ANTIVIRUS PLUS 2012

Guía de Usuario

Bitdefender Antivirus Plus 2012
Guía de Usuario

fecha de publicación 2011.07.27

Advertencia legal


Bitdefender

Tabla de contenidos

1. Pasos de la Instalación

1.1. Preparándose para la instalación

Antes de instalar Bitdefender Antivirus Plus 2012, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese que el equipo donde va a instalar Bitdefender cumple los requisitos mínimos de sistema.Si el equipo no cumple todos los requisitos mínimos del sistema, Bitdefender no se instalará o, si es instalado, no funcionará correctamente y provocará que el sistema se ralentice y sea inestable.Para una lista completa de los requisitos de sistema, por favor diríjase a "*Requisitos del Sistema*" (p. 1).
- Inicie sesión en el equipo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del equipo.La ejecución de dos programas de seguridad simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema.Windows Defender se desactivará durante la instalación.
- Durante la instalación, se recomienda que su equipo esté conectado a Internet.Si existen nuevas versiones de los archivos de aplicación aparte de los incluidos en el paquete de instalación, Bitdefender los descargará e instalará.

1.2. Requisitos del Sistema

Sólo podrá instalar Bitdefender Antivirus Plus 2012 en aquellos equipos que dispongan de los siguientes sistemas operativos:

- Windows XP con Service Pack 3 (32bit)
- Windows Vista con Service Pack 2
- Windows 7 con Service Pack 1

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

Nota

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

1.2.1. Requisitos mínimos del sistema

- 1,8 GB de espacio libre en disco duro (al menos 800 MB en la unidad del sistema)
- 800 MHz procesador
- 1 GB de memoria (RAM)

1.2.2. Requisitos de sistema recomendados

- 2,8 GB de espacio libre en disco duro (al menos 800 MB en la unidad del sistema)
- Intel CORE Duo (1.66 GHz) o procesador equivalente
- Memoria (RAM):
  - 1 GB para Windows XP
  - 1,5 GB para Windows Vista y Windows 7

1.2.3. Requisitos de Software

Para poder usar Bitdefender y todas sus funciones, su equipo necesita cumplir los siguientes requisitos software:

- Internet Explorer 7 o superior
- Mozilla Firefox 3.6 o superior
- Yahoo! Messenger 8.1 o superior
- .NET Framework 3

1.3. Instalando su producto Bitdefender

Puede instalar Bitdefender desde el CD de instalación de Bitdefender o utilizando el archivo de instalación descargado en su equipo desde el sitio Web de Bitdefender o desde otros sitios autorizados (por ejemplo, el sitio Web de un distribuidor de Bitdefender o una tienda online).Puede descargar el archivo de instalación desde la página web de Bitdefender en la siguiente dirección: http://www.bitdefender.com/site/Downloads/.

- Para instalar Bitdefender desde el disco de instalación, inserte el disco en la unidad.En breves momentos debería mostrarse una pantalla de bienvenida. Siga las instrucciones para iniciar la instalación.

  

  Nota

  La pantalla de bienvenida proporciona una opción para copiar el paquete de instalación desde el disco de instalación a un dispositivo de almacenamiento USB.Esto es útil si necesita instalar Bitdefender en un equipo que no posea una unidad de disco (por ejemplo, en un netbook).Insertar el dispositivo de almacenamiento en la unidad de USB y entonces haga en **Copiar a USB**.Después, diríjase al equipo que no tiene unidad de disco, inserte el dispositivo de almacenamiento en la unidad USB y haga doble clic en `runsetup.exe` de la carpeta donde tiene guardado el paquete de instalación.

  Si la pantalla de bienvenida no aparece, diríjase al directorio principal del disco y haga doble clic en el archivo `autorun.exe`.

- Para instalar Bitdefender utilizando el instalador Web descargado en su equipo, localice el archivo y haga doble clic en él.Esto iniciará la descarga de los archivos

de instalación, que puede tomar cierto tiempo, dependiendo de su conexión a Internet.

Bitdefender comprobará primero su equipo para validar la instalación.

Si su sistema no cumple con los requisitos mínimos para la instalación de Bitdefender, se le informará de las zonas qu desea mejorar antes de proceder.

Si se detecta un programa antivirus incompatible o una versión anterior de Bitdefender, se le solicitará que lo desinstale de su sistema.Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así posibles problemas que ocurran en un futuro.

Nota

Es posible que deba reiniciar su equipo para completar la eliminación de los programas antivirus detectados.

Siga los pasos del asistente de instalación para instalar Bitdefender Antivirus Plus 2012.

Paso 1 - Bienvenido

Por favor, lea el Acuerdo de licencia y seleccione **Aceptar y Continuar**.El acuerdo de licencia contiene los términos y condiciones bajo los cuales usted puede usar Bitdefender Antivirus Plus 2012.

Nota

Si no acepta estos términos, cierre la ventana.Se abandonará el proceso de instalación y saldrá del programa instalador.

Paso 2 - Registrar su producto

Para completar el registro de su producto es necesario introducir una clave de licencia y crear una cuenta MyBitdefender.Se necesita una conexión a Internet activa.

Proceda de acuerdo con su situación:

- **He adquirido el producto**

  En este caso, registre el producto siguiendo estos pasos:

  1. Seleccione **He adquirido el producto y quiero registrarlo ahora**.
  2. Introduzca la licencia en el campo correspondiente.

Nota

Puede encontrar su número de licencia en:

- en la etiqueta del CD/DVD.
- la tarjeta de licencia del producto.

- el mensaje de confirmación de compra online.

3. Escriba su dirección de correo electrónico en el campo correspondiente.

Importante

Se necesita una dirección de correo electrónico válida.Se enviará un mensaje de confirmación a la dirección que proporcionó.

4. Haga clic en **Registrar Ahora**.

- **Deseo evaluar Bitdefender**

  En este caso, puede utilizar el producto durante un período de 30 días.Para empezar el periodo de evaluación seleccione **Deseo evaluar el producto**.

  Para utilizar las funciones online del producto, es necesario que cree una cuenta MyBitdefender.Para crear una cuenta, escriba su dirección de correo electrónico en el campo correspondiente.Se enviará un mensaje de confirmación a la dirección que proporcionó.Si ya dispone de una cuenta, escriba la dirección de correo electrónico asociada a ella para registrar el producto con esa cuenta.

Configuración personalizada

Opcionalmente, puede personalizar durante este paso la configuración de la instalación, haciendo clic en **Configuración personalizada**.

Ruta de la Instalación

Por defecto, Bitdefender Antivirus Plus 2012 se instalará en `c:\Archivos de Programa\Bitdefender\Bitdefender2012`.Si desea cambiar la ruta de instalación, haga clic en **Cambiar** y seleccione la carpeta donde desea instalar Bitdefender.

Configurar las opciones del proxy

Bitdefender Antivirus Plus 2012 necesita acceso a Internet para el registro del producto, la descarga de actualizaciones de seguridad y de productos, componentes de detección en la nube, etc.Si utiliza una conexión proxy en lugar de una conexión directa a Internet, debe seleccionar esta opción y configurar las opciones del proxy.

Los ajustes se pueden importar desde el navegador predeterminado o puede introducirlos manualmente.

Activar actualización P2P

Puede compartir los archivos del producto y las firmas con otros usuarios de Bitdefender.De esta manera, Bitdefender puede actualizarse más rápido. Si no quiere activar esta característica, marque la casilla correspondiente.

Nota

No se compartirá información personal identificable si activa esta característica.

Si desea minimizar el impacto del tráfico de red en el rendimiento del sistema durante las actualizaciones, utilice la opción de compartir actualización.Bitdefender usa los puertos 8880 - 8889 para la actualización peer-to-peer.

Enviar informes anónimos de uso

Los Informes de Uso Anónimos están activados por defecto.Activando esta opción se envían informes con datos sobre cómo utiliza el producto a los servidores de Bitdefender.Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro.Los informes no tendrán datos confidenciales, tales como nombre, dirección IP u otra información, ni serán utilizados con fines comerciales.

Haga clic en **Aceptar** para confirmar sus preferencias.

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

Paso 3 - Progreso de la instalación

Espere a que la instalación se complete.Se muestra información detallada sobre el progreso.

Se analizan las áreas más críticas de su sistema en busca de virus, se descargan e instalan las últimas versiones de los archivos de aplicación, y se inician los servicios de Bitdefender.Este paso puede durar un par de minutos.

Paso 4 - Finalizar

Se muestra un resumen de la instalación.Si durante la instalación se detecta y elimina cualquier tipo de malware activo, puede que necesite reiniciar su equipo.

Haga clic en **Finalizar**.

1.3.1. Actualizar desde una versión anterior

Si ya está usando una versión anterior de Bitdefender, tiene dos maneras de actualizarse a Bitdefender Antivirus Plus 2012:

- Instalar Bitdefender Antivirus Plus 2012 directamente encima de la versión anterior.Bitdefender detectará la versión antigua y le ayudará a desinstalarla antes de instalar la nueva.Tendrá que reiniciar el equipo para completar el proceso.
- Desinstale la versión antigua, reinicie el equipo e instale la nueva versión como se describe en en las páginas anteriores.Utilice el método de actualización si los fallan.

Nota

La configuración del producto y los contenidos de cuarentena no se importarán desde la versión anterior.

2. Primeros Pasos

Una vez tiene instalado Bitdefender Antivirus Plus 2012, su equipo está protegido contra todo el malware (tales como virus, spyware y troyanos).

El modo Auto está activado por defecto y no necesita configurar ningún ajuste.De todos modos, puede que quiera aprovechar las opciones de Bitdefender para optimizar y mejorar su protección.

Bitdefender tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes.Los detalles sobre las acciones adoptadas y la información sobre la operación del programa están disponibles en la ventana de Eventos.Para más información, por favor vea "*Eventos*" (p. 13).

De vez en cuando, debe abrir Bitdefender y reparar las incidencias existentes.Puede que tenga que configurar componentes específicos de Bitdefender o tomar medidas de prevención para proteger su sistema y sus datos.

Si aún no ha registrado su producto (incluyendo la creación de una cuenta MyBitdefender), recuerde que debe hacerlo antes de que finalice el periodo de evaluación.Debe crear una cuenta para poder utilizar las funciones online del producto.Para más información sobre el proceso de registro, por favor diríjase a "*Registro*" (p. 8).

2.1. Abrir Bitdefender

Para acceder a la interfaz principal de Bitdefender Antivirus Plus 2012, utilice el menú Inicio de Windows, siguiendo la ruta **Inicio → Todos los programas → Bitdefender 2012 → Bitdefender Antivirus Plus 2012** o, de una manera más rápida, haga doble clic en el icono de Bitdefender del área de notificación.

Para obtener más información sobre la ventana de Bitdefender y el icono del área de notificación, consulte "*Interfaz de Bitdefender*" (p. 19).

2.2. Qué debe hacer después de la instalación

Si desea que Bitdefender controle por usted todas las decisiones relacionadas con la seguridad, mantenga activado el modo Piloto automático.Para más información, por favor vea "*Modo auto*" (p. 14).

Aquí dispone de una lista de tareas que puede necesitar completar después de la instalación:

- Si su equipo se conecta a Internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en "*¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?*" (p. 33).

- Si ha instalado Bitdefender en varios equipos en su red doméstica, puede administrar todos los productos Bitdefender de forma remota desde un único equipo.Para más información, por favor vea "*Mapa de la Red*" (p. 67).
- Cree reglas de protección de datos para evitar que sus datos personales importantes se divulguen sin su consentimiento.Para más información, por favor vea "*Protección de datos*" (p. 63).

2.3. Registro

A fin de que Bitdefender le mantenga protegido, debe registrar su producto introduciendo una clave de licencia y creando una cuenta MyBitdefender.

La clave de licencia especifica el tiempo que puede usar el producto.Cuando el número de licencia caduca, Bitdefender deja de realizar sus funciones y de proteger su equipo.

Debería adquirir un número de licencia o renovar su licencia unos días antes de que finalice el período de validez de la licencia actual.Para más información, por favor vea "*Adquirir o renovar claves de licencia*" (p. 11).Si está utilizando una versión de evaluación de Bitdefender, debe registrarse con una clave de licencia si desea seguir utilizándolo después del período de evaluación.

Una cuenta MyBitdefender le ofrece el acceso a las actualizaciones del producto y le permite utilizar los servicios online que ofrece Bitdefender Antivirus Plus 2012.Si ya dispone de una cuenta, registre su producto Bitdefender con esa cuenta.

Una cuenta MyBitdefender le permite:

- Mantenga actualizado el producto.
- Recuperar su clave de licencia, en caso de que la pierda.
- Póngase en contacto con el servicio de Atención al cliente de Bitdefender.
- Obtenga protección para su cuenta de Facebook con SafeGo.

2.3.1. Introducir su clave de licencia

Si durante la instalación ha seleccionado la opción de evaluación del producto, podrá utilizarlo durante un período de prueba de 30 días.Para continuar utilizando Bitdefender después del periodo de evaluación, debe registrarse con una clave de licencia.

Para registrar el producto con una clave de licencia o cambiar la licencia actual, haga clic en el enlace **Información de licencia**, que se encuentra en la parte inferior de la ventana de Bitdefender.Aparecerá la ventana de registro.

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

Para registrar Bitdefender Antivirus Plus 2012:

1. Introduzca el número de licencia en el campo editable.

Nota

Puede encontrar su número de licencia en:

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

Si no dispone de una clave de licencia Bitdefender, haga clic en el enlace que aparece en la ventana para abrir una página Web desde donde se puede adquirir una.

2. Haga clic en **Registrar Ahora**.

2.3.2. Iniciar sesión en MyBitdefender

Si proporcionó una dirección de correo electrónico durante la instalación, se ha enviado una confirmación por correo electrónico a la dirección que indicó.Haga clic en el enlace del correo electrónico para completar el registro.

Si no ha completado aún el registro, Bitdefender le notificará que necesita hacerlo.

Importante

Debe iniciar una sesión en una cuenta antes de haber transcurrido 30 días tras la instalación de Bitdefender.De lo contrario, Bitdefender dejará de actualizarse.

Para crear o acceder a una cuenta MyBitdefender, haga clic en el enlace **Completar registro** / **MyBitdefender**, situado en la parte inferior de la ventana de Bitdefender.

Se abrirá la ventana MyBitdefender.Proceder de acuerdo a su situación.

Quiero crear una cuenta MyBitdefender

Para crear con éxito una cuenta MyBitdefender, siga estos pasos:

1. Seleccione **Crear una cuenta nueva**.

   Aparecerá una nueva ventana.

2. Introduzca la información requerida en los campos correspondientes.Los datos que introduzca aquí serán confidenciales.

   - **Nombre** - introduzca un nombre de usuario para su cuenta. Este campo es opcional.
   - **E-mail** - introduzca su dirección de correo electrónico.
   - **Contraseña** - introduzca una contraseña para su cuenta.La contraseña debe tener al menos 6 caracteres.
   - **Confirmar contraseña** - vuelva a escribir la contraseña.

- Opcionalmente, Bitdefender puede informarle sobre ofertas especiales y promociones a través de la dirección de correo de su cuenta.Para activar esta opción, seleccione **Autorizo a Bitdefender a que me envíe mensajes de correo electrónico**.

Nota

Una vez que se ha creado la cuenta, puede utilizar la dirección de correo electrónico y contraseña proporcionadas para acceder a su cuenta en http://my.bitdefender.com.

3. Haga clic en **Enviar**
4. Antes de poder utilizar su cuenta debe completar el registro.Verifique su correo electrónico y siga las instrucciones en el correo electrónico de confirmación enviado por Bitdefender.

Nota

También puede iniciar una sesión con su cuenta de Facebook o Google.Para más información, por favor diríjase a"Quiero iniciar la sesión con mi cuenta de Facebook o Google" (p. 10)

Quiero iniciar la sesión con mi cuenta de Facebook o Google

Para iniciar su sesión con su cuenta de Facebook o Google, siga estos pasos:

1. Haga clic en el icono del servicio que desee utilizar para iniciar la sesión.Será redirigido a la página de inicio de sesión de ese servicio.
2. Siga las instrucciones proporcionadas por el servicio seleccionado para vincular su cuenta a Bitdefender.

Nota

Bitdefender no tiene acceso a información confidencial, como la contraseña de la cuenta que utiliza para conectarse, o la información personal de sus amigos y contactos.

Ya dispongo de una cuenta MyBitdefender

Si anteriormente ha iniciado una sesión en una cuenta de su producto, Bitdefender lo detectará e iniciará la sesión desde esa cuenta.Puede visitar su cuenta en http://my.bitdefender.com haciendo clic en **Ir a MyBitdefender**.

Si desea iniciar una sesión en una cuenta diferente, haga clic en el enlace correspondiente y siga las instrucciones en las secciones anteriores.

Si ya dispone de una cuenta activa, pero Bitdefender no la detecta, siga estos pasos para acceder a esa cuenta:

1. Escriba la dirección de correo y la contraseña de su cuenta en los campos correspondiente.

Nota

Si ha olvidado su contraseña, haga clic en **Olvidó su contraseña** y siga las instrucciones para recuperarla.

2. Haga clic en **Inicio de sesión**.

2.3.3. Adquirir o renovar claves de licencia

Si el período de evaluación está a punto de finalizar, debería adquirir una licencia y registrar su producto.Igualmente, si su actual licencia está apunto de caducar, debe renovar su licencia.

Bitdefender le avisará cuando se esté acercando la fecha de vencimiento de su licencia actual. Siga las instrucciones de la alerta para adquirir una nueva licencia.

Puede visitar una página Web desde donde puede adquirir una clave de licencia en cualquier momento siguiendo estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el enlace **Información de licencia**, situado en la parte inferior de la ventana de Bitdefender, para abrir la ventana de registro del producto.
3. Haga clic en el enlace que aparece en la parte inferior de la ventana.

2.4. Reparando incidencias

Bitdefender utiliza un sistema de seguimiento de incidencias para detectar e informarle acerca de las incidencias que pueden afectar a la seguridad de su equipo y datos. Por defecto, monitorizará sólo una serie de incidencias que están consideradas como muy importantes. Sin embargo, puede configurar según su necesidad, seleccionando que incidencias específicas desea que se le notifique.

Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad. Se agrupan en dos categorías:

- Las **Incidencias críticas**- impiden que Bitdefender le proteja contra el malware o representan un riesgo de seguridad importante.
- Las **incidencias menores (no críticas)** - pueden afectar a su protección en un futuro próximo.

El icono Bitdefender en la bandeja de sistema indica las incidencias pendientes cambiando su color de la siguiente manera:

Color rojo: Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.

Color amarillo: No hay incidencias críticas que afecten a la seguridad de su sistema. Debe marcar y reparar estas cuando tenga tiempo.

Además, si mueve el cursor del ratón encima del icono, una ventana emergente le confirmará la existencia de incidencias pendientes.

Cuando abra la ventana Bitdefender, el área de Estado de seguridad en la barra de herramientas superior indicará el número y la naturaleza de las incidencias que afectan a su sistema.

2.4.1. Asistente Reparar todas las incidencias

Para solucionar las incidencias detectadas siga el asistente **Reparar Todo**.

