Bitdefender®

TOTAL SECURITY 2017

GUÍA DE USUARIO

Bitdefender Total Security 2017
Guía de Usuario

fecha de publicación 12/19/2016

Advertencia legal

Bitdefender

Tabla de contenidos

Acerca de esta Guía

1. Propósito y público al que va dirigida

Su suscripción Bitdefender Total Security 2017 puede proteger hasta diez PC, Mac y smartphones o tablets Android diferentes. La gestión de los dispositivos protegidos se puede efectuar a través de una cuenta de Bitdefender, que ha de ir asociada a una suscripción activa.

Esta guía le ayudará con la instalación y el uso de los productos incluidos en suscripción: Bitdefender Total Security, Bitdefender Antivirus for Mac y Bitdefender Mobile Security & Antivirus.

Puede aprender a configurar Bitdefender en varios dispositivos diferentes para mantenerlos protegidos frente a todo tipo de amenazas.

2. Cómo usar esta guía

Esta guía se basa en los tres productos incluidos en Bitdefender Total Security 2017:

- “Total Security para PC” (p. 1)

  Aprenda a usar el producto en sus PCs y portátiles Windows.

- “Antivirus for Mac” (p. 220)

  Aprenda a usar el producto en sus Macs.

- “Mobile Security para Android” (p. 257)

  Aprenda a usar el producto en sus tablets y smartphones Android.

- “Contacto” (p. 289)

  Sepa dónde buscar ayuda si surge algún problema.

TOTAL SECURITY PARA PC

1. PASOS DE LA INSTALACIÓN

1.1. Preparándose para la instalación

Antes de instalar Bitdefender Total Security, 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. 2).
- 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.
- Desactive o elimine cualquier programa cortafuego que puede estar ejecutándose en el equipo. La ejecución de dos programas de cortafuego simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Firewall se desactivará durante la instalación.
- Durante la instalación, se recomienda que su equipo esté conectado a Internet. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

1.2. Requisitos del sistema

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

- Windows 7 con Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

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

Nota
Para saber qué sistema operativo Windows está ejecutando su equipo y obtener información del hardware:

- En **Windows 7**, haga clic con el botón derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** del menú.
- En **Windows 8**, desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono. En **Windows 8.1**, acceda a **Este equipo**.

  Seleccione **Propiedades** en el menú inferior. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.
- En **Windows 10**, escriba **Sistema** en el cuadro de búsqueda de la barra de tareas y haga clic en su icono. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.

Requisitos mínimos del sistema

- 1.5 GB de espacio libre en disco duro (al menos 800 MB en la unidad del sistema)
- 1.6 GHz procesador
- 1 GB de memoria (RAM)

Requisitos de sistema recomendados

- 2 GB de espacio libre en disco duro (al menos 800 MB en la unidad del sistema)
- Intel CORE Duo (2 GHz) o procesador equivalente
- 2 GB de memoria (RAM)

Requisitos de software

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

- Internet Explorer 10 o superior
- Mozilla Firefox 30 o superior
- Google Chrome 34 o superior

- Skype 6.3 o superior
- Microsoft Outlook 2007 / 2010 / 2013
- Mozilla Thunderbird 14 o superior

1.3. Instalando su producto Bitdefender

Puede instalar Bitdefender desde el disco de instalación, o recurrir al instalador Web descargado en su equipo desde Bitdefender Central.

Si su compra cubre más de un equipo, repita el proceso de instalación y active su producto con la misma cuenta en cada equipo. La cuenta que tiene que utilizar es la que contiene la suscripción activa a su Bitdefender.

Instalar desde Bitdefender Central

Desde Bitdefender Central puede descargar el kit de instalación correspondiente a la suscripción adquirida. Una vez que el proceso de instalación se haya completado, se activa Bitdefender Total Security.

Para descargar Bitdefender Total Security desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Validación de la instalación

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

El paquete de instalación de Bitdefender Total Security está constantemente actualizado.

Nota
Descargar los archivos de instalación puede llevar un buen rato, especialmente con conexiones a Internet lentas.

Una vez que se haya validado la instalación, aparecerá el asistente de configuración. Siga los pasos para instalar Bitdefender Total Security.

Paso 1 - Instalación de Bitdefender

La pantalla de instalación de Bitdefender le permite elegir qué tipo de instalación desea realizar.

Para una sencilla instalación, simplemente haga clic en el botón **INSTALAR**. Bitdefender se instalará en la ubicación por defecto con los ajustes por omisión y usted irá directamente al Paso 3 del asistente.

Si desea configurar los ajustes de instalación, haga clic primero en **INSTALACIÓN PERSONALIZADA**.

En este paso pueden realizarse tres tareas adicionales:

- Lea la Licencia de usuario final antes de proseguir con la instalación. El acuerdo de licencia contiene los términos y condiciones bajo los cuales usted puede usar Bitdefender Total Security.

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

- Mantenga activada la opción **Enviar informes anónimos**. Permitiendo 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.

- Seleccione el idioma en el que desea que se instale el producto.

Paso 2 - Personalización de ajustes de instalación

> **Nota**
> Este paso sólo aparece si ha elegido personalizar la instalación en el paso anterior.

Tiene las siguientes opciones a su disposición:

Ruta de instalación

Por omisión, Bitdefender Total Security se instalará en C:\Archivos de Programa\Bitdefender\Bitdefender 2017. Si desea cambiar la ruta de instalación, haga clic en **CAMBIAR** y seleccione la carpeta donde desea instalar Bitdefender.

Configurar ajustes proxy

Bitdefender Total Security necesita acceder a Internet para la activación 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, active el conmutador correspondiente y configure las opciones del proxy.

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

Analizar el equipo durante la instalación

Desactive esta opción si no quiere analizar su sistema durante la instalación del producto Bitdefender.

Haga clic en **INSTALAR** para confirmar sus preferencias y comenzar la instalación. Si cambia de parecer, haga clic en el botón **Atrás**.

Paso 3 - Instalación en curso

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 tardar un par de minutos.

Paso 4 - Instalación completada

Su producto Bitdefender se ha instalado correctamente.

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 **EMPEZAR A USAR Bitdefender** para continuar.

Paso 5 - Plan de suscripción

En la ventana del **Plan de suscripción** puede ver la información relativa a su suscripción activa.

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Total Security.

Instalar desde el disco de instalación

Para instalar Bitdefender desde el disco de instalación, inserte el disco en la unidad.

En breves momentos debería mostrarse una pantalla de instalación. Siga las instrucciones para comenzar la instalación.

Si no aparece la pantalla de instalación, utilice el explorador de Windows para acceder al directorio raíz en el disco y haga doble clic en el archivo autorun.exe.

Si su velocidad de Internet es lenta, o su sistema no está conectado a Internet, haga clic en el botón **Instalar desde CD/DVD**. En tal caso, se instalará el producto Bitdefender disponible en el disco y se descargará una versión más reciente de los servidores de Bitdefender mediante la actualización del producto.

Validación de la instalación

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

Nota
Descargar los archivos de instalación puede llevar un buen rato, especialmente con conexiones a Internet lentas.

Una vez que se haya validado la instalación, aparecerá el asistente de configuración. Siga los pasos para instalar Bitdefender Total Security.

Paso 1 - Instalación de Bitdefender

La pantalla de instalación de Bitdefender le permite elegir qué tipo de instalación desea realizar.

Para una sencilla instalación, simplemente haga clic en el botón **INSTALAR**. Bitdefender se instalará en la ubicación por defecto con los ajustes por omisión y usted irá directamente al Paso 3 del asistente.

Si desea configurar los ajustes de instalación, haga clic primero en **INSTALACIÓN PERSONALIZADA**.

En este paso pueden realizarse tres tareas adicionales:

- Lea la Licencia de usuario final antes de proseguir con la instalación. El acuerdo de licencia contiene los términos y condiciones bajo los cuales usted puede usar Bitdefender Total Security.

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

- Mantenga activada la opción **Enviar informes anónimos**. Permitiendo 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. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizarán con fines comerciales.

- Seleccione el idioma en el que desea que se instale el producto.

Paso 2 - Personalización de ajustes de instalación

> **Nota**
> Este paso sólo aparece si ha elegido personalizar la instalación en el paso anterior.

Tiene las siguientes opciones a su disposición:

Ruta de instalación

Por defecto, Bitdefender Total Security se instalará en C:\Archivos de programa\Bitdefender\Bitdefender 2017\. Si desea cambiar la ruta de instalación, haga clic en **CAMBIAR** y seleccione la carpeta donde desea instalar Bitdefender.

Configurar ajustes proxy

Bitdefender Total Security necesita acceder a Internet para la activación 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, active el conmutador correspondiente y configure las opciones del proxy.

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

Analizar el equipo durante la instalación

Desactive esta opción si no quiere analizar su sistema durante la instalación del producto Bitdefender.

Haga clic en **INSTALAR** para confirmar sus preferencias y comenzar la instalación. Si cambia de parecer, haga clic en el botón **Atrás**.

Paso 3 - Instalación en curso

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

Las áreas críticas de su sistema se analizan en busca de virus y se inician los servicios de Bitdefender. Este paso puede tardar un par de minutos.

Paso 4 - Instalación completada

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 **EMPEZAR A USAR Bitdefender** para continuar.

Paso 5 - Cuenta Bitdefender

Tras completar la configuración inicial, aparece la ventana cuenta Bitdefender. Es necesaria una cuenta Bitdefender para poder activar el producto y utilizar sus características online. Para más información, por favor vea "*Bitdefender Central*" (p. 37).

Proceder de acuerdo a su situación.

Quiero crear una cuenta Bitdefender

Escriba la información requerida en los campos correspondientes y, a continuación, haga clic en **CREAR CUENTA**.

Los datos que introduzca aquí serán confidenciales.

La contraseña debe tener al menos ocho caracteres e incluir un número.

Lea las Condiciones del servicio de Bitdefender antes de seguir adelante.

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 https://central.bitdefender.com.

Ya tengo una cuenta de Bitdefender

Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.

Haga clic en **INICIAR** para continuar.
Si olvidó la contraseña de su cuenta o, sencillamente, desea cambiar la que ya estableció, haga clic en el enlace **Olvidé la contraseña**. Escriba su dirección de correo electrónico y, a continuación, haga clic en el botón **OLVIDÉ LA CONTRASEÑA**. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

Nota

Si ya tiene una cuenta de MyBitdefender, puede utilizarla para acceder a cuenta Bitdefender. Si ha olvidado su contraseña, primero tiene que ir a https://my.bitdefender.com para restablecerla. A continuación, utilice las credenciales actualizadas para iniciar sesión en cuenta Bitdefender.

Quiero iniciar la sesión con mi cuenta de Microsoft, Facebook o Google

Para iniciar sesión con su cuenta de Microsoft, Facebook o Google:

1. Seleccione el servicio que desee usar. 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.

Paso 6 - Active su producto

Nota
Este paso aparece si ha elegido crear una cuenta Bitdefender nueva durante el paso anterior, o si inició sesión con una cuenta que tenga la suscripción caducada.

Es preciso conectarse a Internet para completar la activación de su producto.

Proceda de acuerdo con su situación:

- Tengo un código de activación

  En este caso, active el producto siguiendo estos pasos:

  1. Escriba el código de activación en el campo **Tengo un código de activación** y, a continuación, haga clic en **CONTINUAR**.

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

  2. **Deseo evaluar Bitdefender**

     En este caso, puede utilizar el producto durante un período de 30 días. Para comenzar el período de prueba, seleccione **No tengo suscripción; quiero probar el producto de forma gratuita** y, a continuación, haga clic en **CONTINUAR**.

Paso 7 - Plan de suscripción

En la ventana del **Plan de suscripción** puede ver la información relativa a su suscripción activa.

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Total Security.

2. PRIMEROS PASOS

2.1. Fundamentos

Una vez haya instalado Bitdefender Total Security, su equipo estará protegido frente a todo tipo de malware (como virus, spyware y troyanos) y amenazas de Internet (como hackers, phishing y spam).

La aplicación utiliza la tecnología Photon para aumentar la velocidad y el rendimiento del proceso de análisis antimalware. Funciona gracias al aprendizaje de los patrones de uso de las aplicaciones de su sistema para saber qué y cuándo analizar, minimizando así el impacto en el rendimiento del sistema.

Puede activar Autopilot para disfrutar de una seguridad silenciosa y no necesitará configurar ningún ajuste. De todos modos, puede que quiera aprovechar las opciones de Bitdefender para optimizar y mejorar su protección.

Siempre que su dispositivo se conecta a una red inalámbrica que no es segura, Bitdefender la identifica y habilita una protección para salvaguardarle de posibles fisgones y espías. Para obtener instrucciones sobre cómo mantener sus datos personales a salvo, consulte el apartado Asesor de seguridad Wi-Fi.

Mientras trabaja, juega o ve películas, Bitdefender puede ofrecerle una experiencia de usuario constante posponiendo las tareas de mantenimiento, eliminando las interrupciones y ajustando los efectos visuales del sistema. Puede beneficiarse de todo esto activando y configurando los Perfiles.

Bitdefender tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes. Los detalles sobre las medidas adoptadas y la información acerca de la operativa del programa están disponibles en la ventana de Notificaciones. Para más información, por favor vea “Notificaciones” (p. 17).

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.

Para usar las opciones online de Bitdefender Total Security y administrar sus suscripciones y dispositivos, acceda a su cuenta Bitdefender. Para más información, por favor vea “*Bitdefender Central*” (p. 37).

La sección "*Cómo*" (p. 48) es donde encontrará paso a paso instrucciones de cómo realizar tareas comunes. Si tiene algún problema mientras utiliza Bitdefender, revise la sección "*Resolución de incidencias comunes*" (p. 186) con soluciones para la mayoría de los problemas comunes.

Apertura de la ventana de Bitdefender

Para acceder a la interfaz principal de Bitdefender Total Security, siga estos pasos:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Haga clic en **Bitdefender 2017**.
  3. Haga en clic en **Bitdefender Total Security**, o más rápido, haga doble clic en el icono de Bitdefender en el área de notificación.
- En **Windows 8 y Windows 8.1**:

  Localice Bitdefender Total Security desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender" en la pantalla de inicio) y luego haga clic en su icono. Opcionalmente, abra la app de escritorio y haga doble clic en el icono de Bitdefender en el área de notificación.
- En **Windows 10**:

  Escriba "Bitdefender" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono. Opcionalmente, haga doble clic en el icono de Bitdefender en el área de notificación.

Para obtener más información sobre la ventana de Bitdefender y el icono del área de notificación, consulte "*Interfaz de Bitdefender*" (p. 22).

Reparando incidencias

Bitdefender utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la seguridad de su equipo e información. Por defecto, monitoriza 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. Están agrupados 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:

Las incidencias críticas 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.

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

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

Asistente de problemas de seguridad

Para solucionar las incidencias detectadas siga el asistente **Incidencias de seguridad**.

