controladores no se instalan en el disco duro, pero serán utilizados por Linux Defender para acceder a las particiones NTFS de Windows. Una vez instalados los controladores, puede hacer doble clic en los iconos de particiones NTFS para acceder a los datos. Para mejorar la administración de los datos puede utilizar la opción Midnight Commander de LinuxDefender (o escriba **mc** en la consola de línea de comandos).

12.4.2. Como realizar un análisis antivirus?

Explore sus carpetas, haga clic derecho en el fichero o los directorio deseados y seleccione **Send to**. A continuación seleccione **BitDefender Scanner**.

También puede utilizar el siguiente comando estando conectado como root en la terminal. **BitDefender Antivirus Scanner** comenzará a analziar los ficheros o las carpetas seleccionados.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Después haga clic en **Start Scan**.

Si desea configurar las opciones del antivirus seleccione **Configure Antivirus** de la parte izquierda de la ventana del programa.

12.5. Crear una protección de mail instantánea

Puede utilziar LinuxDefender para crear una solución de análisis de mails, sin necesidad de instalar ningún software o de modificar el servidor de correo. La idea

es de poder delante del servidor de correo la protección Linux Defender para analizar todo el trafico em búsqueda de virus y spam. Una vez analizados los mensajes se enviarán al servidor de correo real.

12.5.1. Requisitos

Necesita un ordenador con un procesador superior a Pentium 3, con mínimo 256MB de RAM y una unidad de CD/DVD bootable. El sistema LinuxDefender recibirá todo el tráfico SMTP enviado al servidor real. Para esto debe realizar unos pequeños cambios.

1. Cambiar la IP del servidor de correo real y asignadle la IP anterior al sistema de protección LinuxDefender
2. Cambiar las DNS y las entradas MX de sus dominios para que apunten al sistema LinuxDefender
3. Configure sus clientes de correo para utilizar el nuevo sistema LinuxDefender como servidor SMTP
4. Cambia las reglas de su cortafuego para reenviar / redireccionar el tráfico SMTP al sistema LinuxDefender

La ayuda de LinuxDefender no explica ninguna de las cuestiones anteriores. Para más información puede consultar las documentaciones Linux Networking guides y Netfilter documentation.

12.5.2. Protección de email

Inicie su CD LinuxDefender y espere a cargarse su sistema.

Para configurar BitDefender SMTP Proxy, haga doble clic en la opción **BitDefender Remote Admin** ubicada en el Escritorio. Se mostrará la siguiente ventana. Utilice el usuario `bd` y la contraseña `bd` para conectarse a la consola de administración.

Una vez conectado podrá configurar las opciones BitDefender SMTP Proxy.

Seleccione **SMTP Proxy** para configurar el servidor de mail real que desea proteger contra virus y spam.

Seleccione la opción **Email domains** e introduzca todos los dominios de correo autorizados a recibir mensajes.

Haga clic en **Add Email Domain** o **Add Bulk Domains** para seguir las instrucciones de configuración del relay de los dominios de correo.

Seleccione **Net domains** para introducir las direcciones de red autorizados a recibir correos.

Haga clic en **Add Net Domain** o **Add Bulk Net Domains** para seguir las instrucciones de configuración del relay de los dominios de la red.

Seleccione **Antivirus** desde la parte izquierda de la ventana, para configurar las acciones a realizar al detectarse virus y otras opciones del antivirus.

Ahora, todo el tráfico SMTP será analizado por BitDefender. Por defecto, todos los mensajes infectados serán desinfectados o eliminados y todos los mensajes de spam detectados por BitDefender se marcarán en el asunto con la palabra `[SPAM]`. En el cabezal de los mensajes analizados se añadirá el texto (`X-BitDefender-Spam: Yes/No`).

12.6. Realice una auditoria de seguridad de la red

Aparte de solución anti-malware, recuperación de datos y opciones de filtrado, LinuxDefender incluye una serie de herramientas capaces de realizar una auditoria compleja de seguridad de la red. Utilizando las herramientas de seguridad de Linux Defender se pueden realizar análisis forenses de los equipos afectados. Lea este pequeño manual para aprender como realizar una auditoria de seguridad de su red.

12.6.1. Compruebe la existencia de rootkits

Antes de comenzar a analizar vulnerabilidades en otros equipos de la red, asegúrense de que el equipo Linux Defender no está afectado. Puede realizar un análisis de virus según las instrucciones presentadas anteriormente y también puede buscar rootkits de UNIX.