1. Para abrir el asistente, realice lo siguiente:
   - Haga clic con el botón derecho en el icono Bitdefender del área de notificación y elija **Reparar todo**.Dependiendo de los problemas detectados, el icono aparece de color rojo (lo que indica incidencias críticas) o amarillo (lo que indica incidencias no críticas).
   - Abra la ventana de Bitdefender y haga clic en cualquier lugar dentro del área de Estado de seguridad en la barra de herramientas superior (por ejemplo, puede hacer clic en el botón **Reparar todo**).
2. Puede ver las incidencias que afectan a la seguridad de su equipo y datos.Todas las incidencias actuales se han seleccionado para su reparación.

   Si no quiere corregir un problema específico inmediatamente, desactive la casilla de verificación correspondiente.Se le pedirá que especifique durante cuánto tiempo desea posponer la resolución de la incidencia.Elija la opción deseada en el menú y haga clic en **Aceptar**.Para detener la monitorización de la categoría de incidencia correspondiente, elija **Permanentemente**.

   El estado de la incidencia cambiará a **Posponer** y no se tomarán medidas para solucionar el problema.
3. Para reparar las incidencias seleccionadas, haga clic en **Iniciar**. Algunas incidencias se reparan inmediatamente. Para otras, un asistente le ayuda a repararlas.

Las incidencias que este asistente le ayuda a reparar pueden ser agrupadas dentro de estas principales categorías:

- **Desactivar configuración de seguridad.** Estas incidencias se reparan inmediatamente, al permitir la configuración de seguridad respectiva.

- **Tareas preventivas de seguridad que necesita realizar.** Cuando repara estas incidencias, un asistente le ayuda a completar la tarea con éxito.

2.4.2. Configuración de las alertas de estado

El sistema de alerta del estado está preconfigurado para monitorizar y alertarle sobre las incidencias más importantes que pueden afectar la seguridad de su equipo y datos.Además de las incidencias monitorizadas por defecto, hay otras incidencias que le pueden informar acerca de estas.

Puede configurar el sistema de alerta como mejor se adapte a sus necesidades eligiendo sobre que incidencias específicas quiere ser informado.Siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** en el menú de la izquierda y luego en la pestaña **Avanzado**.
4. Localice y haga clic en el enlace **Configurar alertas de estado**.
5. Haga clic en los conmutadores para activar o desactivar las alertas de estado de acuerdo con sus preferencias.

2.5. Eventos

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC.Los eventos son una herramienta muy importante en la supervisión y la gestión de la protección de Bitdefender.Por ejemplo, puede comprobar fácilmente si la actualización se ha realizado con éxito, si se ha encontrado malware en su equipo, etc.Además, si es necesario puede realizar acciones adicionales o cambiar las acciones que Bitdefender ha llevado a cabo.

Para abrir la ventana de Eventos, abra la ventana de Bitdefender y haga clic en el botón **Eventos** de la barra de herramientas superior.

Para ayudarle a filtrar los eventos de Bitdefender, se muestran las siguientes categorías en el menú izquierdo:

- **Antivirus**
- **Control De Privacidad**
- **Mapa de la Red**
- **Actualización**
- **SafeGo**
- **Registro**

Para cada categoría hay una lista de eventos disponibles.Para encontrar información sobre un evento particular en la lista, haga clic sobre él. Los detalles del evento se muestran en la parte inferior de la ventana.Cada evento incluye la siguiente información: una breve descripción, la acción que Bitdefender tomó cuando éste

se produjo, y la fecha y hora de cuando ocurrió.Si fuera necesario pueden proporcionarse opciones con el fin de tomar nuevas medidas.

Puede filtrar los eventos por su importancia.Hay tres tipos de eventos, cada uno de los cuales se identifica con un icono específico:

Los eventos de **Información** indican operaciones que se han completado con éxito.
Los eventos de **advertencia** indican incidencias no críticas. Cuando tenga tiempo debería comprobarlos y corregirlos.
Los eventos **críticos** indican problemas críticos. Debe verificarlos inmediatamente.

Para ayudar a administrar fácilmente los eventos registrados, cada sección de la ventana de eventos proporciona opciones para eliminar o marcar como leídos todos los eventos en esta sección.

2.6. Modo auto

Para todos los usuarios que no pidan nada más a su solución de seguridad que estar protegidos sin que le moleste, Bitdefender Antivirus Plus 2012 ha sido diseñado con un modo Auto incorporado.

Mientras se encuentre en el modo de Piloto automático, Bitdefender aplica una configuración de seguridad óptima y toma por usted todas las decisiones relacionadas con la seguridad.Esto significa que no verá ni ventanas emergentes, ni alertas, y no tendrá que ajustar ninguna configuración.

En el modo Piloto automático, Bitdefender repara y administra automáticamente y en silencio las incidencias críticas:

- Protección antivirus, proporcionada por el análisis on-access y el análisis continuo.
- Protección del cortafuego.
- Protección de la privacidad, proporcionada por el filtrado antiphishing y antimalware para su navegación Web.
- Actualizaciones automáticas.

Por defecto, el modo Piloto automático se activa en el momento en que se completa la instalación de Bitdefender.En la medida en que esté activado el Piloto automático, el icono de Bitdefender en el área de notificación cambiará a  .

Para activar o desactivar el Piloto automático, abra la ventana de Bitdefender y haga clic en el conmutador **Piloto automático** de la barra de herramientas superior.

Importante
Cuando el Piloto automático esté activado, la modificación de cualquiera de las opciones hará que éste se desactive.

Para ver el historial de las acciones realizadas por Bitdefender, mientras mantiene activado el Piloto automático, abra la ventana Eventos.

2.7. Modo Juego y Modo Portátil

Algunas de las actividades del equipo, como juegos o presentaciones, requieren una mayor respuesta e incremento del sistema, y no interrupciones.Cuando el portátil está funcionando con la batería, es mejor que las operaciones innecesarias, que consumen más energía, se aplacen hasta que el portátil está conectado de nuevo a la corriente.

Para adaptarse a estas situaciones particulares, Bitdefender Antivirus Plus 2012 incluye dos modos de trabajar:

- Modo Juego
- Modo Portátil

2.7.1. Modo Juego

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

- Todas las alertas y ventanas emergentes de Bitdefender quedan desactivadas.
- Autoanálisis está desactivado.El Autoanálisis detecta y utiliza periodos de tiempo cuando el uso de los recursos del sistema cae por debajo de un umbral determinado para así realizar análisis recurrente de todo el sistema.
- La Actualización automática está desactivada.
- La barra de herramientas de Bitdefender en su navegador de Internet se desactiva cuando juega a juegos online basados en el navegador.

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

Usando el Modo Juego

Por defecto, Bitdefender activa automáticamente el Modo Juego al iniciar un juego que se encuentra en la lista de juegos de Bitdefender, o al ejecutar una aplicación en modo pantalla completa.Bitdefender volverá automáticamente al modo de operación normal cuando cierre el juego o cuando se detecte que se ha salido de una aplicación en pantalla completa.

Si desea activar manualmente el Modo Juego, utilice uno de los siguientes métodos:

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

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

Cambiar la combinación de teclas del modo Juego

Puede activar manualmente el Modo Juego usando la combinación de teclas predeterminada, `Ctrl+Alt+Shift+G`.Si desea cambiar el atajo de teclado, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** del menú de la izquierda y luego en **Configuración**.
4. Bajo la opción **Activar combinación de teclas para el modo Juego**, puede definir la combinación de teclas que desee:
   a. Elija las teclas que desea utilizar seleccionado alguna de las siguientes: Control (`Ctrl`), Shift (`Shift`) o Alternate (`Alt`).
   b. En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

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

Nota
Para desactivar la combinación de teclas, desactive la opción **Habilitar combinación de teclas del modo Juego**.

Activar o desactivar el modo de juego automático

Para activar o desactivar el modo de juego automático, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** del menú de la izquierda y luego en **Configuración**.
4. Activar o desactivar el modo de juego automático haciendo clic en el botón correspondiente.

2.7.2. Modo Portátil

El Modo Portátil está diseñado especialmente para los usuarios de ordenadores portátiles. Su objetivo es minimizar el impacto de Bitdefender sobre el consumo de energía mientras estos dispositivos funcionan con batería.Cuando Bitdefender opera en modo Portátil, se desactivan las funciones de Autoanálisis y Actualización

automática, ya que requieren más recursos del sistema e, implícitamente, aumentan el consumo de energía.

Bitdefender detecta cuando su portátil hace uso de la batería y activa automáticamente el Modo Portátil.Asimismo, Bitdefender desactivará automáticamente el Modo Portátil cuando detecte que el portátil ha dejado de funcionar con batería.

Para activar o desactivar el modo Portátil automático, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** del menú de la izquierda y luego en **Configuración**.
4. Active o desactive el modo portátil automático, haciendo clic en el conmutador correspondiente.

Si Bitdefender no está instalado en un ordenador portátil, desactive el modo portátil automático.

2.8. Configuración de protección por contraseña de Bitdefender

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

Para configurar la protección por contraseña para la configuración deBitdefender, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** del menú de la izquierda y luego en **Configuración**.
4. En la sección **Opciones de protección por contraseña**, active la protección por contraseña haciendo clic en el botón.
5. Haga clic en el enlace **Cambiar contraseña**.
6. Introduzca la contraseña en los dos campos y haga clic en **Aceptar**.La contraseña debe tener al menos 8 caracteres.

Una vez que haya establecido una contraseña, cualquiera que desee cambiar la configuración de Bitdefender tendrá primero que proporcionar la contraseña.

Importante

Asegúrese de recordar su contraseña o guardarla en un lugar seguro.Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para soporte.

Para eliminar la protección por contraseña, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** del menú de la izquierda y luego en **Configuración**.
4. En la sección **Configuración protegida por contraseña**, active la protección por contraseña haciendo clic en el conmutador.
5. Introduzca la contraseña y haga clic en **Aceptar**.

2.9. Informes de uso anónimos

Por defecto, Bitdefender envía informes con datos sobre cómo utiliza la aplicación a los servidores Bitdefender.Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro.Los informes no tendrán datos confidenciales, tales como nombre, dirección IP u otra información, ni serán utilizados con fines comerciales.

Si desea detener el envío de Informes de uso anónimo, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** en el menú de la izquierda y luego en la pestaña **Avanzado**.
4. Desactive los informes de usuario anónimos, haciendo clic en el conmutador correspondiente.

2.10. Reparar o Desinstalar Bitdefender

Si desea reparar o desinstalar Bitdefender Antivirus Plus 2012, siga la ruta desde el menú de Inicio de Windows: **Inicio → Todos los programas → Bitdefender 2012 → Reparar o Desinstalar**.

Seleccione la acción que desea realizar:

- **Reparar** - Reinstala todos los componentes del programa.
- **Eliminar** - para quitar todos los componentes instalados.

Nota

Recomendamos elegir la opción **Desinstalar** para realizar una re-instalación limpia.

Esperar a que Bitdefender complete la acción que ha seleccionado.Tomará varios minutos.

Tendrá que reiniciar el equipo para completar el proceso.

3. Interfaz de Bitdefender

Bitdefender Antivirus Plus 2012 satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz de usuario gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.

Para ver el estado del producto y llevar a cabo tareas esenciales, dispone en cualquier momento del icono del área de notificación de Bitdefender.

La ventana principal le ofrece un acceso rápido a los módulos del producto así como a información importante del producto, y además le permite realizar tareas comunes.

Para configurar su producto Bitdefender de manera detallada y realizar tareas administrativas avanzadas, puede encontrar todas las herramientas que necesita en la ventana configuración.

3.1. Icono del área de notificación

Para administrar el producto con mayor rapidez, puede usar el Icono Bitdefender en la bandeja de sistemaSi hace doble clic en este icono se abrirá la interfaz de Bitdefender. Si hace clic derecho sobre el icono, aparecerá un menú contextual desde el que podrá administrar rápidamente el producto Bitdefender.

Icono Bandeja

- **Mostrar** - abre la ventana principal de Bitdefender.
- **Acerca de** - abre la ventana dónde puede verse información sobre Bitdefender y dónde encontrar ayuda en caso necesario.
- **Reparar Todas** - ayuda a eliminar las actuales vulnerabilidades de seguridad.Si esta opción no está disponible, no hay ninguna incidencia para reparar.Para más información, por favor, consulte el apartado "*Reparando incidencias*" (p. 11).
- **Activar / Desactivar Modo Juego** - activa / desactiva Modo Juego.
- **Actualizar** - realiza una actualización inmediata.Puede seguir el estado de la actualización en el panel de Actualización de la ventana principal de Bitdefender.

El icono de Bitdefender en la barra de herramientas le informa cuando una incidencia afecta a su equipo o como funciona el producto, mostrando un símbolo especial, como el siguiente:

Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.

Las incidencias no críticas afectan a la seguridad de su sistema.Cuando tenga tiempo debería comprobarlas y repararlas.

El producto funciona en Modo Juego.

Bitdefender Auto Pilot is engaged.

Si Bitdefender no funciona, el icono del área de notificación aparecerá en un fondo gris: .Normalmente sucede cuando una licencia caduca. Esto puede ocurrir cuando los servicios de Bitdefender no están respondiendo o cuando otros errores afectan al funcionamiento normal de Bitdefender.

3.2. Ventana principal

La ventana principal de Bitdefender le permite realizar tareas comunes, resolver rápidamente incidencias de seguridad, ver información sobre los eventos en el funcionamiento del producto y personalizar la configuración del mismo.Todo se encuentra a tan sólo unos clics.

La ventana está organizada en dos áreas principales:

Barra de herramientas superior
: Aquí es donde puede comprobar el estado de la seguridad de su equipo y acceder a tareas importantes.

Área de paneles
: Aquí es donde puede administrar los principales módulos de Bitdefender.

Además, puede encontrar varios enlaces útiles en la parte inferior de la ventana:

Enlace	Descripción
Feedback	Abre una página Web en su navegador donde puede completar una breve encuesta sobre su experiencia con el uso del producto.Contamos con sus comentarios en nuestro empeño constante de mejorar los productos Bitdefender.
Completar registro / MyBitdefender	Abre la ventana de la cuenta MyBitdefender, donde puede crear o acceder a una cuenta.Es necesario disponer de una cuenta MyBitdefender para poder recibir las actualizaciones y beneficiarse de las características online de su producto.Para obtener más información acerca de cómo puede crear una cuenta y los beneficios que ofrece, por favor consulte "*Iniciar sesión en MyBitdefender*" (p. 9).
Info Licencia	Abre una ventana donde puede ver la información de la actual licencia y podrá registrar su producto con una nueva licencia.
Ayuda y Soporte	Haga clic en este enlace si necesita ayuda con Bitdefender.

Enlace	Descripción
	Añade signos de interrogación en las diferentes áreas de la ventana de Bitdefender para ayudarle a encontrar fácilmente información sobre los diferentes elementos de la interfaz. Mueva el cursor del mouse sobre una marca para ver información rápida sobre el elemento adyacente.

3.2.1. Barra de herramientas superior

La barra de herramientas superior contiene los siguientes elementos:

- El **área de Estado de seguridad** a la izquierda de la barra de herramientas, le informa si hay incidencias que afectan a la seguridad del equipo y le ayuda a repararlas.

  El color del área del estado de la seguridad cambia en función de las incidencias detectadas y se muestran diferentes mensajes:

  - **El área aparece en color verde.** No hay incidencias que solucionar.Su equipo y sus datos están protegidos.
  - **La zona aparece en color amarillo.** Las incidencias no críticas afectan a la seguridad de su sistema.Cuando tenga tiempo debería comprobarlas y repararlas.
  - **El área es de color rojo.** Las incidencias críticas afectan a la seguridad de su sistema.Debe tratar estas incidencias de inmediato.

  Al hacer clic en el botón **Ver incidencias** en el centro de la barra de herramientas o en cualquier parte del área de estado de seguridad a su izquierda, puede acceder a un asistente que le ayudará a eliminar fácilmente cualquier amenaza de su equipo.Para más información, por favor, consulte el apartado "*Reparando incidencias*" (p. 11).

- **Eventos** le permite acceder a un historial detallado de hechos relevantes producidos mientras el producto estaba activo.Para más información, por favor, consulte el apartado "*Eventos*" (p. 13).
- **Configuración** le permite acceder a la ventana de configuración desde donde puede configurar el producto.Para más información, por favor, consulte el apartado "*Ventana de configuración*" (p. 24).
- El **Piloto automático** le permite activar el piloto automático y disfrutar de la seguridad en completo silencio.Para más información, por favor, consulte el apartado "*Modo auto*" (p. 14).

3.2.2. Área de paneles

El área de paneles es donde puede administrar directamente los módulos Bitdefender.

Puede organizar los paneles como desee.Para organizar el área de acuerdo a sus necesidades, arrastre paneles individuales y colóquelos en otros espacios.

Para navegar a través de los paneles, utilice la barra situada debajo del área de paneles o las flechas que aparecen a la derecha y a la izquierda.

De arriba a abajo, cada panel modular contiene los siguientes elementos:

- El nombre del módulo.
- Un mensaje de estado.
- El icono del módulo.Haga clic en el icono de un módulo para configurar sus ajustes en la ventana de configuración.
- Se trata de un botón que le permite realizar tareas importantes relacionadas con el módulo.
- En algunos paneles dispone de un conmutador que le permite activar o desactivar una característica importante del módulo.

Los paneles disponibles en esta área son:

Antivirus

La protección antivirus es la base de su seguridad. Bitdefender le protege en tiempo real y bajo demanda contra todo tipo de malware, como virus, troyanos, spyware, adware, etc.

Desde el panel Antivirus puede acceder fácilmente a tareas de análisis importantes.Haga clic en **Analizar** y seleccione una tarea en el menú desplegable:

- Quick Scan
- Análisis Completo
- Análisis Personalizado
- Vulnerabilidades
- Modo de rescate

El conmutador **Autoanálisis** le permite activar y desactivar la función de Autoanálisis.

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte “*Protección Antivirus*” (p. 35).

Actualización

En un mundo donde los cibercriminales tratan constantemente de encontrar nuevas maneras de delinquir, es esencial que mantenga al día su solución de seguridad si desea ir un paso por delante de ellos.

Por defecto, Bitdefender comprueba automáticamente cada hora si existen actualizaciones. Si desea desactivar las actualizaciones automáticas, utilice el conmutador **Actualización automática** en el panel Actualización.

Aviso

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

Haga clic en el botón **Actualizar** del panel para iniciar una actualización inmediata.

Para más información sobre la configuración de actualizaciones, por favor consulte "*Actualización*" (p. 71).

Control De Privacidad

El módulo de control de privacidad le ayuda a mantener la privacidad de su información personal principal.Le protege mientras navega por Internet contra ataques de phishing, intentos de fraude, filtraciones de datos privados, etc.

Haga clic en el botón **Administrar reglas** del panel de Control de privacidad para ir a la sección Protección de datos, donde puede configurar las reglas de privacidad.

El conmutador Antiphishing le permite activar o desactivar la protección antiphishing.

Para obtener más información acerca de cómo configurar Bitdefender para proteger su privacidad, por favor diríjase a "*Control De Privacidad*" (p. 60).