1. Para abrir el asistente, realice lo siguiente:
   - Haga clic con el botón derecho en el icono Bitdefender del área de notificación y elija **Ver incidencias de seguridad**.
   - Abra la Interfaz Bitdefender y haga clic en cualquier sitio dentro del área de estado Seguridad en la barra de herramientas superior.
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 **Pospuesto** y no se adoptarán medidas para solucionar el problema.

3. Para solucionar las incidencias seleccionadas, haga clic en **Reparar**. Algunas incidencias serán reparadas 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.

Configuración de las alertas de estado

Bitdefender puede informarle cuando se detectan incidencias en la actividad de los siguientes componentes de programa:

- Antimalware
- Cortafuego
- Actualizar
- Seguridad del navegador

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. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Haga clic en el enlace **Configurar alertas de estado**.
4. Haga clic en los conmutadores para activar o desactivar las alertas de estado de acuerdo con sus preferencias.

Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC. Siempre que ocurra algo relevante respecto a la seguridad de su sistema o información, se añadirá un nuevo mensaje a las Notificaciones de Bitdefender, de forma parecida a un nuevo e-mail apareciendo en su bandeja de entrada.

Las notificaciones son una herramienta importante en la supervisión y la gestión de la protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o malware en su equipo, etc. Además, si es necesario puede realizar acciones adicionales o cambiar las acciones que Bitdefender ha llevado a cabo.

Para acceder al registro de notificaciones, haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender. Cada vez que se produce un evento crítico, se puede ver un contador en el icono .

Dependiendo del tipo y la gravedad, las notificaciones se agrupan en:

- Los eventos **críticos** indican problemas críticos. Debe verificarlos inmediatamente.
- Los eventos de **Advertencia** indican incidencias no críticas. Cuando tenga tiempo debería comprobarlas y repararlas.
- Los eventos de **Información** indican operaciones que se han completado con éxito.

Haga clic en cada pestaña para obtener más información sobre los eventos generados. Con un simple clic en el título de cada evento se muestran algunos detalles: una breve descripción, la medida que Bitdefender adoptó cuando este se produjo, y la fecha y hora en que ocurrió. Si fuera necesario pueden proporcionarse opciones con el fin de tomar nuevas medidas.

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

Autopilot

Para todos aquellos usuarios que desean protegerse con una solución de seguridad que no les moleste, Bitdefender Total Security ha sido diseñado con un Modo autopilot integrado.

Mientras esté en Autopilot, Bitdefender aplicará una configuración óptima de seguridad y tomará 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 Modo autopilot, Bitdefender soluciona automáticamente las incidencias críticas, habilita y administra silenciosamente:

- Protección antivirus, proporcionada por el análisis on-access y el análisis continuo.
- Protección del cortafuego.
- Protección Web.
- Actualizaciones automáticas.

Para activar o desactivar Autopilot, haga clic en el conmutador **Autopilot** en la barra de herramientas superior de la interfaz de Bitdefender.

Mientras Autopilot esté activo, el icono de Bitdefender en el área de notificación cambiará a .

> **Importante**
> Mientras el Autopilot esté activo, modificar alguno de los ajustes que administre lo desactivaría.

Para ver un historial de acciones llevadas a cabo por Bitdefender mientras estaba activado Autopilot, abra la ventana Notificaciones.

Perfiles

Algunas actividades informáticas, como los juegos online o las presentaciones en vídeo, requieren mayor capacidad de respuesta del sistema, alto rendimiento y ausencia de 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.

Los Perfiles de Bitdefender asignan más recursos del sistema a las aplicaciones en ejecución, modificando temporalmente los ajustes de protección y adaptando la configuración del sistema. En consecuencia, se minimiza el impacto del sistema en sus actividades.

Para adaptarse a las diferentes actividades, Bitdefender viene con los siguientes perfiles:

Perfil de Trabajo
: Optimiza la eficiencia en su trabajo identificando y adaptando los ajustes del producto y del sistema.

Perfil de Películas
: Mejora los efectos visuales y elimina las interrupciones cuando se ven películas.

Perfil de Juego
: Mejora los efectos visuales y elimina las interrupciones cuando se juega.

Perfil de redes Wi-Fi públicas
: Aplica los ajustes del producto para beneficiarse de una protección completa mientras está conectado a una red inalámbrica no segura.

Perfil del modo Batería
: Aplica los ajustes del producto y reduce la actividad en segundo plano para ahorrar batería.

Configurar la activación automática de perfiles

Para una experiencia de usuario sencilla, puede configurar Bitdefender para que gestione su perfil de trabajo. En tal caso, Bitdefender detecta automáticamente la actividad que usted lleva a cabo y aplica los ajustes de optimización del producto y del sistema.

Para permitir que Bitdefender active los perfiles:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Utilice el conmutador correspondiente para habilitar **Activar perfiles automáticamente**.

Si no desea que los perfiles se activen automáticamente, deshabilite el conmutador.

Para obtener más información sobre los Perfiles, por favor consulte"*Perfiles*" (p. 178)

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 los ajustes de Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **General**.
3. Habilite la protección por contraseña haciendo clic en el conmutador correspondiente.
4. 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 protección por contraseña:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **General**.
3. Desactive la protección por contraseña haciendo clic en el conmutador correspondiente. Introduzca la contraseña y haga clic en **Aceptar**.

> **Nota**
>
> Para modificar la contraseña de su producto, haga clic en el enlace **Cambiar contraseña**.

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 anónimos de uso:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Haga clic en el conmutador correspondiente para deshabilitar los informes de uso anónimos.

Ofertas especiales y notificaciones de productos

Cuando haya ofertas promocionales disponibles, el producto Bitdefender está configurado para que se lo notifique mediante una ventana emergente. Esto le da la oportunidad de beneficiarse de precios ventajosos y mantener sus dispositivos protegidos durante un mayor período de tiempo.

Además, pueden aparecer notificaciones del producto cuando realice cambios en el mismo.

Para activar o desactivar las ofertas especiales y las notificaciones del producto:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **General**.
3. Active o desactive las ofertas especiales y notificaciones del producto haciendo clic en el conmutador correspondiente.

La opción de ofertas especiales y notificaciones del producto está activada por defecto.

2.2. Interfaz de Bitdefender

Bitdefender Total Security 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 permite gestionar el comportamiento del producto mediante Autopilot, le da acceso a información importante sobre el producto y le permite realizar tareas habituales. En la barra lateral izquierda puede acceder a cuenta Bitdefender y a las secciones de Bitdefender para proceder a una configuración detallada y a tareas administrativas avanzadas.

Si desea vigilar constantemente la información de seguridad esencial y tener un acceso rápido a los ajustes clave, añada el Widget de seguridad en su escritorio.

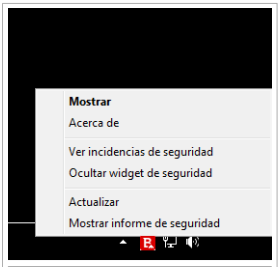
Icono del área de notificación

Para administrar todo el producto más fácilmente, puede usar el icono Bitdefender en la barra de tareas.

Nota
El icono de Bitdefender puede que no esté visible en todo momento. Para que el icono se muestre de forma permanente:

- En **Windows 7, Windows 8 y Windows 8.1**:
  1. Haga clic en la flecha en la esquina inferior derecha de la pantalla.
  2. Haga clic en **Personalizar...** para abrir la ventana de Iconos del área de notificación.
  3. Seleccione la opción **Mostrar icono y notificaciones** en el icono del **Agente de Bitdefender**.
- En **Windows 10**:
  1. Haga clic derecho en la barra de tareas y seleccione **Propiedades**.
  2. Haga clic en **Personalizar** en la ventana de la barra de tareas.
  3. Haga clic en el enlace **Seleccionar qué iconos aparecen en la barra de tareas** en la ventana **Notificaciones y acciones**.
  4. Active el conmutador junto a **Agente de Bitdefender**.

Si hace doble clic en este icono se abrirá la interfaz de Bitdefender. Además, al hacer clic derecho sobre el icono, un menú contextual le permitirá administrar rápidamente el producto Bitdefender.



Icono de la 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.
- **Ver incidencias de seguridad** - le ayuda a eliminar las vulnerabilidades de seguridad actuales. Si esta opción no está disponible, no hay ninguna incidencia para reparar. Para más información, por favor, consulte el apartado "Reparando incidencias" (p. 14).
- **Ocultar / Mostrar el Widget de seguridad** - habilita / deshabilita el Widget de seguridad.
- **Actualizar** - realiza una actualización inmediata. Puede seguir el estado de la actualización en el panel de Actualización de la ventana principal de Bitdefender.
- **Mostrar informe de seguridad** - abre una ventana donde puede ver un estado semanal y recomendaciones para su sistema. Puede seguir las recomendaciones para mejorar la seguridad de su sistema.

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 Autopilot de Bitdefender está activado.

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

Ventana principal

La ventana principal de Bitdefender le permite realizar tareas comunes, solucionar rápidamente problemas de seguridad, ver la información sobre el uso del producto y acceder a los paneles desde los cuales se configuran los ajustes del mismo. Todo se encuentra a tan sólo unos clics.

La ventana está organizada en tres áreas principales:

Área de Estado
: Aquí es donde puede comprobar el estado de seguridad de su equipo, iniciar una actualización y configurar Autopilot.

Barra lateral izquierda
: Este menú le permite acceder y administrar cuenta Bitdefender junto con las funciones online de su producto, o alternar entre las tres secciones principales del producto. Desde aquí puede acceder también a las Notificaciones, al Informe de seguridad semanal, a los ajustes Generales y al área de Ayuda y soporte.

Botones de acción y acceso al área de módulos
: Aquí es donde puede ejecutar diferentes tareas para mantener su sistema protegido y funcionando a la velocidad óptima. Además, puede acceder a los módulos de Bitdefender para configurarlo como desee.

Área de Estado

El área de estado contiene los siguientes elementos:

- El **Estado de seguridad** a la izquierda de la área, 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.

Haciendo clic en cualquier lugar dentro del área de estado de seguridad, puede acceder a un asistente que le ayudará a eliminar amenazas fácilmente de su equipo. Para más información, por favor, consulte el apartado "Reparando incidencias" (p. 14).

- **AUTOPILOT** le permite disfrutar de una seguridad excelente y totalmente silenciosa. Para más información, por favor, consulte el apartado "Autopilot" (p. 18).
- **ACTUALIZAR AHORA** le permite ejecutar una actualización del producto siempre que desee asegurarse de que posee las últimas firmas de malware. Para más información, por favor, consulte el apartado "*Mantenimiento de Bitdefender al día*" (p. 44).
- **Perfil activo** muestra el perfil habilitado actualmente en su producto Bitdefender. Para más información, por favor, consulte el apartado "*Perfiles*" (p. 178).

Barra lateral izquierda

En la barra lateral izquierda dispone de unos iconos intuitivos que le dan acceso a lo siguiente: cuenta Bitdefender, secciones del producto, informe de actividad, notificaciones, ajustes generales y soporte.

Puede ver los nombres de los iconos haciendo clic en el icono ☰, como se indica a continuación:

- **Protección**. Los botones de acción **Quick Scan** y **Análisis de vulnerabilidades** aparecen en la esquina inferior izquierda de la interfaz de Bitdefender. También se muestra información acerca de las aplicaciones bloqueadas, los ataques y las amenazas detectadas. Haga clic en el enlace **VER MÓDULOS** para acceder al área de configuración.
- **Privacidad**. Los botones de acción **Safepay** y **Asesor parental** aparecen en la esquina inferior izquierda de la interfaz de Bitdefender. También se muestra información acerca de los blindajes de archivos y Wallets detectados. Haga clic en el enlace **VER MÓDULOS** para acceder al área de configuración.
- **Herramientas**. Los botones de acción **Optimizador en un clic** y **Optimizador de inicio** aparecen en la esquina inferior izquierda de la interfaz de Bitdefender. Además, se muestra información sobre el espacio optimizado y se puede ejecutar la **Limpieza de disco** para hacer sitio a

nuevos datos mediante la eliminación de carpetas y archivos de gran tamaño que ya no utilice. Por otra parte, se puede acceder al Antirrobo.

- **Actividad**. Aquí puede ver la actividad del producto durante los últimos treinta días y acceder al informe de seguridad que se genera cada siete días.
- **Información de la cuenta**. Dispone de información acerca de cuenta Bitdefender y de la suscripción en uso. Acceda a su cuenta de Bitdefender para verificar sus suscripciones y realizar tareas de seguridad en los dispositivos que administra.
- **Notificaciones**. Desde aquí tiene acceso a las notificaciones generadas.
- **Ajustes**. Desde aquí tiene acceso a los ajustes generales.
- **Soporte**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su Bitdefender Total Security, puede ponerse en contacto con el servicio de soporte técnico de Bitdefender.

Botones de acción y acceso al área de módulos

Utilizando los botones de acción puede poner rápidamente en marcha tareas importantes. Los botones de acción se muestran en la esquina inferior izquierda de la interfaz de Bitdefender cuando se selecciona cualquiera de las tres secciones: **Protección**, **Privacidad** o **Herramientas** de la barra lateral izquierda.

Dependiendo de la sección que elija, los botones de acción visibles en esta área pueden ser:

- **Análisis rápido**. Ejecute un análisis rápido para asegurarse de que su equipo está libre de malware.
- **Análisis de vulnerabilidades**. Analice su equipo en busca de vulnerabilidades para asegurarse de que todas las aplicaciones instaladas, además del sistema operativo, están actualizadas y funcionan correctamente.
- **Safepay**. Abra Bitdefender Safepay™ para proteger sus datos confidenciales mientras efectúa transacciones online.
- **Asesor parental**. Acceda al Asesor parental de Bitdefender para mantenerse informado sobre las actividades de sus hijos.
- **Optimizador de inicio**. Disminuya el tiempo de arranque del sistema evitando que las aplicaciones innecesarias se ejecuten en el arranque.

- **Optimizador en un clic**. Libere espacio en disco, corrija errores del registro y proteja su privacidad eliminando archivos que ya no le hacen falta con solo hacer clic en un botón.

Las secciones de Bitdefender

El producto Bitdefender viene con tres secciones divididas en útiles módulos que le ayudarán a mantenerse protegido mientras trabaja, navega por la Web o efectúa pagos online, mejorar la velocidad de su sistema y mucho más.

Para acceder a los módulos de una determinada sección o para empezar a configurar su producto, utilice los siguientes iconos situados en la barra lateral izquierda de la interfaz de Bitdefender:

- Protección
- Privacidad
- Herramientas

Protección

En la sección de Protección puede configurar su nivel de seguridad, gestionar los amigos y los emisores de spam, ver y editar los ajustes de conexión de red, configurar las opciones de protección Web y contra ransomware, buscar y corregir posibles vulnerabilidades del sistema y evaluar la seguridad de las redes inalámbricas a las que se conecta.

Los módulos que puede administrar en la sección de Protección 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.