Primero de todo, debe montar las particiones de disco, haciendo doble clic sobre sus iconos ubicados en el Escritorio o utilizando el comando **mount** en la consola de comandos. A continuación haga doble clic en el icono **ChkRootKit** o ejecute el comando **chkrootkit** desde la consola utilizando los parametros `-r NEWROOT` para especificar el nuevo / (root) directorio del equipo.

```
# chkrootkit  -r  /dev/hda3
```

Si se detecta algún rootkit, chkrootkit lo mostrará en un texto marcado en **negrita**.

12.6.2. Nessus - Analizador de Red

Nessus es el escáner de vulnerabilidades de código abierto más popular del mundo, y se utiliza en más de 75,000 organizaciones de todo el mundo. Algunas de las empresas más grandes ahorran costes de forma significativa usando Nessus para auditar los dispositivos y aplicaciones críticos para el negocio.

—www.nessus.org

Nessus puede analizar remotamente todos los equipos de la red en búsqueda de vulnerabilidades. También recomienda tomar ciertas medidas para disminuir el riesgo y evitar las incidencias de seguridad.

Haga doble clic en el icono **Nessus Security Scanner** ubicado en el Escritorio o ejecute el comando **startnessus** desde la terminal. Espere que se muestren las siguientes ventanas. Dependiendo de la configuración del equipo, puede tardar más de 10 minutos en cargarse ya que tiene una gran base de datos de vulnerabilidades. Debe utilizar el usuario y la contraseña `knoppix` para logarse.

Seleccione **Target selection** e introduzca la IP o el nombre del equipo que desea analizar. Asegúrese que ha configurado todas las opciones de análisis acorde con la configuración de su sistema o red antes de iniciar un análisis, para ahorrar ancho de banda y recursos, y obtener unos resultados óptimos. Después haga clic en **Start the scan**.

Una vez finalizado el análisis el programa Nessus mostrará las vulnerabilidades y las recomendaciones a realizar. Puede guardar el informe en varios formatos, incluyendo el HTML para visualziarlo en el navegador web.

12.7. Compruebe el estado de la memoria RAM

Es habitual que muchos problemas con los ordenadores se deben al mal estado de la memoria RAM. Puede testear la integridad de los módulos de memoria RAM utilizando la aplicación **memtest** descrita a continuación.

Inicie el sistema Linux Defender desde el CD. Escriba **memtest** el inicio y presione Intro.

El programa Memtest se iniciará inmediatamente y realizará unos test de análisis de la RAM. Puede configurar que test realizar y ptras opciones de Memtest presionando la tecla `c`.

Un análisis completo con Memtest puede durar hasta 8 horas, dependiendo de las caracteristicas del equipo y de la memoria RAM. Se recomienda configurar Memtest para realziar todos los tests en busqueda de errores de la RAM. Puede salir en cualquier momento presionando la tecla `ESC`.

Si desea comprar un nuevo hardware se recomienda utilizar Linux Defender para comprobar posibles errores o incompatibilidades.

Conseguir Ayuda

13. Soporte

13.1. Departamento de soporte

Como cualquier compañía orientada a satisfacer las necesidades de sus clientes, SOFTWIN 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 SOFTWIN, el interés por ahorrar tiempo y dinero a nuestros clientes facilitándoles los productos más avanzados al mejor precio siempre ha sido una prioridad. Además, pensamos que para tener un negocio de éxito es necesaria una comunicación eficiente y el compromiso de ofrecer excelentes servicios a nuestros clientes.

Puede contactar con nosotros por correo elctrónico a través de la siguiente dirección <soporte@bitdefender-es.com>. 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.

13.2. Ayuda On-line

13.2.1. 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.

13.3. Información de contacto

SOFTWIN aprecia 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.

13.3.1. Direcciones Web

Departamento Comercial: <comercial@bitdefender-es.com>
Soporte técnico: <soporte@bitdefender-es.com>
Documentación: <documentation@bitdefender.com>
Programa de Partners: <partners@bitdefender-es.com>
Marketing: <marketing@bitdefender-es.com>
Relaciones con la Prensa: <prensa@bitdefender-es.com>
Oportunidades de Trabajo: <jobs@bitdefender-es.com>
Envío de Virus: <virus@bitdefender-es.com>
Envío de Spam: <spam_submission@bitdefender.com>
Notificar abuso: <abuso@bitdefender-es.com>
Página web del producto: http://www.bitdefender-es.com
Productos en ftp: ftp://ftp.bitdefender.com/pub
Distribuidores locales: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

13.3.2. Filiales

Las oficinas de BitDefender están listas a responder a cualquier pregunta relativa a sus áreas de operación, tanto a nivel comercial como en asuntos generales. Sus direcciones y contactos están listados a continuación.