Mapa de la Red

Con la función Mapa de red puede manejar fácilmente la seguridad de sus equipos desde su casa y con un único equipo.

Para empezar, haga clic en **Administrar** en el panel Mapa de red y seleccione **Habilitar red**.

Una vez que la red esté activada, haciendo clic en **Administrar** del panel Mapa de red podrá acceder a las opciones siguientes.

- **Desactivar conexión** - desactiva la red.
- **Analizar todo** - iniciar un QuickScan de análisis completo del sistema en los equipos administrados.
- **Actualizar todos los equipos** - actualiza los productos Bitdefender en los equipos administrados.

Para más información, por favor vea "*Mapa de la Red*" (p. 67).

Safego

Para ayudarle a mantenerse seguro en Facebook, puede utilizar SafeGo, la solución de seguridad para redes sociales de Bitdefender, directamente desde su producto.

Haga clic en **Activar** para activar y administrar Safego desde su cuenta de Facebook.

Si ya ha activado SafeGo, podrá acceder a las estadísticas relacionadas con su actividad haciendo clic en el botón **Ver informes**.

Para más información, por favor vea "*Protección SafeGo para las redes sociales*" (p. 75).

3.3. Ventana de configuración

La ventana de configuración le permite acceder a todos los componentes y opciones de personalización del producto.Aquí es donde puede configurar Bitdefender con más detalle.

En la parte izquierda de la ventana hay un menú que contiene todos los módulos de seguridad.Cada módulo tiene una o más pestañas donde puede configurar los correspondientes ajustes de seguridad, ejecutar seguridad o tareas administrativas.La siguiente lista describe brevemente cada módulo.

General

Le permite configurar los ajustes generales del producto, como la configuración de contraseña, el modo Juego, el modo Portátil, la configuración del proxy y las alertas de estado.

Antivirus

Le permite configurar la protección contra malware, detectar y corregir las vulnerabilidades de su sistema, establecer exclusiones de análisis y administrar los archivos en cuarentena.

Control De Privacidad

Le ayuda a impedir el robo de datos de su equipo y protege su privacidad mientras está conectado a Internet.Configure la protección de su navegador Web y de su software de mensajería instantánea, administre la protección de datos, y mucho más.

Mapa de la Red

Le permite configurar y administrar los productos Bitdefender instalados en sus equipos domésticos desde un único equipo.

Actualización

Le permite obtener información sobre las últimas actualizaciones, actualizar el producto y configurar el proceso de actualización en detalle.

Además, puede encontrar varios enlaces útiles en la parte inferior de la ventana:

Enlace	Descripción
Feedback	Abre una página Web en su navegador donde puede completar una breve encuesta sobre su experiencia con el uso del producto.Contamos con sus comentarios en nuestro empeño constante de mejorar los productos Bitdefender.
Completar registro / **MyBitdefender**	Abre la ventana de la cuenta MyBitdefender, donde puede crear o acceder a una cuenta.Es necesario disponer de una cuenta MyBitdefender para poder recibir las actualizaciones y beneficiarse de las características online de su producto.Para obtener más información acerca de cómo puede crear una cuenta y los beneficios que ofrece, por favor consulte "*Iniciar sesión en MyBitdefender*" (p. 9).
Info Licencia	Abre una ventana donde puede ver la información de la actual licencia y podrá registrar su producto con una nueva licencia.
Ayuda y Soporte	Haga clic en este enlace si necesita ayuda con Bitdefender.
	Añade signos de interrogación en las diferentes áreas de la ventana de Bitdefender para ayudarle a encontrar fácilmente información sobre los diferentes elementos de la interfaz. Mueva el cursor del mouse sobre una marca para ver información rápida sobre el elemento adyacente.

Para volver a la ventana principal, haga clic en el botón **Inicio** de la esquina superior derecha de la ventana.

4. Cómo

Este capítulo proporciona instrucciones paso a paso para configurar los parámetros de uso general o para completar las tareas comunes con Bitdefender.Algunos de los temas incluyen referencias a otros temas donde puede encontrar información detallada.

4.1. ¿Cómo registro una versión de evaluación?

Si ha instalado una versión de evaluación, sólo podrá utilizarla durante un periodo limitado de tiempo.Para continuar utilizando Bitdefender después del período de evaluación, debe registrar su producto con una clave de licencia y crear una cuenta MyBitdefender.

- Para registrar Bitdefender, siga estos pasos:

  1. Abra la ventana de Bitdefender.
  2. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.Aparecerá la ventana de registro.
  3. Introduzca la licencia y haga clic en **Registrar Ahora**.

     Si no dispone de una clave de licencia, haga clic en el enlace que aparece en la ventana para visitar una página Web desde la que podrá adquirir una.

4. Espere hasta que el proceso de registro se haya completado y cierre la ventana.

- Para crear una cuenta MyBitdefender, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en **Completar registro** en la parte inferior de la ventana.Aparecerá la ventana de cuenta.
3. Seleccione el enlace correspondiente para crear una nueva cuenta.
4. Introduzca la información requerida en los campos correspondientes.Los datos que introduzca aquí serán confidenciales.

   Haga clic en **Enviar**
5. Compruebe su correo electrónico y siga las instrucciones recibidas con el fin de completar el registro.

Nota

Puede utilizar la dirección de correo electrónico y contraseña proporcionados para acceder a su cuenta en http://my.bitdefender.com.

4.2. ¿Cómo registro Bitdefender sin conexión a Internet?

Si acaba de adquirir Bitdefender, y no dispone de una conexión a Internet, también puede registrar Bitdefender aunque se encuentre desconectado.

Para registrar Bitdefender con su clave de licencia, siga estos pasos:

1. Diríjase a un PC conectado a Internet.Por ejemplo, puede utilizar el equipo de un amigo o un PC desde un lugar público.
2. Diríjase a https://my.bitdefender.compara crear una cuenta MyBitdefender.
3. Acceda a su cuenta y seleccione **Obtener registro sin conexión**.
4. Introduzca la clave de licencia que ha adquirido.
5. Haga clic en **Enviar** para obtener un código de confirmación.

Importante

Escriba el código de confirmación.

6. Vuelva a su PC con el código de confirmación.
7. Abra la ventana de Bitdefender.
8. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.Aparecerá la ventana de registro.
9. Seleccione la opción para registrar el producto con un código de confirmación.

10. Introduzca el código de confirmación en el campo correspondiente y haga clic en **Enviar**.
11. Espere hasta que el proceso de registro se haya completado y haga clic en **Finalizar**.

4.3. ¿Cómo puedo actualizar a otro producto de Bitdefender 2012?

Puede actualizar fácilmente desde un producto Bitdefender 2012 a otro.

Consideremos el siguiente escenario: lleva usando Bitdefender Antivirus Plus 2012 por un tiempo y recientemente ha decidido adquirir Bitdefender Total Security 2012 y disfrutar de las características adicionales que ofrece.

Todo lo que necesita hacer es adquirir una licencia para el producto Bitdefender 2012 que desea actualizar e introducir ésta en la ventana de registro del producto Bitdefender 2012 que está utilizando actualmente.

Siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.Aparecerá la ventana de registro.
3. Introduzca la licencia y haga clic en **Registrar Ahora**.
4. Bitdefender le informará de que la licencia es para un producto diferente y le dará la opción de instalarlo.Haga clic en el enlace correspondiente y siga el procedimiento para ejecutar la actualización.

4.4. ¿Cuándo debería reinstalar Bitdefender?

En algunas situaciones puede que necesite reinstalar su producto Bitdefender.

Las situaciones típicas en las cuales necesitaría reinstalar Bitdefender incluyen las siguientes:

- ha reinstalado el sistema operativo
- ha adquirido un equipo nuevo
- usted quiere cambiar el idioma en que se muestra la interfaz de Bitdefender

Para reinstalar Bitdefender puede usar el disco de instalación que adquirió o descargar una nueva versión desde el Sitio Web de Bitdefender.

Durante la instalación, se le preguntará que registre el producto con su clave de licencia.

Si no puede encontrar la clave de licencia, puede iniciar la sesión en https://my.bitdefender.com para recuperarla.Escriba la dirección de correo y la contraseña de su cuenta en los campos correspondiente.

4.5. ¿Cuándo caduca mi protección Bitdefender?

Para averiguar el número de días que le quedan a su clave de licencia, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.
3. En la ventana **Registrar su producto** puede encontrar el número de días restante.

4.6. ¿Cómo renuevo mi protección Bitdefender?

Cuando su protección de Bitdefender esté a punto de caducar, deberá renovar su licencia.

- Siga estos pasos para visitar un sitio Web donde podrá renovar su clave de licencia Bitdefender:
  1. Abra la ventana de Bitdefender.
  2. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.
  3. Haga clic en **¿No tiene una clave de licencia? ¡Adquiérala ahora!**
  4. Se abrirá una página Web en su navegador de Internet donde se puede adquirir una clave de licencia de Bitdefender.

  

  Nota
  Como alternativa, puede contactar con el vendedor al que adquirió su producto Bitdefender.

- Siga estos pasos para registrar su Bitdefender con la nueva clave de licencia:
  1. Abra la ventana de Bitdefender.
  2. Haga clic en el enlace **Información de licencias** en la parte inferior de la ventana.Aparecerá la ventana de registro.
  3. Introduzca la licencia y haga clic en **Registrar Ahora**.
  4. Espere hasta que el proceso de registro se haya completado y cierre la ventana.

Para obtener más información puede contactar con el soporte de Bitdefender como se describe en la sección “*Soporte*” (p. 92).

4.7. ¿Qué producto Bitdefender estoy utilizando?

Para conocer qué programa Bitdefender ha instalado, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. En la parte superior de la ventana debería ver uno de los siguientes:
   - Bitdefender Antivirus Plus 2012
   - Bitdefender Internet Security 2012
   - Bitdefender Total Security 2012

4.8. ¿Cómo analizo un archivo o una carpeta?

La forma más sencilla y recomendada de analizar un archivo o carpeta es hacer clic con botón derecho sobre el objeto que desea analizar y seleccionar **Analizar con Bitdefender** desde el menú.Para completar el análisis, siga las indicaciones del asistente de Análisis antivirus.

Las situaciones típicas en las cuales debería utilizar este método de análisis incluyen las siguientes:

- Sospecha que un fichero o carpeta concreta está infectada.
- Siempre que descarga desde Internet ficheros que piensa que podrían ser peligrosos.
- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

4.9. ¿Cómo analizo mi sistema?

Para ejecutar un análisis completo del sistema, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en **Analizar** y seleccione **Análisis Completo del Sistema** desde el menú desplegable.
4. Siga el asistente de Análisis Antivirus para finalizar el análisis.

4.10. ¿Cómo creo una tarea de análisis personalizada?

Para crear una tarea de análisis personalizada, proceda como se indica a continuación:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.

3. Haga clic en **Analizar** y seleccione **Análisis personalizado** desde el menú desplegable.
4. Haga clic en **Explorar** para seleccionar los archivos o carpetas a analizar.
5. Si desea configurar las opciones de análisis en detalle, haga clic en **Opciones de análisis**.

   Puede seleccionar la opción **Apagar equipo**.

   Su durante el análisis no se encuentran amenazas, su equipo se apagará cuando el análisis termine.Recuerde que este será el comportamiento predeterminado cada vez que ejecute esta tarea.
6. Haga clic en **Iniciar análisis** para ejecutar la tarea.

4.11. ¿Cómo excluyo una carpeta para que no sea analizada?

Bitdefender permite excluir del análisis archivos, carpetas o extensiones de archivo específicas.

Las exclusiones son para que las utilicen usuarios con conocimientos avanzados en informática y sólo en las siguientes situaciones:

- Tiene una carpeta de gran tamaño en su sistema donde guarda películas y música.
- Tiene un archivo grande en su sistema donde guarda distintos tipos de datos.
- Mantenga una carpeta donde instalar diferentes tipos de software y aplicaciones para la realización de pruebas.Analizar la carpeta puede provocar la pérdida de algunos de los datos.

Para añadir la carpeta a la lista de Exclusiones, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. Haga clic en el enlace **Archivos y carpetas excluidos**.
5. Haga clic en el botón **Añadir** ubicado en la parte superior de la tabla de exclusiones.
6. Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Aceptar**.
7. Haga clic en **Añadir** y luego haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

4.12. ¿Qué hacer cuando Bitdefender detecta un archivo limpio como infectado?

Existen casos cuando Bitdefender erróneamente señal aun archivo legítimo como una amenaza (un falso positivo).Para corregir este error, añada el archivo al área de Exclusiones de Bitdefender:

1. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Abra la ventana de Bitdefender.
   b. Haga clic en el botón **Configuración** en la barra de herramientas superior.
   c. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
   d. Haga clic en el conmutador para apagar el **análisis on-access**.
2. Muestra los objetos ocultos en Windows.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 100).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Abra la ventana de Bitdefender.
   b. Haga clic en el botón **Configuración** en la barra de herramientas superior.
   c. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Cuarentena**.
   d. Seleccione el archivo y haga clic en **Restaurar**.
4. Agregue el archivo a la lista de Exclusiones.Para saber como se hace esto, por favor diríjase a "*¿Cómo excluyo una carpeta para que no sea analizada?*" (p. 31).
5. Active la protección antivirus en tiempo real de Bitdefender.
6. Contacte con nuestros representantes del servicio de soporte de forma que podamos eliminar la firma de detección.Para saber como se hace esto, por favor diríjase a "*Pedir ayuda*" (p. 93).

4.13. ¿Cómo protejo mi información personal?

El Control de privacidad monitoriza los datos que salen de su equipo a través de formularios Web, mensajes de correo o mensajes instantáneos.

Para asegurar que ningún dato privado abandona su equipo sin su consentimiento, debe crear reglas adecuadas de protección de datos y excepciones a estas reglas.

Las reglas de protección de datos especifican la información que hay que bloquear.

Para crear una regla de Protección de datos, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.

3. Haga clic en **Control de privacidad** en el menú izquierdo y luego en la pestaña **Protección de datos**.
4. Si la **Protección de datos** está desactivada, actívela utilizando el interruptor correspondiente.
5. Seleccione la opción **Añadir regla** para iniciar el asistente de Protección de datos.
6. Siga los pasos del asistente.

4.14. ¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?

Si su equipo está conectado a Internet a través de un servidor proxy, debe configurar Bitdefender utilizando la configuración del proxy.Normalmente, Bitdefender automáticamente detecta e importa la configuración del proxy desde su sistema.

Importante

Las conexiones a Internet desde el propio domicilio no suelen utilizar un servidor proxy.Como regla de oro, compruebe y configure las opciones de la conexión proxy de su programa Bitdefender mientras no se estén aplicando actualizaciones.Si Bitdefender se puede actualizar, entonces está configurado correctamente para conectarse a Internet.

Para gestionar la configuración del proxy, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **General** en el menú de la izquierda y luego en la pestaña **Avanzado**.
4. En la sección **Configuración del proxy**, haga clic en el botón para activar la utilización del proxy.
5. Haga clic en el enlace **Gestionar proxys**.
6. Hay dos opciones para establecer la configuración del proxy:
   - **Importar configuración proxy desde el navegador predeterminado** - la configuración del proxy del usuario actual, extraída del navegador predeterminado. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.

Nota

Bitdefender puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Internet Explorer, Mozilla Firefox y Opera.

- **Configuración personalizada del proxy** - la configuración del proxy que puede modificar.Deben indicarse las siguientes opciones:
  - **Dirección** - introduzca la IP del servidor proxy.
  - **Puerto** - introduzca el puerto que Bitdefender debe utilizar para conectarse con el servidor proxy.
  - **Nombre de usuario** - escriba un nombre de usuario que el proxy reconozca.
  - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

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

Bitdefender usará las opciones disponibles de proxy hasta que consiga conectarse a Internet.

Importante

Recuerde desactivar la utilización del proxy cuando cambie a una conexión a Internet directa.

5. Protección Antivirus

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

- Análisis on-access - impide que las nuevas amenazas de malware entren en su sistema.Por ejemplo, Bitdefender analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.

  El análisis on-access garantiza la protección en tiempo real contra el malware, siendo un componente esencial de cualquier programa de seguridad informática.

  

  Importante
  Para evitar que los virus infecten su equipo, mantenga activado **Análisis on-access**.

- Análisis bajo demanda - permite detectar y eliminar el malware que ya reside en el sistema.Se trata del clásico análisis antivirus iniciado por el usuario - usted selecciona la unidad, carpeta o archivo que Bitdefender debe analizar, y Bitdefender lo analizará cuando se lo indique.

  Manteniendo Autoanálisis activado, prácticamente no existe necesidad de ejecutar manualmente los análisis en busca de malware.Autoanálisis analiza su equipo una y otra vez, adoptando las medidas adecuadas si detecta malware.La función de Autoanálisis sólo se ejecuta cuando dispone de suficientes recursos del sistema, para no ralentizar el equipo.

Bitdefender analiza automáticamente cualquier dispositivo extraíble que se conecte a su equipo para así asegurarse de que se puede acceder al mismo de forma segura.Para más información, por favor vea "*Análisis automático de los medios extraíbles*" (p. 48).

Los usuarios avanzados pueden configurar exclusiones de análisis si no desean que se analicen ciertos archivos o tipos de archivo.Para más información, por favor vea "*Configurar exclusiones de análisis*" (p. 50).

Cuando detecta un virus u otro malware, Bitdefender intentará eliminar automáticamente el código malware del archivo infectado y reconstruir el archivo original.Esta operación se conoce como desinfección.Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección.Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 52).

Si su equipo ha sido infectado con malware, por favor consulte "*Eliminando malware de su sistema*" (p. 83).Para ayudarle a limpiar su equipo de malware que no puede eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece el modo Rescate.Este es un entorno de confianza, especialmente diseñado para la

eliminación de malware, lo que le permite arrancar el equipo independientemente de Windows.Cuando el equipo se ejecuta en modo Rescate, el malware de Windows está inactivo, por lo que es fácil de eliminar.

Para protegerse de aplicaciones maliciosas desconocidas, Bitdefender utiliza Active Virus Control, una tecnología de heurística avanzada que monitoriza continuamente las aplicaciones que se ejecutan en su sistema.Active Virus Control bloquea automáticamente las aplicaciones que presentan un comportamiento similar al del malware para que dejen de dañar su equipo.En ocasiones, pueden bloquearse aplicaciones legítimas. En tal caso, se puede configurar Active Virus Control para no bloquear las aplicaciones mediante la creación de reglas de exclusión.Para obtener más información, consulte "*Active Virus Control*" (p. 53).

Muchas formas de malware están diseñadas para infectar los sistemas mediante la explotación de sus vulnerabilidades, como son la falta de actualizaciones del sistema operativo o las aplicaciones obsoletas.Bitdefender le ayuda fácilmente a identificar y corregir las vulnerabilidades del sistema con el fin de hacer que su equipo sea más seguro ante el malware y los hackers.Para más información, por favor vea "*Reparar vulnerabilidades del sistema*" (p. 56).

5.1. Análisis on-access (protección en tiempo real)

Bitdefender le ofrece una protección ininterrumpida (Protección en Tiempo Real) frente a todo tipo de amenazas de malware, al analizar todos los archivos a los que accede, los mensajes y las comunicaciones a través de aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger).