En el módulo Antivirus puede acceder fácilmente a las siguientes tareas de análisis:

- Análisis rápido
- Análisis de sistema
- Administrar análisis
- Modo de rescate

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte "*Protección Antivirus*" (p. 84).

PROTECCIÓN WEB

La protección Web le ayuda a mantenerse protegido contra ataques de phishing, intentos de fraude y filtraciones de datos privados mientras navega por Internet.

Para obtener más información sobre cómo configurar Bitdefender para proteger sus actividades en la Web, consulte "*Protección Web*" (p. 119).

VULNERABILIDAD

El módulo de Vulnerabilidades le ayuda a mantener al día el sistema operativo y las aplicaciones que usa con regularidad, así como identificar las redes inalámbricas inseguras a las que se conecta.

Haga clic en **Análisis de vulnerabilidades** en el módulo de Vulnerabilidades para empezar a identificar las actualizaciones críticas de Windows, actualizaciones de aplicaciones, contraseñas débiles pertenecientes a cuentas de Windows y redes inalámbricas que no sean seguras.

Haga clic en el **Asesor de seguridad Wi-Fi** para ver la lista de redes inalámbricas a las que se conecta, junto con nuestra evaluación de reputación de cada una de ellas y las medidas que puede adoptar para mantenerse a salvo de fisgones potenciales.

Para obtener más información sobre la configuración de la protección contra vulnerabilidades, consulte "*Vulnerabilidad*" (p. 128).

CORTAFUEGOS

El cortafuego le protege mientras está conectado a redes y a Internet mediante el filtrado de todos los intentos de conexión.

Para obtener más información sobre la configuración del cortafuego, consulte "*Cortafuego*" (p. 136).

ANTISPAM

El módulo antispam de Bitdefender garantiza que su Bandeja de entrada esté libre de correo electrónico no deseado mediante el filtrado del tráfico de correo POP3.

Para obtener más información sobre la protección antispam, consulte "*Antispam*" (p. 110).

Protección contra ransomware

El módulo de Protección contra ransomware se asegura de que sus archivos personales permanecen protegidos contra los ataques de los chantajistas online.

Para obtener más información sobre cómo configurar la Protección contra ransomware para protegerse frente a este tipo de ataques, consulte "*Protección contra ransomware*" (p. 144).

Privacidad

En la sección de Privacidad puede cifrar sus datos privados, proteger sus transacciones online, mantener a salvo su experiencia de navegación y proteger a sus hijos visualizando y restringiendo sus actividades online.

Los módulos que puede administrar en la sección de Privacidad son:

PROTECCIÓN DE DATOS

El módulo de Protección de datos le permite borrar archivos de forma permanente.
Haga clic en el **Destructor de archivos** en el módulo de Protección de datos para iniciar un asistente que le permitirá eliminar completamente archivos de su sistema.

Para obtener más información sobre la configuración de la Protección de datos, consulte "*Protección de datos*" (p. 121).

WALLET

El Gestor de contraseñas de Bitdefender le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

En el módulo Gestor de contraseñas puede seleccionar las siguientes tareas:

- **Abrir Wallet** - abre la base de datos de Wallet existente.
- **Bloquear Wallet** - bloquea la base de datos de Wallet existente.
- **Exportar Wallet** - le permite guardar la base de datos existente en una ubicación de su sistema.
- **Crear nuevo Wallet** - inicia un asistente que le permitirá crear una nueva base de datos de Wallet.
- **Eliminar** - le permite eliminar una base de datos de Wallet.

- **Ajustes** - aquí puede cambiar el nombre de su base de datos de Wallet y establecer que se sincronice o no la información existente con todos sus dispositivos.

Para obtener más información sobre la configuración del Gestor de contraseñas, consulte "*Protección del Gestor de contraseñas para sus credenciales*" (p. 152).

SAFEPAY

El navegador Bitdefender Safepay™ le ayuda a mantener a salvo y en privado su banca electrónica, sus compras por Internet y cualquier otro tipo de transacción online.

Haga clic en el botón de acción **Safepay** de la interfaz de Bitdefender para empezar a realizar transacciones online en un entorno seguro.

Para obtener más información sobre Bitdefender Safepay™, consulte "*Seguridad Safepay para las transacciones online*" (p. 147).

Asesor parental

El Asesor parental de Bitdefender le permite supervisar lo que hace su hijo en el equipo. En caso de contenidos inapropiados, puede decidir restringir su acceso a Internet o a ciertas aplicaciones.

Haga clic en **Configurar** en el módulo Asesor parental para empezar a configurar los dispositivos de sus hijos y monitorizar sus actividades desde cualquier parte.

Para obtener más información sobre la configuración del Asesor parental, consulte "*Asesor parental*" (p. 160).

CIFRAR ARCHIVOS

Cree unidades lógicas encriptadas y protegidas por contraseña (o blindajes) en su equipo donde podrá almacenar con seguridad todos sus documentos confidenciales y sensibles.

Para obtener más información acerca de cómo crear unidades lógicas cifradas protegidas por contraseña (o blindajes) en su equipo, consulte "*Cifrado de archivo*" (p. 122).

Herramientas

En la sección Herramientas puede mejorar la velocidad del sistema y administrar sus dispositivos.

Optimizador

Bitdefender Total Security no sólo ofrece seguridad, sino que también le ayuda a mantener en forma el funcionamiento de su equipo.

En el módulo Optimizador puede acceder a una serie de herramientas útiles:

- Optimizador en un clic
- Optimizador de inicio
- Limpieza de disco

Para obtener más información acerca de las herramientas de optimización del rendimiento, consulte "*Herramientas*" (p. 174).

Antirrobo

Bitdefender Antirrobo protege su equipo e información contra robo o pérdida. En caso de un evento de este tipo, le permite localizar de forma remota o bloquear su equipo. También puede borrar todos los datos presentes en su sistema.

Bitdefender Antirrobo ofrece las siguientes características:

- Localizar remotamente
- Bloqueo remoto
- Borrado remoto
- Alerta remota

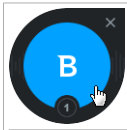
Para obtener más información sobre cómo puede evitar que su sistema caiga en malas manos, consulte "*Antirrobo de Dispositivos*" (p. 170).

Widget de seguridad

El **Widget de seguridad** es la forma rápida y fácil de monitorizar y controlar Bitdefender Total Security. Añadir este pequeño y no intrusivo widget a su escritorio le permite ver la información crítica y realizar tareas clave en todo momento:

- abra la ventana principal de Bitdefender.
- monitorice la actividad del análisis en tiempo real.
- monitorice el estado de seguridad de su sistema y solucione cualquier incidencia existente.
- vea cuándo una actualización está en curso.

- vea las notificaciones y tenga acceso a los últimos eventos de los que haya informado Bitdefender.
- analice archivos o carpetas arrastrando y soltando uno o varios elementos sobre el widget.



Widget de seguridad

El estado global de seguridad de su equipo se muestra **en el centro** del widget. El estado está indicado por el color y la forma del icono que se muestra en esta área.


Las incidencias críticas afectan a la seguridad de su sistema.

Requieren su atención inmediata y deben ser reparadas lo antes posible. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.


Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.


Su sistema está protegido.


Cuando hay un análisis bajo demanda en curso, se muestra este icono animado.

Cuando se informe sobre las incidencias, haga clic en el icono de estado para ejecutar el asistente de Solución de incidencias.

En la **parte inferior** del widget se muestra el contador de eventos no leídos (el número de eventos destacados de los que ha informado Bitdefender, si los hay). Haga clic en el contador de eventos, por ejemplo  para un evento no leído, para abrir la ventana de Notificaciones. Para más información, por favor vea “Notificaciones” (p. 17).

Análisis de archivos y carpetas

Puede usar el Widget de seguridad para analizar rápidamente archivos y carpetas. Arrastre cualquier archivo o carpeta que desee analizar y suéltelo sobre el **Widget de seguridad**.

El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Las opciones de análisis están preconfiguradas para obtener los mejores resultados de detección y no se pueden cambiar. Si se detectan ficheros infectados, Bitdefender intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados.

Ocultar / mostrar el Widget de seguridad

Cuando no desee ver más el widget, haga clic en .

Para restaurar el Widget de seguridad, utilice uno de los métodos siguientes:

- Desde el área de notificación:
  1. Haga clic derecho en el icono de Bitdefender en el área de notificación.
  2. Haga clic en **Mostrar widget de seguridad** en el menú contextual que aparece.
- Desde la interfaz de Bitdefender:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Seleccione la pestaña **General**.
  3. Active Mostrar widget de seguridad haciendo clic en el conmutador correspondiente.

Actividad

La ventana de actividad muestra información sobre las medidas adoptadas por Bitdefender en su dispositivo durante los últimos treinta días. Aquí puede comprobar qué aplicaciones, amenazas y ataques se bloquearon durante este período, y si se sufrió algún intento de ransomware. Además, puede acceder al panel de control de Actividad de Bitdefender Central haciendo clic en el enlace correspondiente.

También se puede acceder al Informe de seguridad, que describe el estado semanal de su producto y le ofrece varios consejos para mejorar la protección del sistema, haciendo clic en el enlace correspondiente. Estos consejos son importantes para gestionar la protección general y puede ver fácilmente las acciones que puede llevar a cabo sobre su sistema.

El informe se genera una vez a la semana y resume la información importante sobre la actividad de su producto de forma que pueda entender fácilmente qué ocurrió durante este periodo de tiempo.

La protección que ofrece el Informe de seguridad se divide en tres categorías:

- Área **Protección** - vea información relacionada con la protección de su sistema.
  - **Archivos analizados**

    Le permite ver los archivos analizados por Bitdefender esta semana. Puede consultar detalles como el número de archivos analizados y el número de archivos limpiados por Bitdefender.

    Para obtener más información sobre la configuración de la protección antispam, por favor consulte "*Protección Antivirus*" (p. 84).
  - **Páginas web analizadas**

    Le permite comprobar el número de páginas Web analizadas y bloqueadas por Bitdefender. Para protegerle de la divulgación de información personal mientras navega, Bitdefender asegura su tráfico Web.

    Para obtener más información sobre la protección Web, consulte "*Protección Web*" (p. 119).
  - **Sistema**

    Le permite identificar y corregir fácilmente las vulnerabilidades del sistema con el fin de hacer que su equipo sea más seguro ante el malware y los hackers.

    Para obtener más información sobre el Análisis de vulnerabilidades, consulte "*Vulnerabilidad*" (p. 128).
  - **Cronología de eventos**

    Le permite disponer de una imagen global de todos los procesos de análisis y los problemas solucionados por Bitdefender durante toda la semana. Los eventos se dividen por días.

Para obtener más información sobre el registro detallado de los eventos relativos a la actividad de su equipo, consulte "Notificaciones" (p. 17).

- Área de **privacidad** - vea información relacionada con la privacidad de su sistema.
  - **Archivos en el blindaje**

    Le permite ver cuántos archivos están protegidos contra accesos indeseados.

    Para obtener más información acerca de cómo crear unidades lógicas protegidas por contraseña cifradas (o blindajes) en su equipo, consulte "*Cifrado de archivo*" (p. 122).
- Área de **optimización** - vea la información relativa al espacio liberado, aplicaciones optimizadas y la cantidad de batería que ha ahorrado utilizando el modo Batería.
  - **Espacio liberado**

    Le permite ver cuánto espacio se ha liberado durante el proceso de optimización del sistema. Bitdefender utiliza el Optimizador para ayudarle a aumentar la velocidad de su sistema.

    Para obtener más información sobre el Optimizador, consulte "*Herramientas*" (p. 174).
  - **Batería ahorrada**

    Le permite ver la cantidad de batería que ahorró mientras el sistema funcionó en el modo Batería.

    Para obtener más información sobre el modo Batería, consulte "Perfil del modo Batería" (p. 184).
  - **Aplicaciones optimizadas**

    Le permite ver el número de aplicaciones que ha utilizado con los Perfiles.

    Para obtener más información sobre los Perfiles, consulte "*Perfiles*" (p. 178).

Consultar el informe de seguridad

El Informe de seguridad utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la

seguridad de su equipo y sus datos. Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad. Mediante este informe, puede configurar componentes específicos de Bitdefender o tomar medidas de prevención para proteger su equipo y sus datos privados.

Para consultar el Informe de seguridad:

1. Seleccione el informe:

   - Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

     Haga clic en el enlace **Informe de seguridad** que se encuentra en la esquina inferior derecha de la ventana del Informe de actividad.

   - Haga clic con el botón derecho en el icono de Bitdefender del área de notificación y seleccione **Mostrar informe de seguridad**.

   - Una vez que el informe está completo recibirá una notificación emergente. Haga clic en **Mostrar** para acceder al informe de actividad.

     Se abrirá una página Web en su navegador Web donde podrá ver el informe generado.

2. Eche un vistazo a la parte superior de la ventana para ver el estado general de seguridad.
3. Consulte nuestras recomendaciones en la parte inferior de la página.

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.
- **El área aparece en naranja.** Hay incidencias no críticas que afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas.
- **El área aparece en rojo.** Hay incidencias críticas que afectan a la seguridad de su sistema. Debe tratar estas incidencias de inmediato.

Activar y desactivar la notificación del Informe de seguridad

Para activar y desactivar la notificación del Informe de seguridad:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **General**.
3. Haga clic en el conmutador correspondiente para activar o desactivar la notificación del Informe de seguridad.

   La notificación del Informe de seguridad está activada de forma predeterminada.

2.3. Bitdefender Central

Bitdefender Central es la plataforma Web en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet con solo acceder a https://central.bitdefender.com. Una vez que haya iniciado sesión, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos Windows, OS X y Android. Los productos disponibles para su descarga son:
  - Bitdefender Total Security
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.
- Proteja los dispositivos de red y sus datos contra robo o pérdida con Antirrobo.

Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central. Dependiendo de la tarea que desee realizar, puede optar por cualquiera de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender:

  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Seleccione el enlace **Acceder a Bitdefender Central**.
3. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.

- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a Internet.
  2. Diríjase a: https://central.bitdefender.com.
  3. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.

Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.

Aquí tiene información sobre la disponibilidad de las suscripciones que posee y el número de dispositivos que utilizan cada una de ellas.

Puede añadir un nuevo dispositivo a una suscripción o renovarlo seleccionando una tarjeta de suscripción.

Nota
Puede tener una o más suscripciones en su cuenta siempre que sean para diferentes plataformas (Windows, Mac OS X o Android).

Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Total Security de la siguiente manera:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.

4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Renovar suscripción

Si no opta por la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.
3. Seleccione la tarjeta de suscripción deseada.
4. Haga clic en **RENOVAR** para continuar.

Se abrirá una página Web en su navegador de Internet, donde puede renovar su suscripción de Bitdefender.

Activar la suscripción

Una suscripción se puede activar durante el proceso de instalación mediante su cuenta de Bitdefender. Tras el proceso de activación, su validez comienza una cuenta atrás.