Alemania

Softwin GmbH
Headquarter Europa Occidental
Karlsdorferstrasse 56
88069 Tettnang
Alemania
Teléfono: 07542/94 44 44
Fax: 07542/94 44 99
E-mail: <info@bitdefender.com>
Comercial: <sales@bitdefender.com>

Web: http://www.bitdefender.com
Soporte técnico: <support@bitdefender.com>

Reino Unido e Irlanda

One Victoria Square
Birmingham
B1 1BD
Teléfono: +44 207 153 9959
Fax: +44 845 130 5069
E-mail: <info@bitdefender.com>
Comercial: <sales@bitdefender.com>
Web: http://www.bitdefender.co.uk
Soporte técnico: <soporte@bitdefender-es.com>

España

Constelación Negocial, S.L
C/ Balmes 191, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Comercial: <comercial@bitdefender-es.com>
Teléfono: (+34) 93 218 96 15
Fax: (+34) 93 217 91 28
Sitio web del producto: http://www.bitdefender-es.com

Estados Unidos

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Soporte técnico: <soporte@bitdefender-es.com>
Atención al Cliente: 954-776-6262
Web: http://www.bitdefender.com

Rumania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Soporte Técnico: <suport@bitdefender.ro>
Comercial: <sales@bitdefender.ro>

Teléfono: +40 21 2330780
Fax: +40 21 2330763
Página web de los Productos: http://www.bitdefender.ro

Glosario

ActiveX

ActiveX es un modo de escribir programas de manera que otros programas y el sistema operativo puedan usarlos. La tecnología ActiveX es empleada por el Microsoft Internet Explorer para hacer páginas web interactivas que se vean y se comporten como programas más que páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, apretar botones, interaccionar de otras formas con la página web. Los mandos de ActiveX se escriben generalmente usando Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desaprueban desalientan el empleo de ActiveX en Internet.

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas 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, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar preocupación acerca de su privacidad a aquellos usuarios que no son plenamente conscientes de los términos de la licencia.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Backdoor

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, 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 hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

Navegador

Forma abreviada de Navegador de Web, aplicación de software empleada para ubicar y cargar las páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer, sendos navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos incluyen información multimedia: sonido e imágenes, aunque requieran plugins para ciertos formatos.

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Descarga

Para copiar información (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

E-mail

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Extensión de un fichero

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Varios sistemas operativos usan extensiones de ficheros (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Podemos indicar "c" para el lenguaje C, "ps" para PostScript, "txt" para un texto arbitrario.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de los virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva versión de un virus ya existente. Sin embargo, ocasionalmente puede notificar sobre la existencia de unos códigos sospechosos en los programas normales, generando el "falso positivo".

IP

Internet Protocol - pertenece a la gama de protocolos TCP/IP y es responsable. Toda la comunicación en Internet se realiza mediante los dos protocolos para el intercambio de información: El Transmission Control Protocol (TCP, o Protocolo de Control de Transmisión) y el Internet Protocol (IP, o Protocolo de Internet). Estos protocolos son conocidos, en forma conjunta, como TCP/IP. No forman un

único protocolo sino que son protocolos separados, pero sin embargo están estrechamente comunicados para permitir una comunicación más eficiente.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Virus de Macro

Es un tipo de virus informático que se encuentra codificado como una macro incluida en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir una macro en un documento y también que la macro se ejecute cada vez que se abra el documento.

Cliente de Correo

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico

Este método de análisis se basa en firmas de virus especificas. La ventaja del análisis no heurístico es que no se le puede engañar por algo que parecería ser un virus. Por consiguiente, no genera alarmas falsas.

Programas empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Ruta

Las direcciones exactas de un fichero en un ordenador, generalmente descritas mediante un sistema jerárquico: se empieza por el límite inferior, mostrando un listado que contiene la unidad de disco, el directorio, los subdirectorios, el fichero mismo, la extensión del fichero si tiene alguna. Esta suma de información es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Fichero de informe

Es un fichero que lista las acciones ocurridas. BitDefender mantiene un fichero de informe (log) conteniendo un listado de las rutas analizadas, las carpetas, el número de archivos y ficheros analizados, el número de ficheros infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y hacía referencia a herramientas recompiladas que proporcionaba a los intrusos de derechos de administrador, permitiéndoles ocultar su presencia para no ser visto por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricoa, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

Es otro término para macro o fichero batch y consiste en una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o los posts basura en los grupos de noticias. Generalmente conocido como correo no solicita.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador

del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos en startup

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Bandeja del sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la parte de debajo de la pantalla, al lado del reloj y contiene iconos miniaturales para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los Troyanos arrastraran el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron del hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo a sus compatriotas entrar y capturar Troya.

Actualización

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

BitDefender tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.