El nivel predeterminado de la protección en tiempo real asegura una buena protección contra el malware, con menor impacto en el rendimiento del sistema.Puede fácilmente cambiar los ajustes de la protección en tiempo real de acuerdo con sus necesidades cambiando uno de los niveles de protección predefinidos.O, si es un usuario avanzado, puede configurar las opciones de análisis en detalle creando un nivel de protección personalizado.

5.1.1. Comprobación de malware detectado por análisis on-access

Para comprobar malware detectado por el análisis en tiempo real (on-access), siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Eventos** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Análisis de virus**.Aquí es donde puede encontrar todos los eventos de análisis de malware, incluyendo amenazas detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.
4. Haga clic en un evento para ver más detalles sobre él.

5.1.2. Ajustar el nivel de protección en tiempo real

El nivel de protección en tiempo real, define las opciones de análisis para la protección en tiempo real.Puede fácilmente cambiar los ajustes de la protección en tiempo real de acuerdo con sus necesidades cambiando uno de los niveles de protección predefinidos.

Para ajustar el nivel de protección en tiempo real siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Mueva la barra sobre la escala para establecer le nivel de protección deseado.Utiliza la descripción en la parte derecha de la escala para selecciona el nivel de protección que mejor se ajuste a sus necesidades.

5.1.3. Crear un nivel de protección personalizado

Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender.Puede configurar los ajustes de la protección en tiempo real en detalle creando un nivel de protección personalizado.

Para crear un nivel de protección personalizado, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Haga clic en **Personal**.
5. Configure los ajustes del análisis como necesite.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario.También puede encontrar información de utilidad buscando en Internet.
- **Opciones de análisis para los archivos a los que accede.** Puede configurar Bitdefender para analizar todos los archivos accedidos o sólo aplicaciones (archivos de programa).Analizando todos los archivos proporciona una mejor protección, mientras analizando solo aplicaciones puede ser utilizado para mejorar el rendimiento del sistema.

  Las aplicaciones (o archivos de programa) son mucho más vulnerables a ataques de malware que otro tipo de archivos.Esta categoría incluye las siguientes extensiones de archivo:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analizar el interior de los archivos.** Analizar dentro de archivos es una proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para la protección en tiempo real. Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema.El malware puede afectar a su sistema su el archivo infectado es extraído del archivo y ejecutado sin tener la protección en tiempo real activada.

  Si decide utilizar esta opción puede establecer un límite máximo aceptado en el tamaño de los archivos a analizar.Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).

- **Opciones de análisis para tráfico e-mail, web y de mensajería instantánea.** Para prevenir de malware se descargue en su equipo, Bitdefender automáticamente analiza los siguiente puntos de entrada de malware:
  - ▶ e-mails entrantes y salientes
  - ▶ tráfico web
  - ▶ archivos recibidos a través de Yahoo! Messenger y Windows Live Messenger

  Analizando el tráfico web debe ralentizar el navegador web un poco, pero bloqueará el malware que viene de Internet, incluyendo descargas nos autorizadas.

  Aunque no se recomienda, puede desactivar el análisis antivirus de e-mail, web o mensajería instantánea para incrementar el rendimiento del sistema.Si desactiva las opciones de análisis correspondientes, los e-mails y archivos recibidos o descargados de Internet no serán analizados, esto permitirá guardar archivos infectados en su equipo.Esta no es una gran amenaza porque la protección en tiempo real bloquea el malware cuando se accede a los archivos infectados (abrir, mover, copiar o ejecutar).

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro.Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque.Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.
- **Analizar sólo archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.

5.1.4. Restaurar la configuración predeterminada

El nivel predeterminado de la protección en tiempo real asegura una buena protección contra el malware, con menor impacto en el rendimiento del sistema.

Para restaurar la configuración predeterminada de la protección en tiempo real, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Haga clic en **Predeterminada**.

5.1.5. Activar o desactivar la protección en tiempo real

Para activar o desactivar la protección en tiempo real contra malware, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Haga clic en el conmutador para activar o desactivar el análisis on-access.
5. Si decide desactivar la protección en tiempo real, aparecerá una ventana de advertencia.Para confirmar su elección, deberá indicar durante cuanto tiempo desea desactivar la protección. Puede desactivar la protección durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

Aviso

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

5.1.6. Medidas adoptadas sobre el malware detectado

Archivos detectados por la protección en tiempo real son agrupados dentro de dos categorías:

- **Archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender.Bitdefender puede eliminar normalmente el código malware de un archivo infectado y reconstruir el archivo original. Esta operación es conocida como desinfección.

  

  Nota

  Las firmas de malware son trozos de código extraído de muestras de malware actual. Son utilizados por los programas antivirus para realizar el reconocimiento de patrones y la detección de malware.
  La Base de Datos de Firmas Malware de Bitdefender es una colección de firmas de malware actualizada cada hora por los investigadores de malware de Bitdefender.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico.Dado que B-HAVE es una tecnología de análisis heurístico, Bitdefender no puede asegurar que el archivo esté realmente infectado con malware.Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

Dependiendo del tipo de archivo detectado, las siguientes acciones se realizan automáticamente:

- Si se detecta un archivo infectado, Bitdefender intentará desinfectarlo automáticamente.Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

  

  Importante

  Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- Si se detecta un archivo sospechoso, se pondrá en cuarentena para evitar una posible infección.

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender.Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

5.2. Análisis solicitado

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.

El análisis bajo demanda se basa en tareas de análisis. Estas tareas indican las opciones y los objetivos a analizar.Puede analizar el equipo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario).Si desea analizar ubicaciones específicas en el equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

5.2.1. Autoanálisis

Autoanálisis es un análisis bajo demanda que analiza silenciosamente todos los datos en busca de malware y toma las medidas apropiadas para cualquier infección que encuentre.El Autoanálisis detecta y utiliza periodos de tiempo cuando el uso de los recursos del sistema cae por debajo de un umbral determinado para así realizar análisis recurrente de todo el sistema.

Beneficios del uso de Autoanálisis:

- Tiene un impacto casi nulo en el sistema.
- Al preanalizar todo el disco duro, las tareas bajo demanda futuras se completarán muy rápido.
- El análisis on-access también tardará mucho menos tiempo.

Para activar o desactivar el Autoanálisis, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en los conmutadores para activar o desactivar el análisis automático.

5.2.2. Analizar un archivo o una carpeta en busca de malware

Debe analizar archivos y carpetas que sospeche que puedan estar infectados.Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **Analizar con Bitdefender**.El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

5.2.3. Ejecución de un análisis Quick Scan

El Quick Scan utiliza el análisis en la nube para detectar malware ejecutándose en su sistema.Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.

Para ejecutar un QuickScan, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en **Analizar** y seleccione **Quick Scan** en el menú desplegable.
4. Siga el Asistente de análisis antivirus para completar el análisis.

5.2.4. Ejecutar un Análisis completo del sistema

La tarea Análisis Completo del Sistema analiza todo el equipo en busca de todos los tipos de malware que puedan amenazar su seguridad, como virus, spyware, adware, rootkits y otros.Si ha desactivado Autoanálisis, se recomienda ejecutar un análisis completo del sistema al menos una vez a la semana.

Nota

Debido a que **Análisis completo del sistema** realiza un análisis de todo el sistema, el análisis puede tardar bastante tiempo. Por tanto, se recomienda ejecutar esta tarea cuando no está utilizando su equipo.

Antes de realizar un Análisis completo del sistema, se recomienda lo siguiente:

- Asegúrese de que Bitdefender está actualizado con las firmas de malware. Analizar su equipo con una base de datos de firmas obsoletas puede impedir que Bitdefender detecte nuevo malware encontrado desde la última actualización.Para más información, por favor vea *"Actualización"* (p. 71).
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en su equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.Para más información, por favor vea *"Configurar y ejecutar un análisis personalizado"* (p. 43).

Para ejecutar un Análisis completo del sistema, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en **Analizar** y seleccione **Análisis Completo del Sistema** desde el menú desplegable.
4. Siga el Asistente de análisis antivirus para completar el análisis.

5.2.5. Configurar y ejecutar un análisis personalizado

Para configurar un análisis detallado en busca de malware y ejecutarlo a continuación, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en **Analizar** y seleccione **Análisis personalizado** desde el menú desplegable.
4. Haga clic en **Añadir destino**, seleccione las casillas de verificación correspondientes a las ubicaciones que desea que se analicen en busca de malware y a continuación haga clic en **Aceptar**.
5. Haga clic en **Opciones de análisis** si quiere configurar las opciones de análisis.Aparecerá una nueva ventana.Siga estos pasos:
   a. Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Desplace la barra sobre la escala para establecer el nivel de análisis deseado.Utilice la descripción en la parte derecha de la escala para identificar el nivel de análisis que mejor se ajuste a sus necesidades.

      Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender.Para configurar las opciones de análisis en detalle, haga clic en **Personalizado**. Puede encontrar información sobre ellas al final de esta sección.

   b. Por defecto, Bitdefender intenta eliminar el código malware de los archivos infectados o, si la desinfección falla, ponerlos en cuarentena.Si ambas acciones fallan, se le pedirá que especifique una acción a elegir sobre las amenazas no resueltas.

      Si sólo desea detectar malware, sin realizar ninguna otra acción, seleccione la casilla de verificación correspondiente en la sección **Acciones**.

   c. Puede además configurar estas opciones generales:

      - **Ejecutar la tarea con baja prioridad.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
      - **Minimizar Asistente 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.
      - Especifica la acción a realizar si no se encuentran amenazas.

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

6. Haga clic en **Iniciar análisis** y siga el Asistente de Análisis Antivirus para completar el análisis.Dependiendo de las ubicaciones a analizar, el análisis puede llevar más tiempo.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario.También puede encontrar información de utilidad buscando en Internet.
- **Analizar ficheros.** Puede configurar Bitdefender para analizar todos los tipos de archivos o aplicaciones (archivos de programa) únicamente.Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.

  Las aplicaciones (o archivos de programa) son mucho más vulnerables a ataques de malware que otro tipo de archivos.Esta categoría incluye las siguientes extensiones de archivo: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Opciones de análisis para archivos.** Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema.El malware puede afectar a su sistema su el archivo infectado es extraído del archivo y ejecutado sin tener la protección en tiempo real activada.Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

Nota

El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro.Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque.Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.
- **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar registro.** Seleccione esta opción para analizar las claves de registro.El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.
- **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su equipo.
- **Analizar sólo archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
- **Ignorar keyloggers comerciales.** Seleccione esta opción si ha instalado y utilizado un software comercial keylogger en su equipo.Los keyloggers comerciales son programas legítimos de monitorización de equipos cuya función básica es grabar todo lo que se escribe en el teclado.

5.2.6. Asistente del análisis Antivirus

Siempre que inicie un análisis bajo demanda (por ejemplo, botón derecho sobre una carpeta y seleccionar **Analizar con Bitdefender**, aparecerá el asistente de Análisis de Bitdefender.Siga el asistente para completar el proceso de análisis.

Nota

Si el asistente de análisis no aparece, puede que el análisis esté configurado para ejecutarse en modo silencioso, en segundo plano.Busque el icono de progreso del análisis en la barra de tareas.Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Paso 1 – Elegir las ubicaciones del análisis

Este paso aparece solamente cuando usa el Análisis personalizado.Para más información, por favor vea *"Configurar y ejecutar un análisis personalizado"* (p. 43).

Paso 2 - Ejecutar análisis

Bitdefender analizará los objetos seleccionados.

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

Espere a que Bitdefender finalice el análisis.

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

Archivos protegidos por contraseña. Cuando se detecta un archivo protegido por contraseña, dependiendo de las opciones de análisis, puede ser preguntado para que proporcione la contraseña.Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña.Tiene las siguientes opciones a su disposición:

- **Introducir contraseña.** Si desea que Bitdefender analice el archivo, seleccione esta opción e introduzca la contraseña.Si no conoce la contraseña, elija una de las otras opciones.
- **No preguntar por una contraseña y omitir este objeto del análisis.** Marque esta opción para omitir el análisis de este archivo.
- **Omitir todos los elementos protegidos con contraseña sin analizarlos.** Seleccione esta opción si no desea que se le pregunte acerca de archivos protegidos por contraseña.Bitdefender no podrá analizarlos, pero se guardará información acerca de ellos en el informe de análisis.

Haga clic en **Aceptar** para continuar el análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento, haciendo clic en botón **Parar**. Irá directamente al último paso del asistente.Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

Paso 3 - Elegir acciones

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

Si no hay amenazas sin resolver, haga clic en **Continuar**.Por otra parte, debe configurar nuevas acciones a realizar en las amenazas sin resolver para proteger su sistema.

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

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias.Una o varias de las siguientes opciones pueden aparecer en el menú:

Ninguna Acción
No se realizará ninguna acción sobre los archivos detectados.Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.

Desinfectar
Elimina el código de malware de los archivos infectados.

Eliminar
Elimina los archivos detectados del disco.

Mover a Cuarentena
Traslada los archivos detectados a la cuarentena.Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 52).

Renombrar archivos
Renombra los ficheros ocultos añadiendo `.bd.ren` a su nombre.Como resultado, podrá buscar y encontrar estos ficheros en su equipo, en caso de que existan.

Por favor tenga en cuenta que estos ficheros ocultos no son ficheros que usted ocultó de Windows. Son fichero ocultados por programas especiales, conocidos como rootkits.Los rootkits no son maliciosos por naturaleza. De todas maneras, son utilizados normalmente para hacer que los virus o spyware no sean detectados por programas normales antivirus.

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

Paso 4 – Resumen

Una vez Bitdefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana.Si desea información exhaustiva del proceso de análisis, haga clic en **Mostrar Log** para ver el informe de análisis.

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

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

Bitdefender No Ha Podido Reparar Algunas Incidencias

En la mayoría de casos, Bitdefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena.Sin embargo, hay incidencias que no pueden resolverse automáticamente.Para más información e instrucciones sobre como eliminar malware manualmente, por favor consulte "*Eliminando malware de su sistema*" (p. 83).

Objetos Sospechosos Detectados por Bitdefender

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

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

5.2.7. Comprobación de los resultados del análisis

Cada vez que realiza un análisis, se crea un registro de análisis.El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez completado el análisis, haciendo clic en **Mostrar Registro**.

Para comprobar los registros de análisis más tarde, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Eventos** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Análisis de virus**.Aquí es donde puede encontrar todos los eventos de análisis de malware, incluyendo amenazas detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.
4. En la lista de eventos puede comprobar qué análisis se han realizado recientemente.Haga clic en un evento para ver más detalles sobre él.
5. Para abrir el registro de análisis, haga clic en **Ver registro**.El informe del análisis se abrirá en su navegador predeterminado.

5.3. Análisis automático de los medios extraíbles

Bitdefender detecta automáticamente si conecta un dispositivo de almacenamiento extraíble a su equipo y lo analiza en segundo plano.Le recomendamos con el fin de evitar virus y otro malware que infecten a su equipo.

La detección de dispositivos se dividen en una de estas categorías:

- Cds/DVDs
- Dispositivos de almacenamiento USB, como lápices flash y discos duros externos.
- Unidades de red (remotas) mapeadas.

Puede configurar el análisis automático de manera independiente para cada categoría de dispositivos de almacenamiento.Por defecto, el análisis automático de las unidades de red mapeadas está desactivado.

5.3.1. ¿Cómo funciona?

Cuando se detecta un dispositivo de almacenamiento extraíble, Bitdefender inicia el análisis en segundo plano en busca de malware (siempre y cuando se haya activado el análisis automático para este tipo). Un icono de análisis Bitdefender aparecerá en la bandeja de sistema.Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Si el piloto automático está activado, no se le preguntará acerca del análisis.Sólo se registrará el análisis, y la información al respecto estará disponible en la ventana Eventos.

Si el Piloto automático está desactivado:

1. Mediante una ventana emergente se le notificará que se ha detectado un nuevo dispositivo y se está analizando.
2. Si se detecta un archivo protegido por contraseña durante el análisis, se le puede solicitar que proporcione la contraseña.Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña.Puede elegir introducir la contraseña, omitir el archivo del análisis o deshabilitar la detección de archivos protegidos por contraseña.
3. En la mayoría de los casos, Bitdefender elimina automáticamente el malware detectado o mantiene aislados en cuarentena los archivos infectados.Si quedan amenazas sin resolver tras el análisis, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Nota

Tenga en cuenta que no se pueden tomar medidas en archivos infectados o sospechosos detectado en CDs/DVDs. Del mismo modo, no se puede realizar ninguna acción en los archivos detectados como infectados o sospechosos en unidades de red si no tiene los privilegios apropiados.

4. Cuando el análisis se ha completado, la ventana de los resultados del análisis se mostrará para informarle si es seguro acceder a los archivos en el medio extraíble.

Esta información le puede ser útil:

- Por favor, tenga cuidado al usar un CD/DVD infectado con malware, porque el malware no puede eliminarse del disco (el soporte es de sólo lectura).Asegúrese de que la protección en tiempo real está activada para evitar que el malware se propague por su sistema.Es una buena práctica copiar los datos importantes desde el disco a su sistema y luego deshacerse de los discos.
- En algunos casos, Bitdefender puede no ser capaz de eliminar el malware de los archivos específicos debido a restricciones legales o técnicas. Un ejemplo son los archivos comprimidos con una tecnología propia (esto es porque el archivo no se puede recrear correctamente).

Para saber cómo hacer frente a malware, diríjase a *"Eliminando malware de su sistema"* (p. 83).

5.3.2. Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de dispositivos extraíbles, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. En la sección **Analizar dispositivos detectados**, elija los dispositivos de almacenamiento que desea que se analicen automáticamente.Haga clic en los conmutadores para activar o desactivar el análisis automático.

Para una mejor protección, se recomienda activar el análisis automático de todos los dispositivos de almacenamiento extraíbles.

Las opciones de análisis están preconfiguradas para mejores resultados de detección.Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso) o los pondrá bajo cuarentena. Si ambas medidas fallan, el asistente de Análisis del Antivirus le permitirá especificar otras acciones a realizar con los archivos infectados.Las opciones de análisis son estándar y no las puede modificar.

5.4. Configurar exclusiones de análisis

Bitdefender le permite excluir del análisis archivos, carpetas o extensiones de archivo específicos. Esta característica está diseñada para evitar interferencias con su trabajo y también para ayudarle a mejorar el rendimiento de su sistema.Las exclusiones las deben utilizar usuarios con conocimientos avanzados de informática o bien siguiendo las recomendaciones de un representante de Bitdefender.

Puede configurar exclusiones para aplicar solamente al análisis en tiempo real o bajo demanda, o ambos.Los objetos excluidos del análisis en tiempo real no serán analizados, tanto si usted o una aplicación acceden al mismo.

Nota

Las exclusiones no se aplicarán para los análisis contextuales.El análisis contextual es un tipo de análisis bajo demanda: haga clic derecha sobre un fichero o carpeta que desee analizar y seleccione **Analizar con Bitdefender**.