Si ha comprado un código de activación a uno de nuestros resellers o si lo ha recibido de regalo, puede añadir su disponibilidad a cualquier suscripción de Bitdefender disponible en su cuenta, siempre que sea para el mismo producto.

Para activar una suscripción mediante un código de activación:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.

4. Haga clic otra vez en el botón **CÓDIGO DE ACTIVACIÓN**.

La suscripción ya está activada. Acceda al panel **Mis dispositivos** y seleccione **INSTALAR Bitdefender** para instalar el producto en uno de sus dispositivos.

Mis dispositivos

El área **Mis dispositivos** en Bitdefender Central le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de dispositivo muestran el nombre del mismo, el estado de protección y la disponibilidad restante de su suscripción.

Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Ajustes**.
4. Cambie el nombre del dispositivo en el campo correspondiente y, a continuación, seleccione **Guardar**.

En caso de que el Autopilot esté desactivado, puede activarlo haciendo clic en el conmutador. Haga clic en **Guardar** para aplicar los cambios.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Perfil**.
4. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes, establezca el sexo, la fecha de nacimiento e incluso añada una imagen al perfil.
5. Haga clic en **AÑADIR** para guardar el perfil.

6. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, haga clic en **ASIGNAR**.

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Actualizar**.

Para tener acceso a más acciones remotas e información acerca de su producto Bitdefender en un dispositivo concreto, haga clic en la tarjeta de dicho dispositivo.

Una vez que haga clic en una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de Control**. En esta ventana puede comprobar el estado de protección de sus productos Bitdefender y el número de días restantes de su suscripción. El estado de protección puede ser verde, cuando no hay ningún problema que afecte a su producto, o rojo cuando el dispositivo está en riesgo. Cuando existan problemas que afecten a su producto, haga clic en **Ver incidencias** para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Haga clic en el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.Para más información sobre estos dos procesos de análisis, consulte “Ejecución de un análisis del sistema” (p. 93) y “Ejecución de un análisis Quick Scan” (p. 92).
- **Optimizador**. Aquí puede mejorar el rendimiento de un dispositivo de forma remota mediante un rápido análisis, detección y limpieza de archivos inútiles. Haga clic en el botón **INICIAR** y, a continuación, seleccione las áreas que desea optimizar. Haga clic nuevamente en el botón **INICIAR** para poner en marcha el proceso de optimización. Haga clic en **Más detalles** para acceder a un informe pormenorizado acerca de los problemas solucionados.

Además, puede mejorar el arranque de su dispositivo identificando qué aplicaciones tienen un alto consumo de recursos del sistema. Haga clic en el botón **INICIO** y, a continuación, elija lo que quiere hacer con las aplicaciones detectadas. Para más información sobre estas características, consulte "Optimizar la velocidad de su sistema con un solo clic" (p. 174) y "Optimización del tiempo de arranque de su PC" (p. 175).

- **Antirrobo**. Si no se acuerda de dónde ha puesto su dispositivo o si se lo han robado o lo ha perdido, con la función Antirrobo puede localizarlo y llevar a cabo acciones remotas. Haga clic en **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora. Para más información sobre esta característica, consulte "*Antirrobo de Dispositivos*" (p. 170).
- **Vulnerabilidad**. Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, haga clic en el botón **ANALIZAR** en la pestaña de Vulnerabilidad. Las vulnerabilidades no se pueden solucionar de forma remota. En caso de encontrar cualquier vulnerabilidad, tendrá que ejecutar un nuevo análisis en el dispositivo y adoptar las medidas recomendadas. Haga clic en **Más detalles** para acceder a un informe detallado acerca de los problemas encontrados. Para más información sobre esta característica, consulte "*Vulnerabilidad*" (p. 128).

Actividad

El área de Actividad de Bitdefender Central solo está disponible para los usuarios que tengan asociada a sus cuentas una suscripción a Bitdefender Family Pack 2017 o Bitdefender Total Security 2017. Su misión es informarle de cómo ha protegido Bitdefender durante los últimos siete días los dispositivos en que se encuentra instalado, y mostrar información acerca de la suscripción incluida.

Una vez que accede a la ventana **ACTIVIDAD**, tiene a su disposición las siguientes fichas:

- **Protección**. Aquí puede ver información acerca de los archivos, aplicaciones y URL que se han bloqueado debido a su comportamiento sospechoso. Para indicarle cuándo se han producido las incidencias, dispone de gráficos que muestran los datos recopilados por días, así como el número de amenazas detectadas. Además, puede mover el ratón sobre los datos mostrados para averiguar el número de amenazas detectadas.

En la parte inferior de la ficha puede ver el nombre del dispositivo con mayor número de amenazas.

- **Optimizador**. Desde aquí puede optimizar el rendimiento de los dispositivos de Windows donde haya instalado el producto Bitdefender Total Security. La información mostrada se basa en el módulo Optimizador de inicio de Bitdefender, que muestra qué aplicaciones se ejecutan durante el inicio del sistema y le permite gestionar su comportamiento en este punto. Dependiendo de las decisiones adoptadas por la comunidad en cuanto a la aplicación del comando **Posponer**, solo se muestran los tres dispositivos principales. Haga clic en **Aplicar** para realizar los cambios sugeridos en el dispositivo seleccionado.

  Haga clic en el enlace que muestra el número de aplicaciones detectadas y el ahorro de tiempo para ver las decisiones de otros usuarios de Bitdefender. Se muestra la información acerca del tiempo que tarda su sistema en arrancar, el tiempo que necesitan las aplicaciones en el inicio y el tiempo optimizado. Seleccione **POSPONER TODAS** si no desea que se ejecuten en el inicio. Para obtener más información acerca del módulo Optimizador de inicio de Bitdefender, consulte "Optimización del tiempo de arranque de su PC" (p. 175).

  > **Nota**
  > Si no tiene instalada la protección de Bitdefender en sus dispositivos Windows, la ficha **Optimizador** no contendrá información alguna.

- **Suscripción**. Aquí puede ver el número de dispositivos que cubre su suscripción y en cuántos ha instalado la protección de Bitdefender. Para instalar Bitdefender en otros dispositivos, haga clic en el botón **INSTALAR** en el sistema operativo que desee y siga los pasos requeridos.

  El nombre de la suscripción en uso se muestra junto con un punto de color:

  - Morado – su suscripción está activa.
  - Rojo – su protección está a punto de caducar. Le recomendamos renovarla lo antes posible para mantener sus dispositivos protegidos.

  Haga clic en el enlace **Más detalles** para que se le redirija a la página **Suscripciones**, donde puede ver información detallada acerca de su suscripción activa.

2.4. Mantenimiento de Bitdefender al día

Cada día se encuentra e identifica nuevo software malintencionado. 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 omisión, busca actualizaciones cuando enciende su equipo y 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. 78).
- 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. 198).
- 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. 45).

Comprobar si Bitdefender está actualizado

Para averiguar cuándo actualizó Bitdefender por última vez, compruebe el **Estado de seguridad**, a la izquierda del área de Estado.

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

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente a la última actualización.

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.

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 interfaz de Bitdefender y haga clic en el enlace **ACTUALIZAR AHORA** que hay debajo del estado de su programa.
- Haga clic con el botón derecho en el icono de Bitdefender en el área de notificación y seleccione **Actualizar ahora**.

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. Le recomendamos que lo haga lo antes posible.

También puede realizar actualizaciones en sus dispositivos de forma remota, siempre y cuando estén encendidos y conectados a Internet.

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono de la tarjeta del dispositivo deseado y, a continuación, seleccione **Actualizar**.

Activar o desactivar la actualización automática

Para activar o desactivar la actualización automática:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
3. Haga clic en el conmutador correspondiente para activar o desactivar la actualización automática.
4. Aparecerá una ventana de advertencia. Debe confirmar esta elección seleccionando del menú cuánto tiempo desea que esté deshabilitada la actualización automática. Puede desactivar la actualización automática durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se 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. Si Bitdefender no se actualiza regularmente, no podrá protegerle contra las amenazas más recientes.

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 modificar los ajustes de actualización:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar** y ajuste la configuración de acuerdo a sus preferencias.

Frecuencia de actualización

Bitdefender está configurado para buscar actualizaciones cada hora. Para cambiar la frecuencia de actualización, arrastre el control deslizante sobre la escala para establecer el período de tiempo deseado en que deben producirse las actualizaciones.

Ubicación de la actualización

Bitdefender esta configurado para actualizarse desde los servidores de actualización en Internet de Bitdefender. La ubicación de actualización es 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).

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.

3. CÓMO

3.1. Pasos de la Instalación

¿Cómo instalo Bitdefender en un segundo equipo?

Si la suscripción que ha adquirido cubre más de un equipo, puede utilizar su cuenta Bitdefender para activar un segundo PC.

Para instalar Bitdefender en un segundo equipo:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Ejecute el producto Bitdefender que ha descargado. Espere hasta que el proceso de instalación se haya completado y cierre la ventana.

El nuevo dispositivo en el que ha instalado el producto Bitdefender aparece en el panel de control de Bitdefender Central.

¿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 Bitdefender Central.

Para obtener más información acerca del proceso de instalación de Bitdefender consulte "*Instalando su producto Bitdefender*" (p. 4).

¿Desde dónde puedo descargar mi producto Bitdefender?

Puede instalar Bitdefender desde el disco de instalación, o recurrir al instalador Web que puede descargar en su equipo desde la plataforma de Bitdefender Central.

Nota
Antes de ejecutar el kit, se recomienda desinstalar cualquier solución antivirus instalada en su sistema. Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable.

Para instalar Bitdefender desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Ejecute el producto Bitdefender que ha descargado.

¿Cómo puedo cambiar el idioma de mi producto Bitdefender?

Si desea utilizar Bitdefender en otro idioma, tendrá que volver a instalarlo en el idioma adecuado.

Para utilizar Bitdefender en otro idioma:

1. Desinstalar Bitdefender siguiendo estos pasos:
   - En **Windows 7**:
     a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
     b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
     c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
        - Archivos trasladados a la cuarentena
        - Wallets
        - Blindaje de Archivos
     d. Haga clic en **CONTINUAR**.
     e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
   - En **Windows 8 y Windows 8.1**:
     a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
     b. Haga clic en **Desinstalar un programa** o **Programas y características**.
     c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
     d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
        - Archivos trasladados a la cuarentena
        - Wallets
        - Blindaje de Archivos
     e. Haga clic en **CONTINUAR**.
     f. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
   - En **Windows 10**:
     a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

f. Haga clic en **CONTINUAR**.

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

2. Cambiar el idioma de Bitdefender Central:

a. Acceda a Bitdefender Central.

b. Haga clic en el icono de la parte superior derecha de la pantalla.

c. Haga clic en **Mi cuenta** en el menú deslizante.

d. Seleccione la pestaña **Perfil**.

e. Seleccione un idioma del cuadro de lista desplegable **Idioma** y, a continuación, haga clic en **GUARDAR**.

3. Descargue el archivo de instalación:

a. Seleccione el panel **Mis dispositivos**.

b. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.

c. Escoja una de las dos opciones disponibles:

- **DESCARGAR**

  Haga clic en el botón y guarde el archivo de instalación.

- **En otro dispositivo**

  Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.

4. Ejecute el producto Bitdefender que ha descargado.

¿Cómo utilizo mi suscripción de Bitdefender después de una actualización de Windows?

Esta situación se da cuando actualiza su sistema operativo y desear continuar utilizando la suscripción de Bitdefender.

Si está utilizando una versión anterior de Bitdefender puede actualizarse, sin cargo alguno, a la última versión de Bitdefender de la siguiente forma:

- Desde una versión anterior de Bitdefender Antivirus a la última versión de Bitdefender Antivirus disponible.
- Desde una versión anterior de Bitdefender Internet Security a la última versión de Bitdefender Internet Security disponible.
- Desde una versión anterior de Bitdefender Total Security a la última versión de Bitdefender Total Security disponible.

Existen 2 casos que pueden aparecer:

- Ha actualizado el sistema operativo utilizando Windows Update y observa que Bitdefender ya no funciona.

  En este caso, necesitará instalar el producto utilizando la última versión disponible.

  Para resolver esta situación:

  1. Desinstalar Bitdefender siguiendo estos pasos:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
       c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena
          - Wallets
          - Blindaje de Archivos
       d. Haga clic en **CONTINUAR**.

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

- En **Windows 8 y Windows 8.1**:

a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

e. Haga clic en **CONTINUAR**.

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

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

f. Haga clic en **CONTINUAR**.

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

2. Descargue el archivo de instalación:
   a. Acceda a Bitdefender Central.
   b. Seleccione el panel **Mis dispositivos**.
   c. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
   d. Escoja una de las dos opciones disponibles:
      - **DESCARGAR**

        Haga clic en el botón y guarde el archivo de instalación.
      - **En otro dispositivo**

        Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
3. Ejecute el producto Bitdefender que ha descargado.

- Ha cambiado su sistema y desea seguir utilizando la protección de Bitdefender.

  Por tanto, necesitará reinstalar el producto utilizando la última versión.

  Para resolver esta situación:

  1. Descargue el archivo de instalación:
     a. Acceda a Bitdefender Central.
     b. Seleccione el panel **Mis dispositivos**.
     c. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
     d. Escoja una de las dos opciones disponibles:
        - **DESCARGAR**

          Haga clic en el botón y guarde el archivo de instalación.
        - **En otro dispositivo**

          Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección

de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.

2. Ejecute el producto Bitdefender que ha descargado.

Para obtener más información acerca del proceso de instalación de Bitdefender consulte "*Instalando su producto Bitdefender*" (p. 4).

¿Cómo puedo reparar Bitdefender?

Si desea reparar su Bitdefender Total Security desde el menú de Inicio de Windows:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. Haga clic en **REPARAR** en la ventana que aparece.

     Esto puede llevar unos minutos.
  4. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Haga clic en **REPARAR** en la ventana que aparece.

     Esto puede llevar unos minutos.
  5. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Apps y características**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.

5. Haga clic en **REPARAR**.

   Esto puede llevar unos minutos.

6. Necesita reiniciar el equipo para completar el proceso.

3.2. Suscripciones

¿Cómo activo la suscripción de Bitdefender utilizando una clave de licencia?

Si tiene una clave de licencia válida y desea utilizarla para activar una suscripción de Bitdefender Total Security, hay dos opciones posibles:

- Ha actualizado desde una versión anterior de Bitdefender a la nueva:

  1. Una vez que la actualización a Bitdefender Total Security se haya completado, se le pedirá que inicie sesión en su cuenta de Bitdefender.
  2. Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.
  3. Haga clic en **INICIAR** para continuar.
  4. Aparecerá una notificación en la pantalla de su cuenta informándole de que se creó una suscripción. La suscripción creada será válida para los días restantes de su clave de licencia y para el mismo número de usuarios.

     Los dispositivos que utilicen versiones anteriores de Bitdefender y que estén registrados con la clave de licencia que haya convertido en suscripción han de activar el producto con la misma cuenta Bitdefender.