5.4.1. Excluir del análisis los archivos o carpetas

Para excluir determinados archivos o carpetas del análisis, siga estos pasos:

1. Abra la ventana de Bitdefender.

2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. Active las exclusiones de análisis para los archivos usando el conmutador correspondiente.
5. Haga clic en el enlace **Archivos y carpetas excluidos**.En la ventana que aparece puede administrar los archivos y carpetas excluidos del análisis.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **Añadir** ubicado en la parte superior de la tabla de exclusiones.
   b. Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Aceptar**.Como alternativa, puede escribir (o copiar y pegar) en el campo de edición la ruta del archivo o carpeta.
   c. Por defecto, el archivo o carpeta seleccionado se excluye tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la exclusión, seleccione una de las otras opciones.
   d. Haga clic en **Añadir**.
7. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

5.4.2. Excluir del análisis las extensiones de archivo

Al excluir una extensión de archivo del análisis, Bitdefender ya no analizará archivos con esta extensión, independientemente de la ubicación en su equipo.La exclusión también se aplica a los archivos en medios extraíbles, como CDs, DVDs, dispositivos de almacenamiento USB o unidades de red.

Importante
Tenga cuidado al excluir las extensiones del análisis ya que tales exclusiones pueden hacer que su equipo sea vulnerable al malware.

Para excluir extensiones de archivo del análisis, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. Active las exclusiones de análisis para los archivos usando el conmutador correspondiente.
5. Haga clic en el enlace **Extensiones excluidas**.En la ventana que aparece puede administrar las extensiones de archivo excluidas del análisis.
6. Añada exclusiones siguiendo estos pasos:

a. Haga clic en el botón **Añadir** ubicado en la parte superior de la tabla de exclusiones.

b. Introduzca las extensiones que desea excluir del análisis, separándolos con punto y coma (;).Aquí tiene un ejemplo:

```
txt;avi;jpg
```

c. Por defecto, todos los archivos con las extensiones mencionadas son excluidos tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la exclusión, seleccione una de las otras opciones.

d. Haga clic en **Añadir**.

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

5.4.3. Administrar exclusiones de análisis

Si las exclusiones de análisis configuradas ya no son necesarias, se recomienda eliminarlas o desactivar las exclusiones de análisis.

Para administrar exclusiones de análisis, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.Utilice las opciones en la sección **Archivos y carpetas** para gestionar exclusiones de análisis.
4. Para eliminar o editar exclusiones de análisis, haga clic en uno de los vínculos disponibles.Siga estos pasos:
   - Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.
   - Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo y haga clic en el botón **Editar**).Aparecerá una nueva ventana donde podrá cambiar la extensión o la ruta a excluir, y el tipo de análisis del que desea excluirlo. Realice los cambios necesarios y haga clic en **Modificar**.
5. Para desactivar las exclusiones de análisis, utilice el botón correspondiente.

5.5. Administración de los archivos en cuarentena

Bitdefender aísla los archivos infectados con malware que no puede desinfectar y los archivos sospechosos en un área segura denominada cuarentena.Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender.Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Adicionalmente, Bitdefender analiza los ficheros de la cuarentena después de cada actualización de firmas de malware.Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Para comprobar y gestionar los archivos en cuarentena, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Cuarentena**.
4. Bitdefender gestiona automáticamente los archivos en cuarentena, según la configuración de cuarentena predeterminada.Aunque no se recomienda, puede ajustar la configuración de la cuarentena según sus preferencias.

   Volver a analizar la cuarentena tras actualizar las firmas
   Mantenga activada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de las definiciones de virus.Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

   Enviar los archivos en cuarentena a Bitdefender para su posterior análisis
   Mantenga esta opción activada para enviar automáticamente los archivos en cuarentena a los Laboratorios de Bitdefender.Los investigadores de malware de Bitdefender analizarán los archivos de muestra.Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

   Eliminar contenido con una antigüedad superior a {30} días
   Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente.Si desea cambiar este intervalo, escriba el valor nuevo en el campo correspondiente.Para desactivar la eliminación automática de sus antiguos archivos en cuarentena, escriba 0.

5. Para eliminar un archivo en cuarentena, selecciónelo y haga clic en el botón **Eliminar**.Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

5.6. Active Virus Control

Bitdefender Active Virus Control es una tecnología de detección proactiva innovadora que utiliza avanzados métodos heurísticos para detectar nuevas amenazas potenciales en tiempo real.

Active Virus Control continuamente monitoriza las aplicaciones que se están ejecutando en su equipo, buscando acciones de malware. Cada una de estas acciones se puntúa y se calcula una puntuación global para cada proceso.Cuando la puntuación global de un proceso alcanza un determinado umbral, el proceso se considera dañino y se bloquea automáticamente.

Si el piloto automático está desactivado, se le notificará a través de una ventana emergente sobre la aplicación bloqueada.De lo contrario, la aplicación se bloquea sin ningún tipo de notificación.En la ventana Eventos puede comprobar qué aplicaciones ha detectado Active Virus Control.

5.6.1. Comprobando aplicaciones detectadas

Para comprobar las aplicaciones detectadas por Active Virus Control, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Eventos** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Active Virus Control**.
4. Haga clic en un evento para ver más detalles sobre él.
5. Si confía en la aplicación, puede configurar Active Virus Control para no bloquearla más haciendo clic en **Permitir y monitorizar**.Active Virus Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y se informará a Bitdefender en la nube como error de detección.

5.6.2. Activar o Desactivar Active Virus Control

Para activar o desactivar el Active Virus Control, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Haga clic en el botón para activar o desactivar el Active Virus Control.

5.6.3. Ajustar la protección de Active Virus Control

Si observa que Active Virus Control detecta frecuentemente aplicaciones legítimas, debería establecer un nivel de protección más permisivo.

Para ajustar la protección de Active Virus Control, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.

3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.
4. Asegúrese de que Active Virus Control está activado.
5. Mueva la barra sobre la escala para establecer le nivel de protección deseado.Utiliza la descripción en la parte derecha de la escala para selecciona el nivel de protección que mejor se ajuste a sus necesidades.

Nota

A medida que aumente el nivel de protección, Active Virus Control necesitará menos indicios de comportamiento tipo malware para informar de un proceso. Esto conducirá a un número mayor de aplicaciones objeto de informe y, al mismo tiempo, a un aumento de probabilidad de falsos positivos (aplicaciones limpias detectadas como maliciosas).

5.6.4. Gestionar procesos excluidos

Puede configurar reglas de exclusión para las aplicaciones de confianza para que Active Virus Control no las bloquee si realizan acciones de tipo malware.Active Virus Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y se informará a Bitdefender en la nube como error de detección.

Para administrar la exclusiones de procesos de Active Virus Control, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. Haga clic en el enlace **Procesos excluidos**.En la ventana que aparece puede administrar las exclusiones de procesos Active Virus Control.
5. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **Añadir** ubicado en la parte superior de la tabla de exclusiones.
   b. Haga clic en **Examinar**, busque y seleccione la aplicación a excluir y a continuación haga clic en **Aceptar**.
   c. Mantenga seleccionada la opción **Permitir** para evitar que Active Virus Control bloquee la aplicación.
   d. Haga clic en **Añadir**.
6. Para eliminar o editar exclusiones, haga lo siguiente:
   - Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

- Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo y haga clic en el botón **Editar**).Haga los cambios necesarios y a continuación haga clic en **Modificar**.

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

5.7. Reparar vulnerabilidades del sistema

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

Bitdefender ofrece dos formas fáciles de solucionar las vulnerabilidades de su sistema:

- Puede analizar su sistema en busca de vulnerabilidades y repararlas paso a paso utilizando el asistente **Analizar Vulnerabilidades**.
- Mediante el control automático de la vulnerabilidad, puede comprobar y corregir las vulnerabilidades detectadas en la ventana Eventos.

Debería revisar y corregir las vulnerabilidades del sistema cada una o dos semanas.

5.7.1. Analizar su sistema en busca de vulnerabilidades

Para reparar vulnerabilidades del sistema usando el asistente de Análisis de vulnerabilidades, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Ir al panel **Antivirus**.
3. Haga clic en **Analizar ahora** y seleccione a continuación **Análisis de vulnerabilidades**.
4. Siga los seis pasos guiado para proceder a la eliminación de vulnerabilidades de su sistema.Puede navegar a través del asistente utilizando el botón **Siguiente**-Para salir del asistente, haga clic en **Cancelar**.

   a. **Proteja su PC**

      Seleccione las vulnerabilidades a comprobar.

   b. **Comprobar incidencias**

      Espere a que Bitdefender finalice la comprobación de su sistema en busca de vulnerabilidades.

   c. **Actualizaciones de Windows**

Puede ver la lista de las actualizaciones críticas y no-críticas que actualmente no están instaladas en su equipo.Seleccione las actualizaciones que desea instalar.

Para iniciar la instalación de las actualizaciones seleccionadas, haga clic en **Siguiente**.Tenga en cuenta que puede llevar bastante tiempo instalar las actualizaciones, y alguna de ellas puede requerir que reinicie el sistema para completar la instalación.Si es necesario, reinicie el sistema en cuanto pueda.

d. **Actualizaciones de aplicaciones**

Si una aplicación no está actualizada, haga clic en el enlace indicado para descargar la nueva versión.

e. **Contraseñas inseguras**

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

Haga clic en **Reparar** para modificar las contraseñas inseguras.Puede elegir entre preguntar al usuario para que cambie la contraseña en el siguiente inicio de sesión o cambiarla usted mismo inmediatamente.Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

f. **Sumario**

Aquí es donde puede ver el resultado de la operación.

5.7.2. Usar el control automático de la vulnerabilidad

Bitdefender analiza frecuentemente el sistema en segundo plano en busca de vulnerabilidades y mantiene las incidencias detectadas en la ventana de Eventos.

Para comprobar y reparar las incidencias detectadas, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Eventos** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y a continuación en la pestaña **Vulnerabilidad**.
4. Puede ver información detallada sobre las vulnerabilidades del sistema detectadas.Dependiendo de la incidencia, para reparar una vulnerabilidad específica haga lo siguiente:
   - Si las actualizaciones de Windows están disponibles, haga clic en **Actualizar ahora** para abrir el asistente de Análisis de vulnerabilidades e instalarlas.
   - Si una aplicación está obsoleta, haga clic en **Actualizar ahora** para encontrar un enlace a la página Web de los proveedores desde donde puede instalar la última versión de esta aplicación.

- Si una cuenta de usuario de Windows tiene una contraseña débil, haga clic en **Reparar contraseña** para forzar al usuario a cambiar la contraseña en el próximo inicio de sesión o cámbiela usted mismo.Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).
- Si la función Ejecución automática de Windows está activada, haga clic en **Desactivar** para desactivarla.

Para configurar las opciones de monitorización de vulnerabilidades, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y a continuación en la pestaña **Vulnerabilidad**.
4. Haga clic en el conmutador para activar o desactivar el análisis de vulnerabilidades automático.

   

   Importante

   Para recibir notificaciones automáticas sobre las vulnerabilidades del sistema o aplicaciones, mantenga activado el **Análisis de vulnerabilidad automático**.

5. Elija las vulnerabilidades del sistema que quiere comprobar regularmente usando los conmutadores correspondientes.

   Actualizaciones críticas de Windows

   Compruebe si su sistema operativo Windows tiene las últimas actualizaciones críticas de seguridad de Microsoft.

   Actualizaciones opcionales de Windows

   Compruebe si su sistema operativo Windows tiene las últimas actualizaciones normales de seguridad de Microsoft.

   Actualizaciones de aplicaciones

   Compruebe si las aplicaciones fundamentales relacionadas con la Web instaladas en su sistema están actualizadas.Las aplicaciones obsoletas pueden ser explotadas por software malicioso, haciendo vulnerable su PC a los ataques externos.

   Contraseñas inseguras

   Comprobar si las contraseñas de las cuentas de Windows configuradas en el sistema son fáciles de adivinar o no.Establecer contraseñas que sean difíciles de averiguar (contraseñas fuertes) hace que sea muy difícil para los hackers entrar en el sistema.Una contraseña segura necesita letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Ejecución automática de dispositivos

Comprobar el estado de la función Ejecución automática de Windows.Esta función permite a las aplicaciones iniciarse automáticamente desde CDs, DVDs, unidades USB y otros dispositivos externos.

Algunos tipos de malware utilizan la ejecución automática para difundirse en el PC desde un medio extraíble de forma automática. Pro lo que se recomienda desactivar esta función de Windows.

Nota

Si desactiva la monitorización de una vulnerabilidad específica, los problemas derivados no se registrarán en la ventana Eventos.

6. Control De Privacidad

Su información privada es un objetivo constante para los ciberdelincuentes.Como las amenazas se han extendido a prácticamente todo el espectro de las actividades online, el correo electrónico, la mensajería instantánea y la navegación web que no estén protegidos debidamente pueden producir la fuga de información que ponga en compromiso su privacidad.

Control de Privacidad Bitdefender gestiona todas estas amenazas con multitud de componentes.

- Protección antiphishing - ofrece un conjunto extenso conjunto de funciones que protegen toda su experiencia de exploración en Internet, incluyendo la capacidad de evitar que desvele información personal en sitios Web fraudulento camuflados como sitios legítimos.
- Protección de datos - le ayuda a asegurarse de que no se envíe desde su equipo información personal sin su consentimiento.Analiza el correo electrónico y los mensajes instantáneos enviados desde su equipo, así como cualquier información enviada a través de páginas Web, y bloquea cualquier tipo de información protegida por la regla de Protección de datos que haya creado.
- Cifrado de chat - cifra sus conversaciones de MI para garantizar que sus contenidos entre usted y su compañero de chat permanecen seguros.

6.1. Protección antiphishing

El Antiphishing de Bitdefender le impide revelar información personal mientras navega por Internet, al avisarle cada vez que detecte una página web de phishing en potencia.

Bitdefender ofrece protección antiphishing en tiempo real para:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Para configurar las opciones Antiphishing, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **COntrol de privacidad** en el menú izquierdo y luego en la pestaña **Antiphishing**.

Las opciones se agrupan en dos categorías.

Funciones de la barra de herramientas

Haga clic en los conmutadores para activar o desactivar:

- Mostrar la barra de herramientas Bitdefender en el navegador.
- El Asesor de búsqueda, un componente que puntúa los resultados de las búsquedas de Google, Bing y Yahoo!, así como enlaces a Facebook y Twitter, colocando un icono delante de cada resultado:

  No debería visitar esta página web.

  Esta página Web puede albergar contenidos peligrosos. Tenga cuidado si decide visitarla.

  Esta página es segura.
- Analizar tráfico Web SSL.

  Los ataques más sofisticados pueden utilizar el tráfico de Internet seguro para engañar a sus víctimas.Por ello se recomienda activar el análisis SSL.

Protección para navegadores

Haga clic en los conmutadores para activar o desactivar:

- Protección contra el fraude.
- Protección contra phishing.
- Protección para mensajería instantánea.

Puede crear una lista de los sitios web que no serán analizados por los motores Antiphishing de Bitdefender.La lista debería contener únicamente sitios web en los que confíe plenamentePor ejemplo, añada las páginas web en las que realice compras online.

Para configurar y gestionar la lista blanca antiphishing, haga clic en el enlace **Lista blanca**.Aparecerá una nueva ventana.

Para añadir un sitio a la Lista blanca, escriba la dirección en el campo correspondiente y haga clic en **Añadir**.

Para eliminar un sitio Web de la lista, selecciónelo y haga clic en el enlace **Eliminar** correspondiente.

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

6.1.1. Protección de Bitdefender en el navegador Web

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

- Internet Explorer
- Mozilla Firefox

- Google Chrome
- Safari
- Opera

La barra de herramientas de Bitdefender no es la barra de herramientas típica de su navegador.La única cosa que se agrega a su navegador es un pequeño arrastrador en la parte superior de cada página Web.Haga clic para ver la barra de herramientas.

La barra de herramientas de Bitdefender contiene los siguientes elementos:

Valoración de página

Dependiendo de cómo clasifique Bitdefender la página Web que esté viendo actualmente, se muestra una de siguientes valoraciones en el lado izquierdo de la barra de herramientas:

- El mensaje "Esta página no es segura" aparece sobre un fondo rojo - debería abandonar inmediatamente la página Web.
- El mensaje "Se aconseja precaución" aparece sobre un fondo naranja - esta página Web puede albergar contenidos peligrosos.Tenga cuidado si decide visitarla.
- El mensaje "Esta página es segura" aparece sobre un fondo verde - esta es una página segura para visitar.

SandBox

Haga clic para iniciar el navegador en un entorno proporcionado por Bitdefender, aislándolo del sistema operativo.Esto evita que las amenazas basadas en el navegador exploten las vulnerabilidades de este para obtener el control de su sistema.Utilice Sandbox cuando visite páginas Web que sospecha que pueden contener malware.

Nota
Sandbox no está disponible en equipos con Windows XP.

Configuración

Haga clic en para seleccionar las características individuales que desea activar o desactivar:

- Filtro Antiphishing
- Filtro antimalware
- Asesor de Búsqueda

Interruptor de encendido

Para activar / desactivar las características de la barra de herramientas por completo, haga clic en el lado derecho de la barra de herramientas.

6.1.2. Alertas de Bitdefender en el navegador

Cada vez que intenta visitar un sitio Web clasificado como peligroso, éste queda bloqueado y aparecerá una página de advertencia en su navegador.

La página contiene información tal como la URL del sitio Web y la amenaza detectada.

Tiene que decidir qué hacer a continuación. Están disponibles las siguientes opciones:

- Navegar fuera de la página Web.
- Diríjase a la página Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.
- Añada la página a la lista blanca Antiphishing haciendo clic en **Añadir a lista blanca**.Los motores Antiphishing de Bitdefender ya no analizarán la página.

6.2. Protección de datos

La Protección de datos evita que se produzcan filtraciones de datos sensibles cuando esté conectado online.

Consideremos un ejemplo simple: ha creado una regla de protección de datos que protege su número de tarjeta de crédito.Si se ha instalado de alguna manera software spyware en su equipo, éste no puede enviar su número de tarjeta de crédito a través del correo electrónico, mensajes instantáneos y páginas Web.Por otra parte, sus hijos no podrán usarlo para realizar compras online o revelar información a personas que conocieron en Internet.

Para saber más, por favor diríjase a estos temas:

- "*Acerca de la protección de datos*" (p. 63).
- "*Configurar la protección de datos*" (p. 64).
- "*Administrando las Reglas*" (p. 65).

6.2.1. Acerca de la protección de datos

Tanto si se trata de su dirección de e-mail como de su número de tarjeta de crédito, cuando esta información no cae en buenas manos puede resultar peligrosa: puede ahogarse entre una multitud de mensajes de spam o encontrar vacía su cuenta bancaria.

En base a las reglas que haya creado, la Protección de datos analiza el tráfico de la Web, de sus correos electrónicos y la mensajería instantánea de su equipo en busca de cadenas de caracteres específicos (por ejemplo, su número de tarjeta de crédito). Si hay una coincidencia, se bloqueará la página Web, el correo electrónico o el mensaje instantáneo correspondiente.