- Bitdefender no se había instalado previamente en el sistema:

  1. Una vez que el proceso de instalación se haya completado, se le pedirá que inicie sesión en su cuenta de Bitdefender.
  2. Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.
  3. Haga clic en **INICIAR SESIÓN** para continuar, y luego pulse el botón **FINALIZAR** para acceder a la interfaz de Bitdefender Total Security.
  4. Haga clic en el icono  de la barra lateral izquierda de la interfaz de Bitdefender.

5. Seleccione el enlace del **Código de activación**.

   Aparecerá una nueva ventana.

6. Haga clic en el enlace **¡Consiga ya su actualización GRATIS!**.

7. Escriba su clave de licencia en el campo correspondiente y haga clic en **ACTUALIZAR MI PRODUCTO**. Hay una suscripción con la misma disponibilidad y número de usuarios de su clave de licencia asociada a su cuenta.

3.3. Bitdefender Central

¿Cómo inicio sesión en Bitdefender Central usando otra cuenta online?

Ha creado una nueva cuenta Bitdefender y desea utilizarla a partir de ahora.

Para utilizar otra cuenta:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón **CAMBIAR CUENTA** para cambiar la cuenta vinculada al equipo.
3. Escriba la dirección de correo electrónico y la contraseña de su cuenta en los campos correspondientes y, a continuación, haga clic en **INICIAR SESIÓN**.

> **Nota**
> El producto Bitdefender de su dispositivo cambia automáticamente de acuerdo con la suscripción asociada a la nueva cuenta de Bitdefender.
> Si no hay ninguna suscripción disponible asociada a la nueva cuenta de Bitdefender, o si desea transferirla desde la cuenta anterior, puede ponerse en contacto con el soporte técnico de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

¿Cómo puedo desactivar los mensajes de ayuda de Bitdefender Central?

Para ayudarle a entender para qué vale cada opción de Bitdefender Central, el panel de control muestra mensajes de ayuda.

Si no desea ver este tipo de mensajes:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. Desactive la opción **Activar o desactivar los mensajes de ayuda**.

¿Cómo puedo dejar de ver las fotos tomadas en mis dispositivos?

Para dejar de visualizar las fotos tomadas en sus dispositivos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. Desactive la opción **Mostrar/no mostrar fotos hechas remotamente desde sus dispositivos**.

He olvidado la contraseña que establecí para cuenta Bitdefender. ¿Cómo la restablezco?

Para establecer una nueva contraseña para cuenta Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón **CAMBIAR CUENTA**.

   Aparecerá una nueva ventana.
3. Haga clic en el enlace **Olvidé mi contraseña**.
4. Escriba la dirección de correo electrónico utilizada para crear su cuenta Bitdefender y, a continuación, haga clic en el botón **RESTABLECER CONTRASEÑA**.
5. Compruebe su correo y haga clic en el botón proporcionado.
6. Escriba su dirección de correo electrónico en el campo correspondiente.

7. Introduzca la nueva contraseña. La contraseña debe tener al menos ocho caracteres e incluir números.
8. Haga clic en el botón **RESTABLECER CONTRASEÑA**.

De ahora en adelante, para acceder a su cuenta Bitdefender, escriba su dirección de correo electrónico y la nueva contraseña que acaba de establecer.

¿Cómo reestablezco la contraseña para la cuenta Bitdefender?

Para cambiar su contraseña actual de cuenta Bitdefender por otra nueva:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Cambiar contraseña**.
5. Escriba la contraseña antigua en el campo **Contraseña antigua**.
6. Escriba la nueva contraseña que desee establecer para su cuenta en el campo **Nueva contraseña**.
7. Haga clic en el botón **CAMBIAR CONTRASEÑA**.

De ahora en adelante, para acceder a su cuenta Bitdefender, escriba su dirección de correo electrónico y la nueva contraseña que acaba de establecer.

¿Cómo elimino mi cuenta Bitdefender?

Para eliminar su cuenta online de Bitdefender:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Eliminar cuenta**.
5. Haga clic en **ELIMINAR CUENTA** y, a continuación, en el botón **ENVIAR E-MAIL** para recibir un mensaje de correo electrónico de confirmación.

6. Haga clic en el botón **ELIMINAR CUENTA** del mensaje de correo electrónico que le hemos enviado.

   Aparecerá una nueva ventana.

7. Confirme su elección.

Nota
Una vez eliminada su cuenta Bitdefender, se cancelarán automáticamente todas las suscripciones activas vinculadas a ella y dejarán de funcionar los productos que utilicen sus credenciales.

3.4. Analizando con Bitdefender

¿Cómo analizo un archivo o una carpeta?

La manera más fácil para analizar un archivo o carpeta es hacer clic con el botón derecho en el objeto que desee analizar, escoger Bitdefender y seleccionar **Analizar con Bitdefender** en el menú.

Para completar el análisis, siga las indicaciones del asistente de Análisis antivirus. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

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 descargue archivos de Internet que crea que pueden ser peligrosos.
- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

¿Cómo analizo mi sistema?

Para llevar a cabo un análisis completo del sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
4. Siga el Asistente de análisis del sistema para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

   Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, por favor vea "Asistente del análisis Antivirus" (p. 97).

¿Cómo puedo programar un análisis?

Puede configurar su producto Bitdefender para que empiece a analizar las ubicaciones importantes del sistema cuando no esté frente a su equipo.

Para programar un análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. Seleccione el tipo de análisis que desea programar: análisis del sistema o Quick Scan y, a continuación, haga clic en **Opciones de análisis**.

   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **Nueva tarea personalizada**.
5. Active el conmutador **Programar**.

   Seleccione una de las opciones correspondientes para establecer una programación:

   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente

En la ventana de **Objetivos de análisis** puede seleccionar las ubicaciones que desea que se analicen.

¿Cómo creo una tarea de análisis personalizada?

Si desea analizar ubicaciones concretas en su equipo o configurar las opciones de análisis, configure y ejecute una tarea de análisis personalizada.

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

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. Haga clic en **Nueva tarea personalizada**. En la **pestaña Basic**, introduzca un nombre para el análisis y seleccione las ubicaciones a analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.

   Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar el nivel de análisis deseado.

   También puede elegir apagar el equipo cuando haya terminado el análisis si no se encuentran amenazas. Recuerde que este será el comportamiento por omisión cada vez que ejecute esta tarea.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
7. Utilice el conmutador correspondiente si desea establecer una programación para su tarea de análisis.
8. Haga clic en **Iniciar análisis** y siga el Asistente de análisis para completar el mismo. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
9. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

¿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:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Haga clic en el menú de acordeón **Lista de archivos y carpetas excluidas del análisis**.
6. Haga clic en el botón **AÑADIR**.
7. Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Aceptar**.
8. Haga clic en **Añadir** para guardar los cambios y cerrar la ventana.

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

Puede haber casos en los que Bitdefender marque erróneamente como amenaza un archivo legítimo (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. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.

d. En la pestaña **Residente**, haga clic en el conmutador correspondiente para desactivar el análisis on-access.

   Aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

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. 80).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. Seleccione la pestaña **Cuarentena**.
   e. 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. 62).
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. 290).

¿Cómo compruebo qué virus ha detectado Bitdefender?

Cada vez que se realiza un análisis, se crea un registro y Bitdefender anota los problemas detectados.

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 revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   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.
3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.
4. Para abrir un registro de análisis, haga clic en **VER LOG**.

3.5. Asesor parental

¿Cómo puedo proteger a mis hijos frente a las amenazas online?

El Asesor parental de Bitdefender le permite restringir el acceso a Internet y a determinadas aplicaciones para evitar que sus hijos vean contenidos inapropiados cuando usted no está.

Para configurar el Asesor parental:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Asesor parental**.

   Se le redirigirá a la página Web de cuenta Bitdefender. Asegúrese de que ha iniciado sesión con sus credenciales.
3. Se abre el panel de control del Asesor parental. Aquí es donde puede comprobar y configurar los ajustes del Asesor parental.
4. Haga clic en **AÑADIR PERFIL** en el lado derecho de la ventana **MIS HIJOS**.

5. Indique la información correspondiente en los campos, como por ejemplo: nombre, sexo y fecha de nacimiento y, a continuación, haga clic en **CONTINUAR**.

   Basándose en los estándares de desarrollo de los niños, al establecer la fecha de nacimiento de su hijo se cargan automáticamente unas especificaciones que se consideran apropiadas para su edad.

6. Si el dispositivo de su hijo ya tiene instalado Bitdefender Total Security, seleccione su dispositivo en la lista y, a continuación, haga clic en **CONTINUAR**.

   Si el dispositivo de su hijo no tiene un producto Bitdefender con la función de Asesor parental incluida, haga clic en **Añadir un nuevo dispositivo**. Seleccione el sistema operativo de su dispositivo y haga clic en **CONTINUAR**.

   Escriba la dirección de correo electrónico a la que debemos enviar el enlace de descarga para la instalación de la aplicación del Asesor parental de Bitdefender.

   En los dispositivos basados en Windows, debe descargarse e instalarse el Bitdefender Total Security que ha incluido en su suscripción. En los dispositivos Android, debe descargarse e instalarse el agente del Asesor parental de Bitdefender.

Compruebe las actividades de sus hijos y cambie los ajustes del Asesor parental usando cuenta Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet.

¿Cómo bloqueo el acceso de mi hijo a un sitio Web?

El Asesor parental de Bitdefender le permite controlar los contenidos a los que accede su hijo mientras utiliza su dispositivo, así como bloquear el acceso a un sitio Web.

Para bloquear el acceso a un sitio Web tiene que añadirlo a la lista de exclusiones de la siguiente manera:

1. Diríjase a: https://central.bitdefender.com.
2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Haga clic en el **Asesor parental** para acceder al panel de control.

4. Seleccione el perfil de su hijo en la ventana **MIS HIJOS**.
5. Seleccione la pestaña de **Intereses**.
6. Haga clic en el botón **ADMINISTRAR**.
7. Escriba la página Web que desea bloquear en el campo correspondiente.
8. Seleccione **Permitir** o **Bloquear**.
9. Haga clic en **Finalizar** para guardar los cambios.

¿Cómo evito que mi hijo juegue a un juego?

El Asesor parental de Bitdefender le permite controlar los contenidos a los que accede su hijo mientras usa el equipo.

Para bloquear el acceso a un juego:

1. Diríjase a: https://central.bitdefender.com.
2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Haga clic en el **Asesor parental** para acceder al panel de control.
4. Seleccione el perfil de su hijo en la ventana **MIS HIJOS**.
5. Seleccione la pestaña **Actividades**.

   Se mostrará una lista con tarjetas. Las tarjetas representan las apps que usa su hijo.
6. Seleccione la tarjeta con la app que desea que su hijo deje de usar.

   El símbolo de marca de verificación que aparece indica que su hijo no podrá utilizar la app.

¿Cómo puedo evitar que mi hijo se ponga en contacto con personas que no son de fiar?

El Asesor parental de Bitdefender le brinda la posibilidad de bloquear las llamadas de números de teléfono desconocidos o de contactos de la agenda telefónica de su hijo.

Para bloquear determinado contacto:

1. Diríjase a: https://central.bitdefender.com.

2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Haga clic en el **Asesor parental** para acceder al panel de control.
4. Haga clic en el icono ⋮ de la tarjeta del perfil deseado y, a continuación, seleccione **Editar**.
5. Escriba el número de teléfono de su hijo en el campo correspondiente y, a continuación, haga clic en **GUARDAR**.
6. Seleccione el perfil del hijo para el que desea establecer restricciones.
7. Seleccione la pestaña **Amigos**.

   Se mostrará una lista con tarjetas. Las tarjetas corresponden a los contactos del teléfono de su hijo.
8. Seleccione la tarjeta con el número de teléfono que desee bloquear.

   El símbolo de marca de verificación que aparece indica que el número de teléfono seleccionado no podrá ponerse en contacto con su hijo.

Para bloquear los números de teléfono desconocidos, active el conmutador **Bloquear la comunicación con números no identificados**.

¿Cómo puedo establecer un lugar como seguro o como restringido para mi hijo?

El Asesor parental de Bitdefender le permite establecer lugares seguros o restringidos para su hijo.

Para establecer un lugar:

1. Diríjase a: https://central.bitdefender.com.
2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Haga clic en el **Asesor parental** para acceder al panel de control.
4. Seleccione el perfil de su hijo en la ventana **MIS HIJOS**.
5. Seleccione la pestaña **Lugares**.
6. Haga clic en **Dispositivos** en el marco que tiene en la ventana **Lugares**.
7. Haga clic en **ESCOGER DISPOSITIVOS** y, a continuación, seleccione el dispositivo que desea configurar.

8. En la ventana **Zonas**, haga clic en el botón **AÑADIR ZONA**.
9. Elija el tipo de lugar, **SEGURO** o **RESTRINGIDO**.
10. Escriba un nombre válido para la zona a la que su hijo tiene permiso para ir o no.
11. Establezca el rango que debe aplicarse para la supervisión en la barra **Radio**.
12. Haga clic en **AÑADIR ZONA** para guardar sus ajustes.

Siempre que quiera establecer un lugar restringido como seguro, o un lugar seguro como restringido, haga clic en él y, a continuación, pulse el botón **EDITAR ZONA**. Dependiendo del cambio que desee hacer, seleccione la opción **SEGURO** o **RESTRINGIDO** y, a continuación, haga clic en **ACTUALIZAR ZONA**.

Cómo eliminar un perfil de hijo

Si desea eliminar un perfil de hijo existente:

1. Diríjase a: https://central.bitdefender.com.
2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Haga clic en el **Asesor parental** para acceder al panel de control.
4. Haga clic en el icono ⋮ del perfil del hijo que desea eliminar y, a continuación, seleccione **Eliminar**.

3.6. Control de privacidad

¿Cómo me aseguro de que mis transacciones online son seguras?

Para asegurarse de que sus operaciones online se mantienen en privado, puede usar el navegador que le proporciona Bitdefender para proteger sus transacciones y aplicaciones de banca electrónica.

Bitdefender Safepay™ es un navegador seguro diseñado para proteger la información de su tarjeta de crédito, número de cuenta o cualquier otra información confidencial que pueda introducir al acceder a diferentes sitios online.

Para mantener sus actividades online protegidas y en privado:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Safepay**.
3. Haga clic en el botón para acceder al **Teclado virtual**.

   Utilice el **Teclado virtual** cuando teclee información sensible como sus contraseñas.

¿Qué puedo hacer si han robado mi dispositivo?

El robo de dispositivos móviles, ya sean smartphones, tablets o portátiles es uno de los principales problemas que afectan hoy en día a personas y organizaciones de todo el mundo.

El Antirrobo Bitdefender le permite no solo localizar y bloquear el dispositivo robado, sino también borrar toda la información del mismo para asegurarse de que el ladrón no podrá utilizarla.

Para acceder a las características de Antirrobo desde su cuenta:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, seleccione el dispositivo con el problema.
4. Haga clic en **Anti-Theft**.
5. Seleccione la característica que desea usar:
   - **LOCALIZAR** - muestra la ubicación de su dispositivo en Google Maps.
   - **Alerta**: envía una alerta al dispositivo.
   - **Bloquear** - bloquee su equipo y establezca un código numérico PIN para desbloquearlo. Como alternativa, active la opción correspondiente para permitir que Bitdefender tome instantáneas de la persona que esté tratando de acceder a su dispositivo.
   - **Borrar** - borra todos los datos de su equipo.

Importante
Después de borrar un dispositivo, todas las características de Anti-Theft dejan de funcionar.

- **Mostrar IP** - Muestra la última dirección IP del dispositivo seleccionado.

¿Cómo puedo utilizar los blindajes de archivos?

El Blindaje de Archivo de Bitdefender le permite crear cifrados, unidades lógicas protegidas con contraseña (o blindajes) en su equipo donde puede almacenar de forma segura sus documentos sensibles y confidenciales. Físicamente, el blindaje es un archivo guardado en el disco duro local que tiene la extensión .bvd.

Cuando crear un blindaje de archivo, dos aspectos son importantes: el tamaño y la contraseña. El tamaño de 100 MB predeterminado debería ser suficiente para sus documentos privados, archivos de Excel y otros datos similares. Sin embargo, para vídeo y otras archivos más grandes puede necesitar más espacio.

Para almacenar de forma segura los archivos o carpetas que contengan información confidencial o sensible en los blindajes de archivos de Bitdefender:

- **Crear un blindaje de archivo y establecer una contraseña fuerte para este.**

  Para crear un blindaje, haga clic con el botón derecho en un área vacía del escritorio o en una carpeta de su equipo, escoja **Bitdefender** > **Blindaje de archivo Bitdefender** y seleccione **Crear blindaje de archivo**.

  Aparecerá una nueva ventana. Siga estos pasos:

  1. Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.
  2. Seleccione la letra de la unidad en el menú. Cuando abre el blindaje, aparece una unidad de disco virtual etiquetada con la letra seleccionada en **Mi PC**.
  3. Introduzca la contraseña del blindaje en los campos **Contraseña** y **Confirme**.
  4. Si desea cambiar el tamaño por defecto del blindaje (100 MB), use las teclas de flecha arriba y abajo en **Tamaño del blindaje (MB)**.
  5. Haga clic en **Crear**.

> **Nota**
> Cuando abre el blindaje, aparece una unidad de disco virtual en **Mi PC**. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

- **Añada los archivos o carpetas que desee mantener a salvo al blindaje.**

  Para añadir un archivo a un blindaje, primero debe abrir el blindaje.

  1. Explorar hasta el archivo de blindaje .bvd.
  2. Haga clic derecho en el archivo de blindaje, apunte a Bitdefender Blindaje de Archivo y seleccione **Abrir**.
  3. En la ventana que aparece, introduzca la contraseña, seleccione una letra de unidad para el blindaje y haga clic en **Aceptar**.

  Puede realizar ahora operaciones en la unidad que corresponde al blindaje de archivo deseado utilizando Windows Explorer, igual que lo haría con una unidad normal. Para añadir un archivo a un blindaje abierto, puede también hacer clic derecho en el archivo, hacer clic en Blindaje de Archivos de Bitdefender y seleccionar **Añadir a Blindaje**.

- **Mantenga el blindaje bloqueado en todo momento.**

  Solo abra los blindajes cuando necesite acceder a ellos o administrar su contenido. Para bloquear un blindaje, haga clic derecho en la unidad de disco virtual correspondiente desde **Mi PC**, apunte a **Blindaje de Archivo Bitdefender** y seleccione **Bloquear**.

- **Asegurar no eliminar el archivo de blindaje .bvd.**

  Borrando el archivo también se borrará el contenido del blindaje.

Para más información sobre la operación con los blindajes de archivo, por favor diríjase a "*Cifrado de archivo*" (p. 122).

¿Cómo elimino permanentemente un archivo con Bitdefender?

Si desea eliminar un archivo de su sistema permanentemente, necesita eliminar físicamente la información de su disco duro.

El Destructor de archivos de Bitdefender le ayudará a eliminar rápidamente archivos o capetas de su ordenador usando el menú contextual de Windows, siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente, escoja Bitdefender y seleccione **Destructor de archivos**.
2. Aparecerá una ventana de confirmación. Haga clic en **Sí** para iniciar el asistente de Destrucción de archivos.
3. Espere a que Bitdefender finalice la destrucción de archivos.
4. Los resultados son mostrados. Haga clic en **Cerrar** para salir del asistente.

3.7. Herramientas de optimización

¿Cómo puedo mejorar el rendimiento de mi sistema?

El rendimiento del sistema depende no sólo de la configuración del hardware, sino también de la carga de la CPU, el uso de la memoria y el espacio del disco duro. También está conectado directamente a su configuración de software y a la administración de sus datos.

Estas son las principales acciones que puede tomar con Bitdefender para mejorar la velocidad y rendimiento de su sistema:

- "Optimice el rendimiento de su sistema con un solo clic" (p. 73)
- "Analice su sistema periódicamente" (p. 74)

Optimice el rendimiento de su sistema con un solo clic

La opción Optimizador en un clic le ahorra un tiempo valioso cuando desea una forma rápida de mejorar el rendimiento de su sistema mediante un rápido análisis, detección y limpieza de archivos inútiles.

Para iniciar el proceso del Optimizador en un clic:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Optimizador en un clic**.
3. Deje que Bitdefender busque los archivos que se pueden borrar y, a continuación, haga clic en el botón **OPTIMIZAR** para finalizar el proceso.

Para obtener más información sobre cómo puede aumentar la velocidad de su equipo con un solo clic, consulte "Optimizar la velocidad de su sistema con un solo clic" (p. 174).

Analice su sistema periódicamente

La velocidad y el comportamiento general de su sistema puede verse afectado por el malware.

Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana.

Se recomienda utilizar el análisis de sistema porque analiza todo los tipos de malware que amenazan la seguridad de su sistema y también analiza el contenido de los archivos comprimidos.

Para iniciar el análisis del sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
4. Siga los pasos del asistente.

¿Cómo puedo mejorar el tiempo de inicio de mi sistema?

Las aplicaciones innecesarias que prolongan irritantemente el tiempo que tarda su PC en arrancar pueden deshabilitarse o posponerse su apertura con el Optimizador de inicio, ahorrándose así un tiempo valioso.

Para utilizar el Optimizador de inicio:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Optimizador de inicio**.
3. Seleccione las aplicaciones que desee posponer en el arranque del sistema.

Para obtener más información sobre cómo optimizar el tiempo de arranque de su equipo, consulte “Optimización del tiempo de arranque de su PC” (p. 175).

3.8. Información de Utilidad

¿Cómo pruebo mi solución antivirus?

Para asegurarse de que su producto Bitdefender se ejecutara correctamente, le recomendamos que utilice la prueba Eicar.

La prueba Eicar le permite comprobar la protección de su antivirus utilizando un archivo seguro desarrollado para este fin.

Para probar su solución antivirus:

1. Descargue la prueba desde la página web oficial de la organización EICAR http://www.eicar.org/.
2. Haga clic en la pestaña **Anti-Malware Testfile**.
3. Haga clic en **Descargar** en el menú de la izquierda.
4. En **Download area using the standard protocol http** haga clic en el archivo de prueba **eicar.com**.
5. Se le informará de que la página a la que está intentando acceder contiene el EICAR-Test-File (no un virus).

   Si hace clic en **Comprendo los riesgos, ir ahí de todas formas**, se iniciará la descarga de la prueba y una ventana emergente de Bitdefender le informará de que se ha detectado un virus.

   Haga clic en **Más detalles** para obtener más información sobre esta acción.

Si no recibe ninguna alerta de Bitdefender, le recomendamos que contacte con Bitdefender para obtener soporte técnico como se describe en la sección "*Pedir ayuda*" (p. 290).

¿Cómo puedo eliminar Bitdefender?

Si desea eliminar su Bitdefender Total Security:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

4. Haga clic en **CONTINUAR**.
5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
4. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
   - Blindaje de Archivos
5. Haga clic en **CONTINUAR**.
6. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets

- Blindaje de Archivos

6. Haga clic en **CONTINUAR**.
7. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

¿Cómo apago el equipo automáticamente después de que finalice el análisis?

Bitdefender ofrece múltiples tareas de análisis que puede utilizar para asegurarse de que su sistema no está infectado con malware. Analizar todo el equipo puede que tarde más tiempo en completarse dependiendo de la configuración de hardware y software de su sistema.

Por esta razón, Bitdefender le permite configurar Bitdefender para que apague su sistema cuando el análisis haya acabado.

Piense en este ejemplo: ha acabado su trabajo con el equipo y quiere irse a dormir. Desearía que Bitdefender comprobase todo su sistema en busca de malware.

Así es como puede configurar Bitdefender para apagar su sistema al finalizar el análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. En la ventana **Administrar tareas de análisis**, haga clic en **Nueva tarea personalizada** para introducir un nombre para el análisis y seleccione las ubicaciones a analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.
6. Elija apagar el equipo cuando el análisis finalice si no se encuentra ninguna amenaza.
7. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
8. Haga clic en el botón **Iniciar análisis** para analizar su sistema.

Si no se encuentran amenazas, su equipo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, por favor vea “Asistente del análisis Antivirus” (p. 97).

¿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 administrar las opciones del proxy:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Active el uso del proxy haciendo clic en el conmutador.
4. Haga clic en el enlace **Gestionar proxys**.
5. 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 Google Chrome.

   - **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** - escriba un nombre de usuario que el proxy reconozca.
- **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

6. 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.

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

Para averiguar si tiene un sistema operativo de 32 o de 64 bits:

- En **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.
- En **Windows 7**:
  1. Desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono.

     En **Windows 8.1**, acceda a **Este equipo**.
  2. Seleccione **Propiedades** en el menú inferior.
  3. Consulte el área del sistema para ver su tipo de sistema.
- En **Windows 10**:
  1. Escriba "Sistema" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
  2. Consulte el área del sistema para obtener información sobre el tipo de sistema.

¿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**, y vaya al **Panel de control**.

   En **Windows 8 y Windows 8.1**: Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

2. Seleccione **Opciones de carpeta**.
3. Vaya a la pestaña **Ver**.
4. Seleccione **Mostrar archivo y carpetas ocultos**.
5. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
6. Desmarque **Ocultar archivos protegidos del sistema operativo**.
7. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

En **Windows 10**:

1. Escriba "Mostrar todos los archivos y carpetas ocultos" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Seleccione **Mostrar archivos, carpetas y unidades ocultos**.
3. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
4. Desmarque **Ocultar archivos protegidos del sistema operativo**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

¿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 Total Security 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:

- En **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.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Espere un momento a que el software instalado se muestre.
  4. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. 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.

¿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:

- En **Windows 7**:
  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.
- En **Windows 8, Windows 8.1 y Windows 10**:
  1. Acceda a la **Configuración del sistema** en Windows pulsando al mismo tiempo las teclas **Windows + R**.
  2. Escriba **msconfig** en el campo **Abrir** del cuadro de diálogo y, a continuación, haga clic en **Aceptar**.
  3. Seleccione la pestaña **Arranque**.
  4. En la sección de **Opciones de arranque**, marque la casilla de verificación **Arranque a prueba de errores**.
  5. Haga clic en **Red** y, a continuación, en **Aceptar**.
  6. Haga clic en **Aceptar** en la ventana de **Configuración del sistema** que le informa de que el sistema debe reiniciarse para realizar los cambios que acaba de establecer.

Su sistema se reiniciará en modo seguro con funciones de red.

Para reiniciarlo en modo normal, vuelva a cambiar los ajustes ejecutando nuevamente la **operación del sistema** y dejando sin marcar la casilla de verificación **Arranque a prueba de errores**. Haga clic en **Aceptar** y, a continuación, seleccione **Reiniciar**. Espere a que se apliquen los nuevos ajustes.

4. GESTIÓN DE SU SEGURIDAD

4.1. 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.

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. 101).

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. 103).

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. 106).

Si su equipo ha sido infectado con malware, por favor consulte *"Eliminando malware de su sistema"* (p. 210). 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 protegerle del ransomware y de aplicaciones maliciosas desconocidas, Bitdefender utiliza Active Threat Control (control activo de amenazas), una tecnología de heurística avanzada que monitoriza continuamente las aplicaciones que se ejecutan en su sistema. Active Threat Control bloquea automáticamente las aplicaciones que presentan un comportamiento similar al del malware, para evitar que dañen su equipo. En ocasiones, pueden bloquearse aplicaciones legítimas. En tal caso, se puede configurar Active Threat Control mediante la creación de reglas de exclusión para no bloquear las aplicaciones. Para obtener más información, consulte "Active Threat Control" (p. 107).

Análisis on-access (protección en tiempo real)

Bitdefender proporciona protección continua en tiempo real contra un amplio abanico de amenazas de malware, analizando todos los archivos a los que se accede y mensajes de correo electrónico.

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.

Activar o desactivar la protección en tiempo real

Para activar o desactivar la protección en tiempo real contra malware:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione el enlace **VER MÓDULOS**.

3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **Residente**, haga clic en el conmutador correspondiente para activar o desactivar el análisis on-access.
5. Si desea desactivar la protección en tiempo real, aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema. La protección en tiempo real se activará automáticamente cuando finalice el tiempo seleccionado.

> **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.

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:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **Residente**, 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.

Configuración de los ajustes de protección en tiempo real

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 configurar los ajustes de protección en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **PERSONALIZADO**.

   Aparecerá una nueva ventana.
5. Configure los ajustes del análisis como necesite.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

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.
- **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.

  Por omisión, tanto las carpetas locales como las compartidas en red están sujetas a análisis al acceso. Para un mejor rendimiento del sistema, puede excluir ubicaciones de red del análisis al acceso.

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 comprimidos.** 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 el correo electrónico y el tráfico HTTP.** 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 HTTP

  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 es recomendable, puede deshabilitar el análisis antivirus del tráfico Web y del correo electrónico para mejorar el rendimiento de su 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 archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
- **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los Keyloggers registran lo que escribe en el teclado y envían informes por Internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.
- **Analizar al arrancar el sistema.** Seleccione la opción de **Análisis de arranque** para analizar su sistema al iniciarse, tan pronto como se hayan cargado todos los servicios críticos. La finalidad de esta característica es mejorar la detección de virus en el inicio del sistema, así como el tiempo de arranque del mismo.

Medidas adoptadas sobre el malware detectado

Puede configurar las acciones llevadas a cabo por la protección en tiempo real.

Para configurar las acciones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.

4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **PERSONALIZADO**.

   Aparecerá una nueva ventana.

5. Seleccione la pestaña **Acciones** y configure los ajustes de análisis como desee.

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

Las siguientes acciones pueden llevarse a cabo por la protección en tiempo real en Bitdefender:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **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 intentará automáticamente eliminar 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. 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. 106).