Puede crear reglas para proteger cualquier tipo de información que considere personal o confidencial, desde su número de teléfono o e-mail hasta información

de su cuenta bancaria.Se incluye soporte multiusuario para que los usuarios que hayan iniciado sesión en distintas cuentas de usuario de Windows puedan configurar y utilizar sus propias reglas.Si su cuenta de Windows es una cuenta de Administrador, las reglas que cree pueden ser configuradas para que se apliquen también cuando otros usuarios del equipo inician sesión en Windows con sus cuentas.

6.2.2. Configurar la protección de datos

Si desea utilizar la protección de datos, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Control de privacidad** en el menú izquierdo y luego en la pestaña **Protección de datos**.
4. Asegúrese de que está activada la protección de datos.
5. Cree las reglas necesarias para proteger su información personal.Para más información, por favor vea "*Creación de reglas de protección de datos*" (p. 64).

Creación de reglas de protección de datos

Para crear una regla, haga clic en el botón **Añadir regla** y siga el asistente de configuración.Puede navegar a través del asistente utilizando los botón **Siguiente** y **Atrás**.Para salir del asistente, haga clic en **Cancelar**.

1. **Seleccionar el tipo y datos de la regla**

   Debe configurar los siguientes parámetros:

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

     

     Importante
     Si introduce menos de tres caracteres, se le pedirá que valide los datos. Recomendamos escribir por lo menos tres caracteres para evitar confusiones durante el bloqueo de mensajes y páginas web.

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

2. **Seleccionar el Tipo de Tráfico y Usuarios.**

a. Debe seleccionar el tipo de tráfico que Bitdefender analizará.

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

Puede elegir entre aplicar las reglas sólo si los datos de la regla coinciden completamente con las palabras, o si los datos de la regla y la cadena de texto detectada coinciden en mayúsculas y minúsculas.

b. Indique los usuarios para los que desea aplicar la regla.

- **Sólo para mi (actual usuario)** - la regla se aplicará sólo a su cuenta de usuario.
- **Cuentas de usuario limitadas** - la regla se aplicará a usted y a todos las cuentas de Windows limitadas.
- **Todos los usuarios** - La regla se aplicará a todas las cuentas de Windows.

3. **Describa la regla**

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

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

A partir de ahora, fallará cualquier intento de enviar los datos especificados (a través de correo electrónico, mensajería instantánea o en una página Web).Se mostrará una entrada en la ventana de Eventos que indica que Bitdefender ha bloqueado el envío de contenido específico de identidad.

6.2.3. Administrando las Reglas

Para administrar las reglas de protección de datos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Control de privacidad** en el menú izquierdo y luego en la pestaña **Protección de datos**.

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

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

Para editar una regla selecciónela y haga clic en el botón **Editar**. Aparecerá una nueva ventana.Aquí puede cambiar el nombre, la descripción y los parámetros de la regla (tipo, datos y tráfico). Haga clic en **Aceptar** para guardar los cambios.

6.3. Cifrado de Chat

El contenido de sus mensajes instantáneos debe permanecer entre usted y si compañero de chat.Cifrando sus conversaciones, puede asegurarse que nadie será capaz de interceptar el contenido de sus conversaciones desde y hacia sus contactos.

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

- Su compañero de chat tiene un producto Bitdefender instalado que soporta Cifrado de Chat y esta función está activada para la aplicación de mensajería instantánea utilizada para conversar.
- Su contacto de chat utilice Yahoo Messenger o Windows Live (MSN) Messenger.

Importante

Bitdefender no cifrará la conversación si su contacto utiliza una aplicación web para chatear, como Meebo, o si uno de los contactos utiliza Yahoo! y el otro Windows Live (MSN).

Para configurar el cifrado de mensajería instantánea:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Control de privacidad** en el menú izquierdo y luego en la pestaña **Cifrado**.

Por defecto, el Cifrado de Chat está activado para Yahoo Messenger y Windows Live (MSN) Messenger.Puede desactivar el Cifrado de chat para una o ambas aplicaciones haciendo clic en el interruptor correspondiente.

7. Mapa de la Red

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

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

1. Permitir la red de Bitdefender en su equipo.Configurar su equipo como **Equipo servidor**.
2. Diríjase a cada unos de los equipos que desee administrar remotamente y únalos a la red (defina una contraseña).Configurar cada equipo como **Equipo normal**.
3. Vuelva a su equipo y añada los equipos que desee administrar.

7.1. Activando la Red Bitdefender

Para activar la red de Bitdefender, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Mapa de la red** en el menú de la izquierda.
4. Haga clic en **Activar Red**.Se le pedirá configurar la contraseña de administración para el mapa de la red.
5. Introduzca la misma contraseña en cada uno de los campos de texto.
6. Establezca el rol del equipo en el mapa de red Bitdefender:
   - **Equipo Servidor** - seleccione esta opción en el equipo que desea utilizar para administrar los demás.
   - **Equipo normal** - seleccione esta opción en el equipo que será administrado por el equipo servidor.
7. Haga clic en **Aceptar**.

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

   Aparece el botón **Desactivar conexión**.

Nota

También puede activar el mapa de red del desde la ventana principal de Bitdefender:

1. Abra la ventana de Bitdefender.
2. Vaya al panel **Mapa de red**.
3. Haga clic en **Administrar** y seleccione **Activar red** desde el menú desplegable.

7.2. Añadir equipos a la red de Bitdefender

Se añadirá cualquier equipo automáticamente a la red si cumple con el siguiente criterio:

- Se activó el mapa de red de Bitdefender.
- el rol se estableció en un Equipo Esclavo.
- la contraseña establecida cuando activa la red es la misma que la contraseña establecida en el Equipo Servidor.

Nota

En cualquier momento puede analizar el mapa de red de los equipos que cumplan los criterios, haciendo clic en el botón **Autodescubrimiento**.

Para añadir manualmente un equipo a la red de Bitdefender desde el equipo servidor, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Mapa de la red** en el menú de la izquierda.
4. Haga clic en **Añadir Equipo**.
5. Escriba la contraseña de administración y haga clic en **Aceptar**.Aparecerá una nueva ventana.

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

    Indica un equipo conectado con ningún producto Bitdefender instalado.

    Indica un equipo conectado con Bitdefender instalado.

    Indica un equipo desconectado con Bitdefender instalado.

6. Realice una de estas acciones:
   - Seleccione un equipo de la lista para añadirlo.
   - Introduzca la dirección IP o el nombre del equipo a añadir en el campo editable correspondiente.
7. Haga clic en **Añadir**.
8. Introduzca la contraseña de administración configurada en el equipo correspondiente.
9. Haga clic en **Aceptar**.Si ha introducido la contraseña correcta, el nombre del equipo seleccionado aparecerá en el mapa de la red.

7.3. Administrando la Red de Bitdefender

Una vez que haya creado con éxito un mapa de red de Bitdefender, podrá gestionar todos los productos de Bitdefender desde el equipo servidor.

Para ejecutar varias tareas en todos los equipos administrados, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Vaya al panel **Mapa de red**.
3. Haga clic en **Administrar** y seleccione el botón correspondiente en el menú desplegable:
   - **Desactivar la conexión** - le permite desactivar la red.
   - **Analizar Todos** - le permite analizar todos los equipos administrados a la vez.
   - **Actualizar Todos** - le permite actualizar todos los equipos administrados a la vez.

Antes de ejecutar una tarea en un equipo determinado, se le solicitará la contraseña de administración local.Escriba la contraseña de administración y haga clic en **Aceptar**.

Para ver el Mapa de red completo y acceder a todas las tareas de administración siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Mapa de la red** en el menú de la izquierda.

Si mueve el cursor del ratón encima de un equipo del mapa de la red, podrá ver una breve información sobre este equipo (dirección IP, número de incidencias que afectan a la seguridad del sistema, estado de registro de Bitdefender).

Si hace clic en el nombre del equipo del mapa de red, puede ver todas las tareas administrativas que pueden ejecutarse en un equipo remoto.

Registrar producto
Permite registrar Bitdefender en este equipo introduciendo una licencia.

Establecer contraseña para la configuración
Permite crear una contraseña para restringir el acceso a la configuración de Bitdefender en este PC.

Ejecutar una tarea de Análisis bajo demanda
Le permite ejecutar un análisis bajo demanda en el equipo remoto. Puede realizar cualquiera de las siguientes tareas de análisis: Quick Scan o Análisis Completo del sistema.

Reparar Todo

Le permite reparar todas las incidencias que están afectando a la seguridad de este equipo siguiendo el asistente Reparar Todas.

Ver eventos

Le permite acceder en este equipo al módulo **Eventos** en el producto instalado de Bitdefender.

Actualizar

Inicie el proceso de Actualización para este producto de Bitdefender instalado en este equipo.

Establecer como servidor de actualizaciones

Permite establecer este equipo como servidor de actualización para todos los productos Bitdefender instalados en los equipos de esta red.Utilice esta opción para reducir el tráfico de Internet, porque sólo se conectará un equipo de esta red a Internet para descargar las actualizaciones.

Eliminar PC del mapa de red

Permite eliminar un PC de la red.

Nota

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

8. Actualización

Cada día se encuentran nuevas amenazas de malware. Por esta razón es muy importante mantener Bitdefender actualizado con las últimas firmas de malware.

Si está conectado a Internet a través de una conexión de banda ancha o ADSL, Bitdefender se actualizará sólo. Por defecto, comprueba si existen nuevas actualizaciones al encender su equipo y a cada **hora** a partir de ese momento.Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

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

Importante

Para estar protegido contra las últimas amenazas mantenga activo Actualización automática.

En algunas situaciones particulares, se precisa su intervención para mantener la protección de su Bitdefender actualizada:

- Si su equipo se conecta a Internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en "*¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?*" (p. 33).
- Si no dispone de una conexión a Internet, puede actualizar Bitdefender manualmente como se describe en "*Mi equipo no está conectado a Internet. ¿Cómo actualizo Bitdefender?*" (p. 79).El archivo de actualización manual se publica una vez por semana.
- Pueden producirse errores durante la descarga de actualizaciones en una conexión a Internet lenta.Para descubrir como superar dichos errores, por favor consulte "*Cómo actualizo Bitdefender en una conexión de internet lenta*" (p. 78).
- Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente.Para más información, por favor vea "*Realizar una actualización*" (p. 72).

8.1. Comprobar si Bitdefender está actualizado

Para comprobar si la protección de Bitdefender está actualizada, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Diríjase al panel **Actualizar**.
3. La hora de la última actualización se muestra justo debajo del nombre del panel.

Para obtener información detallada sobre las últimas actualizaciones, compruebe los eventos de actualización:

1. En la ventana principal, haga clic en **Eventos** en la barra de herramientas superior.
2. Haga clic en **Actualizar** en el menú izquierdo.

Puede saber cuándo se iniciaron las actualizaciones y obtener información sobre ellas (si se realizaron con éxito o no, si requieren reiniciar para completar la instalación).Si es necesario, reinicie el sistema en cuanto pueda.

8.2. Realizar una actualización

Para poder hacer actualizaciones es necesaria una conexión a Internet.

Para iniciar una actualización, haga cualquier cosa de las siguientes:

- Abra la ventana de Bitdefender, diríjase al panel **Actualización** y haga clic en **Actualizar ahora**.
- Haga clic derecho en el icono Bitdefender  en el área de notificación y seleccione **Actualizar**.

El módulo Actualizar conectará con el servidor de actualización de Bitdefender y comprobará la existencia de actualizaciones.Al detectar una actualización se le solicitará su confirmación para instalarla, o bien podrá realizarse de forma automática dependiendo de lo haya definido en la Configuración de actualización.

Importante

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

8.3. Activar o desactivar la actualización automática

Para activar o desactivar las actualizaciones automáticas, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Diríjase al panel **Actualizar**.
3. Haga clic en el conmutador para activar o desactivar las Actualizaciones automáticas.
4. Si decide desactivar la actualización automática, aparecerá una ventana de advertencia.Para confirmar su elección, deberá seleccionar durante cuanto tiempo desea desactivar la actualización. Puede desactivar la actualización durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

Aviso

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

8.4. Ajustar las opciones de actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy. Por defecto, Bitdefender comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

La configuración de actualizaciones predeterminada se ajusta a la mayoría de usuarios y normalmente no tiene que cambiarla.

Para configurar las opciones de actualización, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Actualizar** en el menú izquierdo.
4. Ajuste las opciones según sus preferencias.

Ubicación de la actualización

Bitdefender esta configurado para actualizarse desde los servidores de actualización en Internet de Bitdefender.La ubicación de actualización es `http://upgrade.bitdefender.com`, una dirección genérica de Internet que es automáticamente redirigida al servidor de actualización más cercano de Bitdefender en su región.

No modifique la ubicación de actualización a no ser que así se lo indique un representante de Bitdefender o por su administrador de red (si está conectado a la red de una oficina).

Si ha instalado Bitdefender en varios equipos en su hogar, puede configurar una red doméstica Bitdefender y designar uno de sus equipos como el servidor de actualizaciones.Se proporciona información detallada en "*Mapa de la Red*" (p. 67).El programa Bitdefender instalado en el servidor designado de actualización se actualizará desde Internet. Los programas Bitdefender en otros equipos obtendrán las actualizaciones desde el servidor de actualización local (su ubicación de actualización se cambia automáticamente de forma acorde).Esta configuración tiene la intención de minimizar el tráfico de Internet y optimizar las actualizaciones.

Puede cambiar a la ubicación de actualización en Internet por defecto haciendo clic en **Predeterminado**.

Reglas de proceso de actualización

Puede elegir entre tres modos de descargar e instalar actualizaciones:

- **Actualización silenciosa** - Bitdefender descarga e instala las actualizaciones automáticamente.
- **Preguntar antes de descargar** - cada vez que exista una actualización disponible, se le consultará si desea descargarla.
- **Preguntar antes de instalar** - cada vez que se haya descargado una actualización, se le pedirá permiso para instalarla.

Algunas actualizaciones necesitan reiniciar el sistema para completar la instalación.Si una actualización necesita reiniciar el sistema, de forma predeterminada Bitdefender seguirá utilizando los archivos antiguos hasta que el usuario reinicie voluntariamente el equipo. Esto es así para evitar que el proceso de actualización de Bitdefender interfiera con el trabajo del usuario.

Si quiere que se le pregunte cuando una actualización requiera un reinicio, desactive la opción **Posponer reinicio** haciendo clic en el conmutador correspondiente.

Actualizaciones P2P

Además del mecanismo de actualización habitual, Bitdefender también utiliza un inteligente sistema para compartir actualizaciones basado en el protocolo peer-to-peer (P2P) para distribuir actualizaciones de firmas de malware entre usuarios de Bitdefender.

Puede activar o desactivar las opciones de actualización P2P usando los conmutadores correspondientes.

Usar sistema de actualización P2P

Active esta opción para descargar actualizaciones de firmas de malware desde otros usuarios de Bitdefender que utilicen un sistema de actualización P2P.Bitdefender usa los puertos 8880 - 8889 para la actualización peer-to-peer.

Distribuir archivos Bitdefender

Active esta opción para compartir las últimas firmas de malware disponibles en su equipo con otros usuarios de Bitdefender.

9. Protección SafeGo para las redes sociales

Confía en sus amigos online.Pero, ¿confía usted en sus equipos?Utilice la protección SafeGo en las redes sociales para proteger su cuenta y a sus amigos frente a las amenazas online.

SafeGo es una aplicación de Facebook desarrollada por Bitdefender para mantener su cuenta de red social segura.Su función consiste en analizar los enlaces que recibe de sus amigos de Facebook y controlar la configuración de privacidad de su cuenta.

Nota

Para poder utilizar esta función es necesario disponer de una cuenta MyBitdefender. Para más información, por favor vea *"Registro"* (p. 8).

Estas son sus principales características:

- Analiza automáticamente los mensajes en su News feed en busca de enlaces maliciosos.
- Protege su cuenta contra las amenazas online.

  Cuando se detecte un mensaje o un comentario que es spam, phishing o malware, recibirá un mensaje de advertencia.
- advierte a sus amigos sobre enlaces sospechosos publicados en sus News Feed.
- Le ayuda a construir una red segura de amigos utilizando la función **Amig'O'metro**.
- Realice una verificación del estado de seguridad del sistema por medio de QuickScan de Bitdefender.

Para acceder a SafeGo desde su producto Bitdefender, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Diríjase al panel **SafeGo**.
3. Haga clic en **Activar**.Será redirigido a su cuenta.

   Si ya ha activado SafeGo, podrá acceder a las estadísticas relacionadas con su actividad haciendo clic en el botón **Ver informes**.
4. Utilice su información de inicio de sesión de Facebook para conectarse a la aplicación SafeGo.
5. Permita el acceso de SafeGo a su cuenta de Facebook.

10. Resolución de Problemas

Este capítulo presenta algunos problema que puede encontrar cuando utiliza Bitdefender y le proporciona las posibles soluciones para estos problemas.La mayoría de estos problemas pueden ser resueltos a través de la configuración apropiada de los ajustes del producto.

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Soporte*" (p. 92).

10.1. Mi sistema parece que se ejecuta lento

Normalmente, después de instalar un software de seguridad, puede aparecer una ligera ralentización del sistema, lo cual en cierto punto es normal.

Si nota una lentitud significativa, esta incidencia puede aparecer por las siguientes razones:

- **Bitdefender no es solo un programa de seguridad instalado en el sistema.**

  Aunque Bitdefender busque y elmine los programas de seguridad encontrados durante la instalación, recomendamos eliminar cualquier otro programa antivirus utilizado antes de instalar Bitdefender.Para más información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 98).

- **No se cumplen los requisitos mínimos del sistema para ejecutar Bitdefender.**

  Si su PC no cumple con los requisitos mínimos del sistema, el equipo se ralentiza, especialmente cuando se ejecutan múltiples aplicaciones al mismo tiempo.Para más información, por favor vea "*Requisitos mínimos del sistema*" (p. 1).

- **Sus unidades de disco duro están demasiado fragmentadas.**

  La fragmentación de archivo ralentiza el acceso a archivos y baja rendimiento del sistema.

Para desfragmentar su disco utilizando su sistema operativo Windows, siga la ruta desde el menú de Inicio de Windows: **Inicio → Todos los programas → Accesorios → Herramientas del Sistema → Desfragmentador de Disco**.

10.2. El análisis no se inicia

Este tipo de incidencia puede tener dos causas principales:

- **Una instalación anterior de Bitdefender la cual no fue desinstalada completamente o es una instalación Bitdefender defectuoso**.

  En este caso, siga estos pasos:

  1. Desinstalar Bitdefender completamente del sistema:
     a. Diríjase a http://www.bitdefender.com/uninstall y descargue la herramienta de desinstalación en su equipo.
     b. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.
     c. Reinicie el equipo.
  2. Reinstalar Bitdefender en el sistema.

- **Bitdefender no es solo una solución de seguridad instalada en su sistema**.

  En este caso, siga estos pasos:

  1. Eliminar las otras soluciones de seguridad.Para más información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 98).
  2. Desinstalar Bitdefender completamente del sistema:
     a. Diríjase a http://www.bitdefender.com/uninstall y descargue la herramienta de desinstalación en su equipo.
     b. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.
     c. Reinicie el equipo.
  3. Reinstalar Bitdefender en el sistema.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

10.3. Ya no puedo usar una aplicación

Esta incidencia ocurre cuando está intentado utilizar un programa el cual estaba trabajando de forma normal antes de instalar Bitdefender.

Es posible que encuentre una de estas situaciones:

- Puede recibir un mensaje de Bitdefender que el programa está intentando realizar una modificación en el sistema.
- Puede recibir un mensaje de error del programa que intentando usar.

Este tipo de situación ocurre cuando el módulo Active Virus Control erróneamente detecta algunas aplicaciones como maliciosas.

Active Virus Control es un módulo de Bitdefender el cual monitoriza constantemente las aplicaciones en ejecución en su sistema e informa del comportamiento malicioso potencial de estas.Puesto que esta característica se basa en un sistema heurístico, puede haber casos en que las aplicaciones legitimas son informadas por Active Virus Control.

Cuando ocurre esta situación, puede excluir la aplicación respectiva de ser monitorizado por Active Virus Control.

Para añadir el programa a la lista de exclusiones, siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Exclusiones**.
4. Haga clic en el enlace **Procesos excluidos**.En la ventana que aparece puede administrar las exclusiones de procesos Active Virus Control.
5. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **Añadir** ubicado en la parte superior de la tabla de exclusiones.
   b. Haga clic en **Examinar**, busque y seleccione la aplicación a excluir y a continuación haga clic en **Aceptar**.
   c. Mantenga seleccionada la opción **Permitir** para evitar que Active Virus Control bloquee la aplicación.
   d. Haga clic en **Añadir**.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección “*Pedir ayuda*” (p. 93).

10.4. Cómo actualizo Bitdefender en una conexión de internet lenta

Si tiene una conexión a Internet lenta (tales como acceso telefónico), pueden ocurrir errores durante el proceso de actualización.

Para mantener su sistema actualizado con las últimas firmas de malware de Bitdefender, siga estos pasos:

1. Abra la ventana de Bitdefender.

2. Haga clic en el botón **Configuración** en la barra de herramientas superior.
3. Haga clic en **Actualizar** en el menú izquierdo y luego en la pestaña **Actualizar**.
4. Bajo **Reglas de proceso de actualización**, seleccione **Preguntar antes de descargar**.
5. Haga clic en el botón **Inicio** en la barra de herramientas superior.
6. Vaya al panel **Actualizar** y haga clic en **Actualizar ahora**.
7. Seleccione solo **Actualizaciones de Firmas** y haga clic en **Ok**.
8. Bitdefender descargará e instalará solo las actualizaciones de firmas de malware.

10.5. Mi equipo no está conectado a Internet. ¿Cómo actualizo Bitdefender?

Si su equipo no está conectado a Internet, debe descargar las actualizaciones manualmente a su equipo con acceso a Internet y luego transferir estas a su equipo utilizando un dispositivo extraíble, tales como una unidad flash.

Siga estos pasos:

1. En un equipo con acceso a Internet, abra un navegador y vaya a:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. En la columna **Actualización Manual**, haga clic en el enlace correspondiente a su producto y a la arquitectura del sistema.Si no sabe si su Windows se ejecuta en 32 o 64 bits, por favor consulte "*¿Estoy utilizando una versión de Windows de 32 o 64 bit?*" (p. 99).
3. Guarde el archivo llamado `weekly.exe` para el sistema.
4. Transferir el archivo descargado a un dispositivo extraíble, como una unidad de flash, y luego a su equipo.
5. Haga doble clic en el archivo y siga los pasos del asistente.

10.6. Los servicios de Bitdefender no responden

Este artículo le ayuda a solucionar problemas del error de **Los servicios de Bitdefender no responden**.Puede encontrar este error de la siguiente manera:

- El icono Bitdefender del área de notificación está en gris y se le informa de que los servicios de Bitdefender no responden.
- La ventana de Bitdefender le indica que los servicios de Bitdefender no responden.

El error puede ser causado por una de las siguientes condiciones:

- una actualización importante esta instalándose.
- Errores temporales de comunicación entre los servicios de Bitdefender.

- algunos de los servicios de Bitdefender están detenidos.
- otras soluciones de seguridad se están ejecutando en su equipo al mismo tiempo que Bitdefender.

Para solucionar este problema, pruebe estas soluciones:

1. Espere unos momentos y mire si algo cambia.El error puede ser temporal.
2. Reinicie el equipo y espere unos momentos a que Bitdefender se inicie. Abra Bitdefender para ver si el error continua.Reiniciando el equipo normalmente soluciona el problema.
3. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la ejecución normal de Bitdefender. Si este es el caso, le recomendamos que elimine todas las otras soluciones de seguridad y reinstale Bitdefender.

   Para más información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 98).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 93).

10.7. La desinstalación de Bitdefender ha fallado

Este artículo le ayuda a solucionar los problemas de errores que pueden ocurrir cuando desinstala Bitdefender.Existen dos situaciones posibles:

- Durante la desinstalación, aparece un error en pantalla.La pantalla proporciona un botón para ejecutar una herramienta de desinstalación que limpiará el sistema.
- La instalación se cuelga y, probablemente, su equipo se pare.Haga clic en **Cancelar** para abortar la desinstalación. Si esto no funciona, reinicie el sistema.

Si la desinstalación falla, alguna claves de registro y archivos de Bitdefender pueden permanecer en su sistema. Tales restos pueden impedir una nueva instalación de Bitdefender. Estas también pueden afectar al rendimiento y estabilidad del sistema.

Para eliminar por completo Bitdefender de su sistema, siga estos pasos:

1. Diríjase a http://www.bitdefender.com/uninstall y descargue la herramienta de desinstalación en su equipo.
2. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.
3. Reinicie el equipo.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

10.8. Mi sistema no se inicia tras la instalación de Bitdefender

Si acaba de instalar Bitdefender y no puede reiniciar más su sistema en modo normal hay varias razones por las cuales puede pasar esto.

Lo más probable es que esto lo haya causado una instalación previa de Bitdefender que no fue desinstalada correctamente o por otra solución de seguridad que todavía está presente en el sistema.

Así es como puede abordar cada situación:

- **Ya tenía Bitdefender anteriormente y no lo desinstaló correctamente.**

  Para solucionarlo, siga estos pasos:

  1. Reinicie su sistema e inicie en Modo Seguro.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 99).
  2. Desinstalar Bitdefender de su sistema:
     a. Diríjase a http://www.bitdefender.com/uninstall y descargue la herramienta de desinstalación en su equipo.
     b. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.
     c. Reinicie el equipo.
  3. Reinicie su sistema en modo normal y reinstale Bitdefender.

- **Antes tenía instalada una solución de seguridad y no fue eliminada correctamente.**

  Para solucionarlo, siga estos pasos:

  1. Reinicie su sistema e inicie en Modo Seguro.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 99).
  2. Desinstalar Bitdefender de su sistema:
     a. Diríjase a http://www.bitdefender.com/uninstall y descargue la herramienta de desinstalación en su equipo.
     b. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.
     c. Reinicie el equipo.
  3. Para desinstalar correctamente el otro programa, diríjase a su sitio Web y ejecute su herramienta de desinstalación o contacte con ellos directamente para que le proporcionen las indicaciones para desinstalar.
  4. Reinicie su sistema en modo normal y reinstale Bitdefender.

Ya ha seguido los pasos anteriores y la situación no se ha solucionado.

Para solucionarlo, siga estos pasos:

1. Reinicie su sistema e inicie en Modo Seguro.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 99).
2. Utilice la opción Restaurar sistema de Windows para restaurar el equipo a un punto anterior antes de la instalación del producto Bitdefender.Para saber como se hace esto, por favor diríjase a "*¿Cómo uso la restauración del sistema en Windows?*" (p. 100).
3. Reinicie el sistema de modo normal y contacte con nuestros represetantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 93).

11. Eliminando malware de su sistema

El Malware puede afectar a su sistema de diferentes maneras y Bitdefender lo enfoca dependiendo del tipo de ataque de malware.Porque los virus cambian su comportamiento frecuentemente, esto dificulta establecer un patrón de comportamiento y sus acciones.

Existen situación en las que Bitdefender no puede eliminar automáticamente la infección de malware de su sistema.En cada caso, su intervención es requerida.

- "*Modo Rescate Bitdefender*" (p. 83)
- "*¿Qué hacer cuando Bitdefender encuentra virus en su equipo?*" (p. 85)
- "*¿Cómo limpiar un virus en un archivo?*" (p. 86)
- "*¿Cómo limpio un virus en un archivo de correo?*" (p. 87)
- "*¿Qué hacer si sospecho que un archivo es peligroso?*" (p. 88)
- "*Cómo limpiar los archivos infectados de la carpeta System Volume Information*" (p. 88)
- "*¿Qué son los archivos protegidos con contraseña del registro de análisis?*" (p. 90)
- "*¿Qué son los elementos omitidos en el registro de análisis?*" (p. 90)
- "*¿Qué son los archivos sobre-comprimidos en el registro de análisis?*" (p. 90)
- "*¿Por qué eliminó Bitdefender automáticamente un archivo infectado?*" (p. 91)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Soporte*" (p. 92).

11.1. Modo Rescate Bitdefender

El **modo de Rescate** es una opción de Bitdefender que le permite analizar y desinfectar todas las particiones existentes del disco duro fuera de su sistema operativo.

Una vez que Bitdefender Antivirus Plus 2012 está instalado, puede utilizar el modo Rescate incluso si no es capaz de arrancar en Windows.

Iniciar el sistema en modo Rescate

Puede acceder al Modo Rescate de dos maneras:

Desde la ventana de Bitdefender

Para entrar en el modo Rescate directamente desde Bitdefender, siga estos pasos:

1. Ir al panel **Antivirus**.
2. Haga clic en **Analizar** y seleccione el **Modo Rescate** en el menú desplegable.

   Aparecerá una ventana de confirmación. Haga clic en **Sí** para reiniciar su equipo.
3. Una vez que reinicie su equipo, aparecerá un menú que le pedirá que seleccione un sistema operativo.Elija **Imagen de rescate Bitdefender** y pulse la tecla **Intro** para arrancar en un entorno de Bitdefender desde donde se podrá limpiar la partición de Windows.
4. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente.A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Inicie su equipo directamente desde el modo Rescate.

Si Windows no se inicia, puede arrancar su equipo directamente en el modo Rescate de Bitdefender, siguiendo los pasos detallados a continuación.

Nota

Este método no está disponible en equipos que ejecuten Windows XP.

1. Inicie / reinicie su equipo y empiece a presionar la **barra espaciadora** en el teclado antes de que aparezca el logotipo de Windows.
2. Aparecerá un menú que le pedirá que seleccione un sistema operativo para iniciar su equipo.Presione **TAB** para ir al área de herramientas.Elija **Imagen de rescate Bitdefender** y pulse la tecla **Intro** para arrancar en un entorno de Bitdefender desde donde se podrá limpiar la partición de Windows.
3. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente.A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Analizando su sistema en modo Rescate

Para analizar el sistema en Modo Rescate, siga estos pasos:

1. Acceda al Modo Rescate, como se describe en “Iniciar el sistema en modo Rescate” (p. 83).
2. El logotipo de Bitdefender aparecerá y se empezarán a copiar los motores del antivirus.
3. Aparecerá una ventana de bienvenida.Haga clic en **Continuar**.
4. Se ha iniciado una actualización de las firmas de antivirus.

5. Tras completarse la actualización, aparecerá la ventana del Análisis de Antivirus de Bitdefender.
6. Haga clic en **Analizar**, seleccione el objeto de análisis en la ventana que aparece y haga clic en **Abrir** para iniciar el análisis.

   Se recomienda analizar toda su partición de Windows.

   

   Nota

   Cuando trabaja en modo Rescate, trata con nombres de particiones de tipo Linux.Las particiones de disco aparecerán como `sda1`, probablemente correspondiendo con el tipo de partición de Windows `(C:)`, `sda2` que se corresponde con `(D:)` y así sucesivamente.

7. Espere a que el análisis se complete. Si se detecta cualquier tipo de malware, siga las instrucciones para eliminar la amenaza.
8. Para salir del modo Rescate, haga clic con el botón derecho en un área vacía del escritorio, seleccione **Salir de la sesión** en el menú que aparece a continuación y elija si desea reiniciar o apagar el equipo.

11.2. ¿Qué hacer cuando Bitdefender encuentra virus en su equipo?

Puede darse cuenta que hay un virus en su equipo de una de estas maneras.

- Ha analizado su equipo y Bitdefender ha encontrado elementos infectados en el.
- Una alerte de virus le informa que Bitdefender ha bloqueado uno múltiples virus en su equipo.

En estas situaciones, actualice Bitdefender para asegurarse de que tiene las últimas firmas de virus y ejecute un Análisis completo para analizar el sistema.

Tan pronto como acabe el análisis en profundidad, seleccione la acción deseada para los elementos infectados (Desinfectar, Eliminar, Trasladar a cuarentena).

Aviso

Si sospecha que el archivo es parte del sistema operativo Windows o que este no es un archivo infectado, no siga estos pasos y contacte con Atención al Cliente de Bitdefender lo antes posible.

Si la acción seleccionado no puede realizarse y el log de análisis muestra una infección la cual no puede ser eliminada, tiene que eliminar el archivo(s) manualmente:

El primer método puede ser utilizado en modo normal:

1. Desactive la protección antivirus en tiempo real de Bitdefender:

a. Abra la ventana de Bitdefender.

b. Haga clic en el botón **Configuración** en la barra de herramientas superior.

c. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.

d. Haga clic en el conmutador para apagar el **análisis on-access**.

2. Muestra los objetos ocultos en Windows.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 100).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Active la protección antivirus en tiempo real de Bitdefender.

En caso de que el primer método falle para eliminar la infección, siga estos pasos:

1. Reinicie su sistema e inicie en Modo Seguro.Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 99).
2. Muestra los objetos ocultos en Windows.
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

11.3. ¿Cómo limpiar un virus en un archivo?

Una archivo es un archivo o una colección de archivos comprimidos bajo un formato especial para reducir el espacio en disco necesario para guardar los archivos.

Algunos de estos formatos son formatos abiertos, proporcionando así Bitdefender la opción de análisis dentro de ellos y luego tomar las acciones apropiadas para eliminar estos.

Otros formatos de archivo están partidos o cerrados completamente, y Bitdefender puede solo detectar la presencia de virus dentro de ellos, pero no es capaz de realizar ninguna otra acción.

Si Bitdefender notifica que se ha detectado un virus dentro de un archivo y no hay ninguna acción disponible, significa que no es posible eliminar el virus debido a la configuración de permisos del archivo.

Aquí es donde puede limpiar un virus guardado en un archivo:

1. Identifica el archivo que incluye el virus realizando un Análisis Completo del sistema.
2. Desactive la protección antivirus en tiempo real de Bitdefender:

a. Abra la ventana de Bitdefender.

b. Haga clic en el botón **Configuración** en la barra de herramientas superior.

c. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.

d. Haga clic en el conmutador para apagar el **análisis on-access**.

3. Vaya a la ubicación del archivo y descomprímalo utilizando una aplicación de descompresión de archivos, como WinZip.
4. Identifique el archivo infectado y elimínelo.
5. Elimine el archivo original con el fin de asegurar que la infección está eliminada totalmente.
6. Recomprime los archivos en nuevo archivo utilizando una aplicación de compresión, como WinZip.
7. Active la protección antivirus en tiempo real de Bitdefender y ejecute un análisis en Profundidad del sistema con el fin de asegurarse que no existe ninguna otra infección en el sistema.

Nota

Es importante señalar que un virus guardado en un archivo no es una amenaza inmediata a su sistema, ya que el virus tiene que ser descomprimido y ejecutado con el fin de infectar su sistema.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

11.4. ¿Cómo limpio un virus en un archivo de correo?

Bitdefender también puede identificar virus en las bases de datos de correo y archivos de correos guardados en disco.

Algunas veces es necesario para identificar el mensaje infectados utilizando la información proporcionada por el informe de análisis, y eliminarlo manualmente.

Aquí es donde puede limpiar un virus almacenado en un archivo de correo:

1. Analizar la base de datos de correo con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:

a. Abra la ventana de Bitdefender.

b. Haga clic en el botón **Configuración** en la barra de herramientas superior.

c. Haga clic en **Antivirus** en el menú izquierdo y luego en la pestaña **Residente**.

d. Haga clic en el conmutador para apagar el **análisis on-access**.

3. Abra el informe de análisis y utilice la información de identificación(Asunto, De, Para) de los mensajes infectados para localizarlos en el cliente de correo.

4. Elimina los mensajes infectados.Muchos de los clientes de correo puede mover los mensajes eliminados a la carpeta de recuperación, desde donde se pueden recuperar.Debería asegurarse que el mensaje también se eliminará de esta carpeta de recuperación.
5. Compactar la carpeta que almacena el mensaje infectado.
   - En Outlook Express:En el menú Archivo, clic en Carpeta, y luego Compactar Todas las Carpetas.
   - En Microsoft Outlook:En el Menú Archivo, haga clic Administración de Datos de Archivo.Seleccione los archivos (.pst) de las carpetas personales para intentar compactar, y haga clic en Configuración. Haga clic en Compactar.
6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

11.5. ¿Qué hacer si sospecho que un archivo es peligroso?

Puede sospechar que un archivo de su sistema es peligroso, incluso aunque su producto Bitdefender no lo haya detectado.

Para asegurase de que su sistema está protegido, siga estos pasos:

1. Ejecute un **Análisis Completo del Sistema** con Bitdefender.Para saber como se hace esto, por favor diríjase a "*¿Cómo analizo mi sistema?*" (p. 30).
2. Si el resultado del análisis parece limpio, pero todavía tiene dudas y quiere asegurarse sobre la naturaleza del archivo, contacte con nuestros representantes de soporte de forma que puedan ayudarle.

   Para saber como se hace esto, por favor diríjase a "*Pedir ayuda*" (p. 93).

11.6. Cómo limpiar los archivos infectados de la carpeta System Volume Information

La carpeta de Información de Volumen de Sistema es una zona de su disco curo creado por el Sistema Operativo y utilizado por Windows para guardar información crítica relacionada con la configuración del sistema.

Los motores de Bitdefender pueden detectar cualquier archivo infectado guardado por el System Volume Information, pero al ser una área protegido no es posible eliminarlos.

Los archivos infectados detectados en las carpetas de Restauración de Sistema aparecerán en el log de análisis de la siguiente forma:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Para completar e inmediatamente eliminar el archivo o archivos infectados en el almacenan datos, desactive y vuelva a activar la característica de Restaurar Sistema.

Cunado la Restauración del Sistema esta desactivada, todos los puntos de restauración son eliminados.

Cuando se vuelve a activar la Restauración del Sistema, los nuevos puntos de restauración están creados como requieren los eventos y programados.

Con el fin de desactivar la Restauración del Sistema siga estos pasos:

- **Para Windows XP:**
  1. Siga esta ruta: **Inicio → Todos los Programas → Accesorios → Herramientas del Sistema → Restaurar Sistema**
  2. Haga clic en **Configuración Restaurar Sistema** ubicado en la parte izquierda de la ventana.
  3. Seleccione la casilla **Desactivar Restaurar Sistema** en todas las unidades y haga clic en **Aplicar**.
  4. Cuando se le avisa que todos los Puntos de Restauración existentes serán eliminados, haga clic en **Si** para continuar.
  5. Para activar la Restauración de Sistema, desmarque la casilla **Desactivar Restauración del Sistema** en todas las unidades, y haga clic en **Aplicar**.
- **Para Windows Vista:**
  1. Siga esta ruta: **Inicio → Panel de Control → Sistema y Mantenimiento → Sistema**
  2. En el panel izquierdo, haga clic **Protección de Sistema**.