  > **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.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  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.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.
  - Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

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. 106).

Bloquear acceso
Si se detecta un archivo infectado, se bloqueará el acceso al mismo.

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:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **NORMAL**.

Análisis solicitado

El objetivo principal de Bitdefender es mantener su ordenador libre de virus. Esto se consigue manteniendo los nuevos virus fuera de su equipo y

analizando los mensajes de correo y cualquier archivo nuevo descargado o copiado a su sistema.

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 está basado en tareas de análisis. Las tareas de análisis especifican las opciones de análisis y los objetos 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.

Analizar un archivo o una carpeta en busca de malware

Debe analizar archivos y carpetas que sospeche que puedan estar infectados. Haga clic con el botón derecho en el archivo o carpeta que desee analizar, escoja **Bitdefender** y seleccione **Analizar con Bitdefender**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

Ejecución de un análisis Quick Scan

El QuickScan 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 análisis Quick Scan:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Quick Scan**.
4. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre

los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

O, aún más rápido, haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender y, a continuación, haga clic en el botón de acción **Quick Scan**.

Ejecución de un análisis del sistema

La tarea de análisis del sistema analiza todo el equipo en busca de todo tipo de malware que amenace su seguridad, como virus, spyware, adware, rootkits y otros.

Nota
Ya que el **Análisis del sistema** realiza un análisis exhaustivo de todo el sistema, el análisis puede tomar cierto tiempo. Por lo tanto, se recomienda ejecutar esta tarea cuando no está utilizando su equipo.

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

- Asegúrese de que Bitdefender está actualizado con las firmas de malware. Analizar su equipo con firmas antiguas puede impedir que Bitdefender detecte nuevo malware surgido después de la última actualización. Para más información, por favor vea "*Mantenimiento de Bitdefender al día*" (p. 44).
- 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 "Configuración de un análisis personalizado" (p. 94).

Para ejecutar un Análisis del sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
4. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre

los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Configuración de un análisis personalizado

Para configurar detalladamente un análisis personalizado y luego ejecutarlo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. Haga clic en el botón **Nueva tarea personalizada**. En la **pestaña Basic**, introduzca un nombre para el análisis y seleccione las ubicaciones a analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**. Aparecerá una nueva ventana. Siga estos pasos:
   a. Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar 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. Puede además configurar estas opciones generales:

      - **Ejecutar la tarea con baja prioridad .** Disminuye la prioridad de los procesos 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 al área de notificación. Haga doble clic en el icono de Bitdefender para abrirlo.
      - Especifica la acción a realizar si no se encuentran amenazas.

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

6. Si desea establecer una programación para su tarea de análisis, utilice el conmutador **Planificar** en la ventana **Básico**. Seleccione una de las opciones correspondientes para establecer una programación:
   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente
7. 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. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
8. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

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 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.

- **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de rootkits y objetos ocultos que utilicen este tipo de software.

Asistente del análisis Antivirus

Cuando inicie un análisis bajo demanda (por ejemplo, haga clic con el botón derecho en una carpeta, escoja Bitdefender y seleccione **Analizar con Bitdefender**) aparecerá el asistente de Bitdefender Antivirus Scan. 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 - Ejecutar análisis

Bitdefender analizará los objetos seleccionados. Puede ver la información en tiempo real sobre el estado del análisis y las estadísticas (incluyendo el tiempo transcurrido, una estimación del tiempo restante y el número de amenazas detectadas).

Espere a que Bitdefender finalice el análisis. El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento que desee, haciendo clic en **Detener**. 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**.

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:

- **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 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.

Elija la acción deseada y haga clic en **Aceptar** para continuar el análisis.

Paso 2 - Elegir acciones

Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

Nota

Cuando ejecute un Quick Scan o un análisis del sistema, Bitdefender llevará automáticamente a cabo las acciones recomendadas sobre los archivos detectados durante el análisis. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

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:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **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 intentará automáticamente eliminar 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. 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. 106).

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.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  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.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.
  - Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Eliminar
Elimina los archivos detectados del disco.

Si se almacenan archivos infectados junto con archivos limpios en un mismo paquete, Bitdefender intentará limpiar los archivos infectados y reconstruir el paquete con los limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

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.

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

Paso 3 – 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.

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

Importante

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. En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección. Para más información e instrucciones sobre como eliminar malware manualmente, por favor consulte "*Eliminando malware de su sistema*" (p. 210).

Comprobación de los resultados del análisis

Cada vez que se realiza un análisis, se crea un registro del mismo y Bitdefender graba los problemas detectados en la ventana del antivirus. 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 revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   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.
3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.
4. Para abrir el registro de análisis, haga clic en **VER REGISTRO**.

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.

¿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). Aparece un icono de análisis de Bitdefender en el área de notificación. 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 Notificaciones.

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. 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 tomar ninguna acción en los archivos detectados como infectados o sospechosos en unidades de red si no tiene los privilegios apropiados.

3. 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. 210).

Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Discos y dispositivos**.

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 ficheros infectados. Las opciones de análisis son estándar y no las puede modificar.

Analizar archivo del host

El archivo hosts viene por defecto con la instalación de su sistema operativo y se utiliza para asignar direcciones IP a nombres de hosts cada vez que accede a una nueva página web, se conecta a un FTP o a otros servidores de Internet. Es un archivo de texto sin formato y los programas maliciosos pueden modificarlo. Los usuarios avanzados saben cómo usarlo para bloquear molestos anuncios, banners, cookies de terceros o programas de secuestro.

Para configurar el análisis del archivo hosts:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Haga clic en el conmutador correspondiente para activar o desactivar el análisis del archivo hosts.

Configurar exclusiones de análisis

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

Excluir del análisis los archivos y carpetas

Para excluir determinados archivos y carpetas del análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Haga clic en el menú de acordeón **Lista de archivos y carpetas excluidas del análisis**. 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**.
   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 es excluido 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**.

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 las extensiones de archivo del análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Haga clic en el menú de acordeón **Lista de extensiones excluidas del análisis**. 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**.
   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**.

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 las exclusiones de análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Utilice las opciones del menú de acordeón **Lista de archivos y carpetas excluidas del análisis** para gestionar las exclusiones del análisis.

6. 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**). Aparece una nueva ventana donde podrá cambiar la extensión o la ruta a excluir, y el tipo de análisis del que desea excluirlo. Haga los cambios necesarios y a continuación haga clic en **Modificar**.

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 administrar los archivos en cuarentena:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Cuarentena**.
5. 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 archivos sospechosos en cuarentena para un análisis detallado
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.

6. 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**.

Active Threat Control

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

Active Threat Control monitoriza continuamente 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 el ransomware detectado o la aplicación bloqueada a través de una ventana emergente. De lo contrario, la aplicación se bloquea sin ningún tipo de notificación. En la ventana Notificaciones puede comprobar qué aplicaciones ha detectado Active Threat Control.

Comprobando aplicaciones detectadas

Para comprobar las aplicaciones detectadas por Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al análisis de Active Threat Control.
3. Si confía en la aplicación, puede configurar Active Threat Control para que no vuelva a bloquearla haciendo clic en **PERMITIR Y MONITORIZAR**. Active Threat Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y comunicará a la nube de Bitdefender como error detectado.

Activar o desactivar Active Threat Control

Para activar o desactivar Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **Residente**, haga clic en el conmutador correspondiente para activar o desactivar el Active Threat Control.

Ajustar la protección de Active Threat Control

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

Para ajustar la protección de Active Threat Control, desplace el control deslizante por la escala para establecer el 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 Threat Control necesitará menos indicios de comportamiento afín al malware para informar de un proceso. Esto conducirá a un número mayor de aplicaciones objeto de informe, y al mismo tiempo, un aumento de falsos positivos (aplicaciones limpias detectadas como maliciosas).

Gestionar procesos excluidos

Puede configurar reglas de exclusión para las aplicaciones de confianza, de modo que Active Threat Control no las bloquee si realizan acciones típicas del malware. Active Threat Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y comunicará a la nube de Bitdefender como error detectado.

Para administrar las exclusiones de procesos de Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Haga clic en el menú de acordeón **Lista de procesos excluidos del análisis**.

   Desde aquí puede administrar las exclusiones de procesos de Active Threat Control.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **AÑADIR**.
   b. Haga clic en **Explorar**, busque y seleccione la aplicación a excluir y a continuación haga clic en **Aceptar**.
   c. Mantenga seleccionada la opción **Permitir** para evitar que Active Threat Control bloquee la aplicación.
   d. Haga clic en **Añadir**.
7. 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**.

4.2. Antispam

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

Bitdefender Antispam emplea sorprendentes innovaciones tecnológicas y filtros antispam estándares en la industria para impedir que el spam llegue a su bandeja de entrada. Para más información, por favor vea "Conocimientos antispam" (p. 111).

La protección Antispam de Bitdefender está disponible solo para clientes de correo configurados para recibir mensajes de correo mediante el protocolo POP3. POP3 es uno de los protocolos más extensos utilizados para descargar mensajes de correo de un servidor de correo.

> **Nota**
> Bitdefender no proporciona la protección antispam para cuentas de correo que accedes a través de un servicio de correo basado en web.

Los mensajes spam detectados por Bitdefender están marcados con el prefijo [spam] en linea del asunto. Bitdefender mueve automáticamente los mensajes de spam a una carpeta específica de la siguiente manera:

- En Microsoft Outlook, los mensajes de spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Elementos eliminados**. La carpeta **Spam** se crea durante la instalación de Bitdefender.
- En Mozilla Thunderbird, los mensajes spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Papelera**. La carpeta **Spam** se crea durante la instalación de Bitdefender.

Si utiliza otro cliente de correo, debe crear una regla para mover los mensajes de correo marcados como [spam] por Bitdefendera una carpeta de cuarentena personalizada.

Conocimientos antispam

Los Filtros Antispam

El Motor Antispam de Bitdefender incorpora protección cloud y otros filtros diversos que aseguran que su buzón esté libre de SPAM, como Lista de amigos, Lista de Spammers y Filtro de juego de caracteres.

Lista de amigos / Lista de Spammers

La mayoría de la gente se suele comunicar con el mismo grupo de personas, o recibe mensajes de empresas y organizaciones de la misma área laboral. Mediante el uso de listas de **amigos o spammers**, podrá distinguir fácilmente la gente de la que desea recibir correo electrónico (amigos), sin importar lo que el mensaje contenga, o la gente de la que no quiere saber nada (spammers).

Nota
Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Bitdefenderno bloquea los mensajes provenientes de este listado; de esta manera, al agregar amigos se asegura que los mensajes legítimos llegarán a su bandeja de entrada.

Filtro de carácteres

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

Manejo de Antispam

El motor de Bitdefender Antispam utiliza todos los filtros combinados para determinar si un correo puede entrar en su **Bandeja de Entrada** o no.

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

Por otra parte, el filtro de la Lista de spammers se hará cargo del e-mail para verificar si la dirección del remitente está en su lista. Si hay una coincidencia, el e-mail se catalogará como SPAM y se moverá a la carpeta de **Spam**.

Si el remitente no se encuentra en ninguno de los dos listados el Filtro de caracteres verificará si el mensaje está escrito con caracteres cirílicos o asiáticos. En tal caso, el mensaje será marcado como SPAM y trasladado a la carpeta **Spam**.

Nota
Si el correo está marcado como SEXUALMENTE EXPLÍCITO en la línea del asunto, Bitdefender lo considerará SPAM.

Clientes de correo electrónico y protocolos soportados

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

- Microsoft Outlook 2007 / 2010 / 2013
- Mozilla Thunderbird 14 o superior

Activar o desactivar la protección antispam

La protección antispam está habilitada por omisión.

Para desactivar el módulo Antispam:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTISPAM**.
4. Haga clic en el conmutador correspondiente para activar o desactivar el **Antispam**.

Utilizar la barra de herramientas antispam en su ventana de cliente de correo

En el área superior de la ventana de su cliente de correo puede ver la barra Antispam. La barra Antispam le ayuda a administrar la protección antispam

directamente desde su cliente de correo. Puede corregir a Bitdefender fácilmente si ha marcado un mensaje legítimo como SPAM.

Importante

Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, por favor diríjase a "Clientes de correo electrónico y protocolos soportados" (p. 112).

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

Configuración - abre una ventana donde puede configurar los filtros antispam y las opciones de la barra de herramientas.
Es spam - indica que el correo electrónico seleccionado es spam. El correo electrónico se trasladará de inmediato a la carpeta **Spam**. Si los servicios antispam en la nube están activados, se envía el mensaje a la nube de Bitdefender para su posterior análisis.
No es spam - indica que el e-mail seleccionado no es spam y Bitdefender no debería haberlo etiquetado. El correo será movido a la carpeta **Spam** de la **Bandeja de Entrada**. Si los servicios antispam en la nube están activados, se envía el mensaje a la nube de Bitdefender para su posterior análisis.

Importante

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

Añadir a Spammer - añade el remitente del correo seleccionado a la lista de Spammers. Puede que necesite hacer clic en **Aceptar** para admitirlo. Los mensajes de correo recibidos de las direcciones que están en la lista de Spammer son marcados automáticamente como [spam].
Añadir Amigo - añade el remitente del correo seleccionado a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
Spammers - abre la **Lista de Spammers** que contiene todas las direcciones de correo electrónico de las cuales no quiere recibir mensajes, independientemente de su contenido. Para más información, por favor vea "Configurando la Lista de Spammers" (p. 117).

Amigos - abre la **Lista de Amigos** que contiene todas las direcciones desde las que siempre quiere recibir mensajes, independientemente de su contenido. Para más información, por favor vea "Configurando la Lista de Amigos" (p. 115).

Indicar los errores de detección

Si está utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando qué mensajes de correo no deben ser marcados como [spam]). Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione el mensaje legítimos incorrecto marcado como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender para añadir los remitentes a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
5. Haga clic en el botón **No es spam** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo). El mensaje de correo electrónico se moverá a la carpeta Bandeja de entrada.

Indicando mensajes spam no detectados

Si esta utilizando un cliente de correo compatible, puede indicar fácilmente que mensajes de correo deben ser detectados como spam. Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta Bandeja de Entrada.
3. Seleccione los mensajes spam no detectados.

4. Haga clic en el botón **Es spam** en la barra antispam de Bitdefender (localizada normalmente en la parte superior de la ventana del cliente de correo). Inmediatamente serán marcados como [spam] y trasladados a la carpeta de correo no deseado.

Configurar las opciones de la barra de herramientas

Para configurar los ajustes de la barra de herramientas antispam para su cliente de correo electrónico, haga clic en el botón **Configuración** de la barra de herramientas y, a continuación, en la pestaña **Opciones de barra de herramientas**.

Aquí tiene las siguientes opciones:

- **Marcar mensajes de spam como 'leídos'** - marca automáticamente los mensajes de spam como leídos de forma que no causen ninguna molestia cuando se reciben.
- Puede elegir si desea o no mostrar las ventanas de confirmación cuando hace clic en los botones **Añadir spammer** y **Añadir amigo** en la barra de herramientas de antispam.