     Si se le pide una contraseña de administrador o confirmación, escriba la contraseña o proporcione la confirmación.
  3. Para desactivar la Restauración del Sistema desmarque la casilla correspondiente a cada unidad y haga clic en **Ok**.
  4. Para activar Restaurar Sistema seleccione la casilla correspondiente para cada unidad y haga clic en **Ok**.
- **Para Windows 7:**
  1. Haga clic en **Inicio**, clic derecho en **Equipo** y clic en **Propiedades**.
  2. Haga clic en **Protección de Sistema** en el panel izquierdo.
  3. En las opciones de **Protección de Sistema**, seleccione cada letra de unidad y haga clic en **Configurar**.
  4. Seleccione **Desconectar protección del sistema** y haga clic en **Aplicar**.

5. Haga clic en **Eliminar**, haga clic en **Continuar** cuando se le solicite y luego haga clic en **Ok**.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 93).

11.7. ¿Qué son los archivos protegidos con contraseña del registro de análisis?

Esto es solo una notificación la cual indica que Bitdefender ha detectado estos archivos y están protegidos con una contraseña o por alguna forma de cifrado.

Por lo general, los elementos protegidos con contraseña son:

- Archivos que pertenecen a otra solución de seguridad.
- Archivos que pertenecen al sistema operativo.

Con el fin de analizar el contenido, estos archivos necesitan ser extraídos o descifrados.

En caso de que dicho contenido sea extraído, Bitdefender análisis en tiempo real analizará automáticamente estos para mantener su equipo protegido.Si desea analizar estos archivos con Bitdefender, tiene que contactar con el fabricante del producto con el fin de que le proporcione más detalles de estos archivos.

Nuestra recomendación es que ignore estos archivos porque no son amenazas para su sistema.

11.8. ¿Qué son los elementos omitidos en el registro de análisis?

Todos los archivos que aparecen como Omitidos en el informe de análisis están limpios.

Para incrementar el rendimiento, Bitdefender no analiza archivos que no han sido cambiados desde el último análisis.

11.9. ¿Qué son los archivos sobre-comprimidos en el registro de análisis?

Los elementos sobrecomprimidos son elementos los cuales no pueden ser extraídos por el motor de análisis o elementos los cuales el tiempo de descifrado ha tomado demasiado tiempo haciendo el sistema inestable.

Los medios sobrecomprimidos que Bitdefender omite el análisis dentro de ese archivo, porque desempaquetando este tomó demasiados recursos del sistema. El contenido será analizado al acceder en tiempo real si es necesario.

11.10. ¿Por qué eliminó Bitdefender automáticamente un archivo infectado?

Si se detecta un archivo infectado, Bitdefender intentará desinfectarlo automáticamente.Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

Este es normalmente el caso con archivos de instalación que son descargados de sitios web no fiables.Si se encuentra en tal situación, descargue el archivo de instalación desde la página web del fabricante u otra página web de confianza.

12. Pedir ayuda

12.1. Soporte

Bitdefender se esfuerza en proporcionar a sus clientes un incomparable soporte rápido y eficiente.Si está experimentando cualquier incidencia o si tiene cualquier pregunta sobre su producto Bitdefender, puede utilizar varios recursos online para encontrar rápidamente una solución una respuesta.O, si lo prefiere, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

12.1.1. Recursos online

Hay varios recursos online disponibles para ayudarle a resolver sus problemas y preguntas relacionadas con Bitdefender.

- Centro de soporte de Bitdefender:http://www.bitdefender.es/site/Main/contactForm/
- Foro de Soporte de Bitdefender:http://forum.bitdefender.com
- el portal de seguridad informática Malware City:http://www.malwarecity.es

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad informática, los productos Bitdefender y la compañía.

Centro de soporte de Bitdefender

El Centro de soporte Bitdefender es una librería de información online sobre el producto Bitdefender.Almacena en un formato de fácil acceso los informes sobre los resultados de las actividades de soporte técnico en curso y de resolución de errores ofrecidas por el soporte y los equipos de desarrollo de Bitdefender, junto con artículos más generales sobre la prevención de virus, la administración de soluciones Bitdefender, con explicaciones detalladas y muchos otros artículos.

El Centro de soporte Bitdefender está abierto al público y puede consultarse gratuitamente.La amplia información que contiene es otro medio de proporcionar a los clientes de Bitdefender los conocimientos técnicos y comprensión que necesitan.Todas las solicitudes válidas de información o informes de errores provenientes de los clientes Bitdefender, finalmente acaban en el Centro de soporte de Bitdefender, como informes de resolución de errores, documentos técnicos o artículos informativos para complementar los archivos de ayuda del producto.

El Centro de soporte Bitdefender está siempre disponible en http://www.bitdefender.es/site/Main/contactForm/.

Foro de Soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una manera fácil para obtener ayuda y ayudar a otros.

Si su producto Bitdefender no funciona bien, si no puede eliminar virus específicos de su equipo o si tiene preguntas sobre de que manera trabaja, escriba su problema o pregunta en el foro.

El soporte técnico de Bitdefender monitoriza el foro para nuevos posts con el fin de asistirle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de postear su problema o pregunta, por favor, busque en el foro un tema similar o relacionado.

El Foro de Soporte de Bitdefender está disponible en http://forum.bitdefender.com, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano.Haga clic en el enlace **Protección Doméstica** para acceder a la sección dedicada a los productos de consumo.

Portal Malware City

El portal de Malware City es un rico recurso de información para la seguridad de equipos. Aquí puede saber las varias amenazas a las que está expuesto su pc cuando está conectado a Internet (malware, phishing, spam, cibercriminales).Un útil diccionario le ayuda a entender los términos de seguridad de equipo con los que usted no está familiarizado.

Se postean nuevos artículos regularmente para que se mantenga actualizado sobre las últimas amenazas descubiertas, amenazas actuales y otra información de la industria de seguridad de equipos.

La página web de Malware City es http://www.malwarecity.com.

12.1.2. Pedir ayuda

La sección **Resolución de problemas** le ofrece la información necesaria sobre las incidencias más frecuentes que puede encontrar al usar este producto.

Si no encuentra la solución a su problema en los recursos proporcionados, puede contactarnos directamente:

- “Contacte con nosotros directamente desde su producto Bitdefender” (p. 94)
- “Póngase en contacto con nosotros a través de nuestro Centro de Soporte online” (p. 94)

Importante

Para contactar con el servicio de Atención al cliente de Bitdefender debe registrar su producto Bitdefender.Para más información, por favor vea “*Registro*” (p. 8).

Contacte con nosotros directamente desde su producto Bitdefender

Si dispone de una conexión a Internet, puede ponerse en contacto con Bitdefender directamente desde la interfaz del producto para obtener asistencia.

Siga estos pasos:

1. Abra la ventana de Bitdefender.
2. Haga clic en el enlace **Ayuda y soporte**, situado en la esquina inferior derecha de la ventana.
3. Dispone de las opciones siguientes:
   - Consulte los artículos o documentos relevantes e intente las soluciones propuestas.
   - Ejecuta una búsqueda en nuestra base de datos en busca de la información que desea.
   - Utilice el botón de **Contactar con soporte** para ejecutar la Herramienta de soporte y contactar así con el departamento de Atención al cliente.Puede navegar a través del asistente utilizando el botón **Siguiente**- Para salir del asistente, haga clic en **Cancelar**.
     a. Seleccione la casilla de verificación de consentimiento y haga clic en **Siguiente**.
     b. Rellene el formulario de envío con los datos necesarios:
        i. Introduzca su dirección de correo.
        ii. Introduzca su nombre completo.
        iii. Seleccione su país desde el menú correspondiente.
        iv. Escriba una descripción del problema que se ha encontrado.
     c. Por favor, espera unos minutos mientras Bitdefender reúne información relacionada con el producto. Esta información ayudará a nuestros ingenieros a encontrar una solución a su problema.
     d. Haga clic en **Finalizar** para enviar la información al Departamento de Atención al Cliente de Bitdefender. Contactarán con usted lo más pronto posible.

Póngase en contacto con nosotros a través de nuestro Centro de Soporte online

Si no puede acceder a la información necesaria utilizando el producto Bitdefender, consulte nuestro Centro de soporte online:

1. Visite http://www.bitdefender.com/help.El Centro de Soporte de Bitdefender alberga numerosos artículos que contienen soluciones de incidencias relacionadas con Bitdefender.
2. Seleccione su producto en la columna de la izquierda y busque en el Centro de soporte Bitdefender artículos que puedan ofrecer una solución a su problema.
3. Consulte los artículos o documentos relevantes e intente las soluciones propuestas.
4. Si la solución no resuelve su problema, utilice el enlace en el artículo para contactar con Atención al Cliente de Bitdefender.
5. Contacte con los técnicos de soporte de Bitdefender a través de correo, chat o teléfono.

12.2. Información de Contacto

BITDEFENDER valora todas las sugerencias e ideas que desee comunicarnos respecto a mejoras en el producto, o sobre la calidad de nuestros servicios. Así mismo, si tiene información referente a nuevos virus esperamos sus descripciones. Por favor no dude en contactar con nosotros.

12.2.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Centro de soporte:http://www.bitdefender.es/site/Main/contactForm/
Documentación: documentation@bitdefender.com
Distribuidores Locales:http://www.bitdefender.com/partners
Programa de partners: partners@bitdefender.com
Relaciones con los medios: pr@bitdefender.com
Empleos: jobs@bitdefender.com
Envíos de virus: virus_submission@bitdefender.com
Envíos de spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Sitio Web:http://www.bitdefender.es

12.2.2. Distribuidores locales

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área, tanto a nivel comercial como en otras áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite http://www.bitdefender.com/site/Partnership/list/.
2. La información de contacto de los distribuidores locales de Bitdefender se debería mostrar automáticamente. Si esto no ocurre, seleccione su país de residencia para ver la información.

3. Si no encuentra un distribuidor de Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es.Por favor escriba su correo en Inglés para que podamos asistirle rápidamente.

12.2.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están listas para responder a cualquier pregunta relativa a sus áreas de acción, tanto a nivel comercial como en otros asuntos. Sus direcciones y otros medios de contacto están listados a continuación.

U.S.A

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Teléfono (oficina&comercial): 1-954-776-6262
Comercial: sales@bitdefender.com
Soporte Técnico: http://www.bitdefender.es/site/Main/contactForm/
Web: http://www.bitdefender.es

Reino Unido e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
Correo: info@bitdefender.co.uk
Teléfono: +44 (0) 8451-305096
Comercial: sales@bitdefender.co.uk
Soporte Técnico: http://www.bitdefender.es/site/Main/contactForm/
Web: http://www.bitdefender.co.uk

Alemania

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Oficina: +49 2301 91 84 0
Comercial: vertrieb@bitdefender.de
Soporte Técnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

España

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª

08037 Barcelona
Fax: +34 93 217 91 28
Teléfono: +34 902 19 07 65
Comercial: comercial@bitdefender.es
Soporte Técnico: http://www.bitdefender.es/ayuda
Página Web: http://www.bitdefender.es

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Teléfono comercial: +40 21 2063470
Correo comercial: sales@bitdefender.ro
Soporte Técnico: http://www.bitdefender.ro/suport
Página Web: http://www.bitdefender.ro

13. Información útil

Este capítulo le presenta algunos de los procesos importante que debe saber antes de iniciar la solución de problemas de una incidencia técnica.

Solucionando problemas en una situación técnica en Bitdefender requiere varios puntos de vista de Windows, por lo tanto los pasos a seguir son en su mayoría relacionados con el sistema operativo Windows.

13.1. ¿Cómo desinstalo otras soluciones de seguridad?

La principal razón para utilizar una solución de seguridad es para proporcionar protección y seguridad para sus datos.¿Pero que pasa cuando tengo más de un producto de seguridad en el mismo sistema?

Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable.El instalador de Bitdefender Antivirus Plus 2012 automáticamente detecta otros programas de seguridad y le ofrece la opción de desinstalarlos.

Si no desea eliminar las otras soluciones de seguridad durante la instalación inicial, siga estos pasos:

- PAra **Windows XP**:
  1. Haga clic en **Inicio**, vaya a **Panel de Control** y haga doble clic en **Agregar/Quitar programas**.
  2. Espero un momento hasta que la lista de software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- Para **Windows Vista** y **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Espere un momento a que el software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.

4. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

Si falla la eliminación de otra solución de seguridad de su sistema, obtenga la herramienta de desinstalación de la página del proveedor o contacte con el directamente con el fin que le proporcionen las lineas de desinstalación.

13.2. ¿Cómo puedo reiniciar en Modo Seguro?

El Modo Seguro es un modo de diagnóstico operativo, utilizado principalmente para resolver problemas que afectan a la operación normal de Windows.Como problemas de conflictos de controladores a virus que impiden que Windows se inicie de forma normal.En Modo Seguro solo una cuantas aplicaciones trabajan y Windows carga solo los controladores básicos y un mínimo de componentes del sistema operativo.Esto es porque la mayoría de virus están inactivo cuando utiliza Windows en Modo Seguro y estos pueden ser fácilmente eliminados.

Para iniciar Windows en Modo Seguro:

1. Reinicie el equipo.
2. Presione la tecla **F8** varias veces antes de iniciar Windows para tener acceso al menú de inicio.
3. Seleccione **Modo seguro** en el menú de arranque o **Modo seguro con red** si quiere disponer de acceso a Internet.
4. Presione la tecla **Intro** y espere mientras Windows se carga en Modo seguro.
5. Este proceso finaliza con un mensaje de confirmación.Haga clic en **Ok** para reconocer.
6. Para iniciar Windows normal, simplemente reinicie el sistema.

13.3. ¿Estoy utilizando una versión de Windows de 32 o 64 bit?

Para encontrar si tiene un sistema operativo de 32 bit o 64 bit, siga estos pasos:

- PAra **Windows XP**:
  1. Haga clic en **Inicio**.
  2. Localice **Mi PC** en el menú de **Inicio**.
  3. Haga clic derecho en **Mi Equipo** y seleccione **Propiedades**.
  4. Si ve **x64 Edition** listado debajo de **sistema**, es que está trabajando en una versión de Windows XP 64 bit.

     Si no ve **x64 Edition** en la lista, es que está ejecutando una versión de Windows XP de 32 bits.

- Para **Windows Vista** y **Windows 7**:
  1. Haga clic en **Inicio**.
  2. Localice **Equipo** en el menú **Inicio**.
  3. Haga clic derecho en **Equipo** y seleccione **Propiedades**.
  4. Mire en **Sistema** para comprobar la información de su sistema.

13.4. ¿Cómo uso la restauración del sistema en Windows?

Si no puede iniciar el equipo en modo normal, puede arrancar en Modo Seguro y usar Restaurar Sistema para restaurarlo a un momento en el que podía iniciar su equipo sin problemas.

Para ejecutar la restauración del sistema, debe iniciar sesión en Windows como administrador.

Para usar Restaurar sistema, siga estos pasos:

- En Windows XP:
  1. Inicie sesión en Windows en Modo Seguro.
  2. Siga la ruta desde el menú Inicio de Windows: **Inicio → Todos los programas → Herramientas del sistema → Restaurar sistema**.
  3. En la página de **bienvenida a Restaurar sistema**, haga clic para seleccionar la opción **Restaurar mi equipo a un estado anterior** y luego haga clic en Siguiente.
  4. Siga los pasos del asistente y debería ser capaz de iniciar el sistema de modo normal.
- En Windows Vista y Windows 7:
  1. Inicie sesión en Windows en Modo Seguro.
  2. Siga la ruta desde el menú Inicio de Windows: **Todos los Programas → Accesorios → Herramientas del sistema → Restaurar sistema**.
  3. Siga los pasos del asistente y debería ser capaz de iniciar el sistema de modo normal.

13.5. ¿Cómo puedo mostrar los objetos ocultos en Windows?

Estos pasos son útiles en los casos en que se trata de una situación del malware y necesitas para encontrar y eliminar los archivos infectados, lo que podría estar oculto.

Siga estos pasos para ver los elementos ocultos de Windows:

1. Haga clic en **Inicio**, vaya **Panel de Control** y seleccione **Opciones de Carpeta**.

2. Vaya a la pestaña **Ver**.
3. Seleccione **Mostrar contenido de las carpetas de sistema** (solo para Windows XP).
4. Seleccione **Mostrar archivo y carpetas ocultos**.
5. Desmarcar **Ocultar extensiones de archivos para tipos de archivo conocidos**.
6. Desmarque **Ocultar archivos protegidos del sistema operativo**.
7. Haga clic en **Aplicar** y luego en **Ok**.

Glosario

ActiveX

El ActiveX es un modelo para escribir programas de manera que otros programas y sistemas operativos puedan usarlos. La tecnología ActiveX se utiliza junto con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y comporten como programas, y no como páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, pulsar botones, interactuar de otras formas con una página web. Los controles ActiveX normalmente se escriben en Visual Basic.

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

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.

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.

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.

Archivo Comprimido

Disco, cinta o directorio que contiene ficheros almacenados.

Fichero que contiene uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones realizadas. Bitdefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura 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.

Backdoor

Se trata de un agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. El objetivo de estos agujeros no es siempre dañino; algunos sistemas operativos funcionan con unas cuentas privilegiadas, creadas para los técnicos de servicio u operadores de mantenimiento.

Cliente de mail

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

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.

Correo

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

Descargar

Para copiar informaciones (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.

Elementos de Inicio

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.

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).

Explorador

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.

Extensión de un archivo

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

Hay varios sistemas operativos que utilizan extensiones de archivos (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Por ejemplo, "c" para archivos de código fuente en lenguaje C, "ps" para PostScript, "txt" para documentos de texto.

Falso positivo

Ocurre cuando un analizador identifica un fichero como infectado cuando éste no lo es.

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 agregar a otros programas.

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 - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP. 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.

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers no son maliciosos por naturaleza. Pueden utilizarse para propósitos legítimos, como la vigilancia de empleados o de la actividad de sus hijos. Sin embargo, son cada vez más utilizados por los cibercriminales con fines ilegales (por ejemplo, para recoger los datos privados, tales como credenciales de acceso y números de identificación).

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.

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.

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.

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.

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.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

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

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

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 informaciones es una ruta completamente válida.

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

Script

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

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.

Spam

Correo basura o los posts basura en grupos de noticias, también denominado correo no solicitado.

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.

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 tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

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).

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.

Virus de boot

Es un virus que infecta el sector de arranque de un disco duro o disquete. Al intentar arrancar el sistema desde un disco infectado con un virus de boot, el virus quedará cargado en la memoria. A partir de ese momento, cada vez que intente arrancar el sistema, tendrá el virus activo en la memoria.

Virus de macro

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

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

Virus Polimórfico

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