  Las ventanas de confirmación pueden evitar que se añadan accidentalmente remitentes de correo electrónico a la lista de Amigos / Correo no deseado.

Configurando la Lista de Amigos

La **Lista de amigos** es una lista con todas las direcciones de e-mail de las que siempre quiera recibir mensajes, cualquiera que sea su contenido. Los mensajes de sus amigos no serán marcados como spam, aunque su contenido tenga múltiples características del correo no solicitado.

Nota

Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Bitdefender no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al agregar a sus conocidos en el Listado de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de entrada.

Para configurar y administrar la lista de Amigos:

- Si está utilizando Microsoft Outlook o Thunderbird, haga clic en el botón **Amigos** en la barra de herramientas antispam de Bitdefender.

- Como alternativa:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el enlace **VER MÓDULOS**.
  3. En el módulo **ANTISPAM**, seleccione **Gestionar amigos**.

Para añadir una dirección de correo electrónico, seleccione la opción **Dirección de correo electrónico**, introduzca la dirección y haga clic en **Añadir**. Sintaxis: nombre@dominio.com.

Para añadir todas las direcciones de correo de un dominio específico, seleccione la opción **Nombre de Dominio**, introduzca el nombre de dominio y luego haga clic en el botón **Añadir**. Sintaxis:

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

Recomendamos evitar añadir dominios enteros, pero esto puede ser útil en algunas situaciones. Por ejemplo, puede añadir el dominio de correo de la compañía con la que trabaja, o sus distribuidores de confianza.

Para eliminar un elemento de la lista, haga clic en el enlace **Eliminar** correspondiente. Para eliminar todas las entradas de la lista, haga clic en el botón **Borrar lista**.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro equipo o después de reinstalar el producto. Para guardar la lista de Amigos, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión .bwl.

Para cargar una lista de Amigos previamente guardada, haga clic en el botón **Cargar** y abra el correspondiente archivo .bwl. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, seleccione **Sobrescribir la lista actual**.

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

Configurando la Lista de Spammers

El **Listado de Spammers** es un listado que reúne todas las personas cuyos mensajes no desea recibir más, independientemente de sus formatos o contenidos. Cualquier mensaje proveniente de una dirección incluida en su **listado de spammers** será automáticamente marcada como spam, sin procesamientos ulteriores.

Para configurar y administrar la lista de Spammers:

- Si está utilizando Microsoft Outlook o Thunderbird, haga clic en el botón **Spammers** en la barra de herramientas antispam Bitdefender integrada dentro de su cliente de correo.
- Como alternativa:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el enlace **VER MÓDULOS**.
  3. En el módulo **ANTISPAM**, seleccione **Gestionar emisores de spam**.

Para añadir una dirección de correo electrónico, seleccione la opción **Dirección de correo electrónico**, introduzca la dirección y haga clic en **Añadir**. Sintaxis: nombre@dominio.com.

Para añadir todas las direcciones de correo de un dominio específico, seleccione la opción **Nombre de Dominio**, introduzca el nombre de dominio y luego haga clic en el botón **Añadir**. Sintaxis:

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

Recomendamos evitar añadir dominios enteros, pero esto puede ser útil en algunas situaciones.

Aviso

No agregar dominio legítimos de correo basados en servicios web (como un Yahoo, Gmail, Hotmail u otros) a la lista de Spammers. De lo contrario, los mensajes recibidos de cualquier usuario registrados en estos servicios serán detectados como spam. Si, por ejemplo, añade yahoo.com a la lista de

Spammers, todas las direcciones de correo que vengan de yahoo.com serán marcados como [spam].

Para eliminar un elemento de la lista, haga clic en el enlace **Eliminar** correspondiente. Para eliminar todas las entradas de la lista, haga clic en el botón **Borrar lista**.

Puede guardar la lista de Spammers en un archivo la cual puede utilizarla en otro equipo o después de reinstalar el producto. Para guardar la lista Spammers, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión .bwl.

Para cargar una lista de Spammers previamente guardad, haga clic en el botón **Cargar** y abra el archivo correspondiente.bwl. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, seleccione **Sobrescribir la lista actual**.

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

Configuración de los filtros antispam locales

Cómo se describe en "Conocimientos antispam" (p. 111), Bitdefender utiliza una combinación de diferentes filtros antispam para identificar el spam. Los filtros antispam están preconfigurados para una protección eficiente.

Importante

Dependiendo en que si recibe o no correo legítimos escrito con caracteres Asiáticos o Cirílicos, desactive o active la configuración que bloquea automáticamente dichos correos. La correspondiente configuración está desactivada en las versiones del programa que utilizan conjunto de caracteres tales como (por ejemplo, en las versiones Rusas o Chinas).

Para configurar los filtros antispam locales:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTISPAM**.
4. Haga clic en los conmutadores para activar o desactivar los filtros locales antispam.

Si está utilizando Microsoft Outlook o Thunderbird, puede configurar los filtros antispam directamente desde su cliente de correo. Haga clic en el botón **Configuración** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y luego en la pestaña **Filtros antispam**.

Configurando la configuración de la nube

La detección en la nube hace uso de los servicios Cloud de Bitdefender para ofrecerle protección antispam siempre actualizada.

La protección cloud funciona mientras tenga activado Bitdefender Antispam.

Las muestras de correos electrónicos legítimos o spam pueden enviarse a la nube Bitdefender si indica errores de detección o correos electrónicos spam no detectados. Esto ayuda a mejorar la detección antispam de Bitdefender.

Configure el envío de muestras por correo electrónico a Bitdefender Cloud seleccionando las opciones deseadas siguiendo estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTISPAM**.
4. Seleccione las opciones deseadas desde la pestaña **Configuración**.

Si está utilizando Microsoft Outlook o Thunderbird, puede configurar la detección cloud directamente desde su cliente de correo. Haga clic en el botón **Configuración** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y luego en la pestaña **Configuración en la nube**.

4.3. Protección Web

La Protección Web de Bitdefender le garantiza una navegación segura por Internet, alertándole sobre posibles páginas Web maliciosas.

Bitdefender ofrece protección Web en tiempo real para:

- Internet Explorer
- Mozilla Firefox

- Google Chrome
- Safari

Para configurar los ajustes de la Protección Web:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN WEB**.

Haga clic en los conmutadores para activar o desactivar:

- Asesor de búsqueda, un componente que califica los resultados de las consultas en su motor de búsqueda y los enlaces publicados en sitios Web de redes sociales añadiendo un icono junto a cada resultado:

  No debería visitar esta página web.

  Esta página Web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.

  Esta página es segura.

  El Asesor de búsqueda califica los resultados de los siguientes motores de búsqueda:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  El Asesor de búsqueda califica los enlaces publicados en los siguientes servicios de redes sociales:
  - Facebook
  - Twitter
- Análisis de 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 contra el fraude.
- Protección contra phishing.

Puede crear una lista de los sitios Web que no serán analizados por los motores antiphishing, antifraude y antimalware de Bitdefender. La lista debería contener únicamente sitios web en los que confíe plenamente Por ejemplo, añada las páginas web en las que realice compras online.

Para configurar y administrar sitios Web utilizando la protección Web proporcionada por Bitdefender, 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.

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 que hacer a continuación. Tiene las siguientes opciones a su disposición:

- Abandone la página Web haciendo clic en **Llévame a un sitio seguro**.
- 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**.

4.4. Protección de datos

Eliminar archivos de forma permanente

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

El Destructor de archivos de Bitdefender le ayuda a borrar datos permanentemente mediante su eliminación física del disco duro.

Puede destruir rápidamente archivos y carpetas desde su equipo usando el menú contextual de Windows, siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente.
2. Seleccione **Bitdefender** > **Destructor de archivos** en el menú contextual que aparece.
3. Aparecerá una ventana de confirmación. Haga clic en **Sí** para iniciar el asistente de Destrucción de archivos.
4. Espere a que Bitdefender finalice la destrucción de archivos.
5. Los resultados son mostrados. Haga clic en **Cerrar** para salir del asistente.

De manera alternativa puede destruir los archivos desde la interfaz de Bitdefender.

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN DE DATOS**, seleccione **Destructor de archivos**.
4. Siga el asistente del Destructor de archivos:
   a. **Agregar carpeta(s)**

      Añada archivos o carpetas que desea eliminar para siempre.

   b. Haga clic en **Siguiente** y confirme que desea continuar con el proceso.

      Espere a que Bitdefender finalice la destrucción de archivos.

   c. **Resultados**

      Los resultados son mostrados. Haga clic en **Cerrar** para salir del asistente.

4.5. Cifrado de archivo

El Blindaje de Archivo de Bitdefender le permite crear unidades logicas cifradas y protegidos por contraseña en su equipo, en los que puede almacenar sus documentos confidenciales y sensibles. Sólo la persona que conozca la contraseña podrá acceder a los datos almacenados en los blindajes.

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

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

Pueden administrase cinco blindajes desde la ventana Bitdefender o utilizando el menú contexto de Windows y la unidad lógica asociada con el blindaje.

Administración de blindajes de archivos

Para administrar sus blindajes de archivos de Bitdefender, haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

Los blindajes de archivos existentes aparecen en el módulo **Blindajes de archivos**.

Crear blindajes de archivo

Para crear un nuevo blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **CIFRADO DE ARCHIVOS**, seleccione **Crear blindaje de archivos**.
4. Especifique el nombre y ubicación del blindaje de archivos.
   - Escriba el nombre del blindaje de archivos en el campo correspondiente.
   - Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.
5. Seleccione una letra de unidad en el menú correspondiente. Al abrir un blindaje, en Mi PC aparecerá un nuevo disco virtual con la letra de unidad seleccionada.
6. Si desea cambiar el tamaño por defecto del blindaje (100 MB), use las teclas de flecha arriba y abajo en **Tamaño del blindaje (MB)**.
7. Escriba la contraseña deseada para el blindaje en los campos **Contraseña** y **Confirmar contraseña**. La contraseña debe tener como mínimo 8

caracteres. Cada vez que alguien que intente abrir el blindaje y acceder a sus archivos, deberá introducir la contraseña.

8. Haga clic en **Crear**.

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para crear un blindaje más rápidamente, haga clic con el botón derecho en una carpeta de su equipo, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Crear blindaje de archivos**.

Nota
Podría ser conveniente guardar todos los blindajes de archivos en la misma ubicación. De esta manera, puede localizarlos fácilmente.

Abrir blindajes de archivo

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

Para abrir un blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

   Los blindajes de archivos existentes aparecen en el módulo **Blindajes de archivos**.

2. Haga clic en el enlace **Ver blindajes** y, a continuación, seleccione el blindaje que desea abrir.
3. Haga clic en el botón **Desbloquear** y, a continuación, escriba la contraseña necesaria.
4. Haga clic en **Aceptar** y, a continuación, en el botón **Abrir** para abrir su blindaje.

Bitdefender le informará de inmediato sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia.

Para abrir rápidamente un blindaje, busque en su equipo el archivo .bvd correspondiente al blindaje que desee abrir. Haga clic derecho en el archivo de blindaje de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de Bitdefender** y seleccione **Abrir**. Escriba la contraseña exigida y, a continuación, haga clic en **Aceptar**.

Añadir archivos a los blindajes

Antes de añadir ficheros o carpetas a un blindaje, deberá abrir el blindaje.

Para añadir nuevos archivos a su blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CIFRADO DE ARCHIVOS**.
4. En la ventana de **Mis blindajes**, seleccione el blindaje que desea abrir.
5. Haga clic en el botón **Desbloquear** y, a continuación, escriba la contraseña necesaria.
6. Haga clic en el botón **Abrir** para abrir su blindaje.
7. Añada archivos o carpetas como hace normalmente en Windows (por ejemplo, puede utilizar el método de copiar y pegar).

Para añadir archivos más rápidamente a su blindaje, haga clic con el botón derecho en el archivo o carpeta que desee copiar a un blindaje, seleccione **Blindaje de archivos de Bitdefender** y haga clic en **Añadir a blindaje de archivos**.

- Si sólo hay un blindaje abierto, el fichero o carpeta será copiado directamente a ese blindaje.
- Si hay varios blindajes abiertos, se le pedirá elegir a qué blindaje copiar el elemento. Seleccione desde el menú la letra correspondiente al blindaje deseado y haga clic en **Aceptar** para copiar el elemento.

Bloquear blindajes

Cuando acabe de trabajar con el blindaje de archivos, debería bloquearlo para proteger sus datos. Al bloquear el blindaje, la unidad de disco virual

desaparecerá de Mi PC. En consecuencia, el acceso a los datos guardados en el blindaje será completamente bloqueado.

Para bloquear un blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En el módulo **Blindajes de archivos**, seleccione **Ver blindajes**.
3. En la ventana **Mis blindajes**, seleccione el blindaje que desee bloquear.
4. Haga clic en el botón **Bloquear**.

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para bloquear más rápidamente un blindaje, haga clic con el botón derecho en el archivo .bvd correspondiente al blindaje, seleccione **Blindaje de archivos de Bitdefender** y haga clic en **Bloquear**.

Borrar archivos del blindaje

Para eliminar archivos o carpetas de un blindaje, el blindaje debe estar abierto. Para eliminar archivos o carpetas de un blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CIFRADO DE ARCHIVOS**.
4. En la ventana **Mis blindajes**, seleccione el blindaje del cual desea eliminar archivos.
5. Haga clic en el botón **Desbloquear** en caso de que esté bloqueado.
6. Haga clic en el botón **Abrir**.

   Elimina archivos o carpetas como lo hace en Windows (por ejemplo, clic derecho en un archivo que quiere eliminar y seleccione **Eliminar**).

Cambiar la contraseña del blindaje

La contraseña protege el contenido de un blindaje de accesos sin autorización. Sólo los usuarios que conocen la contraseña pueden abrir el blindaje y tener acceso a los documentos y datos guardados dentro de él.

El blindaje debe bloquearse antes de cambiar la contraseña. Para cambiar la contraseña de un blindaje:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CIFRADO DE ARCHIVOS**.
4. En la ventana **Mis blindajes**, seleccione el blindaje del cual desea cambiar la contraseña.
5. Haga clic en el botón **Configuración**
6. Introduzca la contraseña actual para el blindaje en el campo **Contraseña Antigua**.
7. Introduzca la nueva contraseña para el blindaje en los campos **Nueva Contraseña** y **Confirmar Nueva Contraseña**.

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

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para cambiar rápidamente la contraseña de un blindaje, busque en su equipo el archivo .bvd correspondiente al blindaje. Haga clic derecho en el archivo, sitúe el cursor en **Bitdefender Blindaje de Archivo** y seleccionar **Cambiar Contraseña del Blindaje**.

4.6. Vulnerabilidad

Un paso importante para la protección de su equipo frente a acciones o aplicaciones malintencionadas es mantener actualizado el sistema operativo y las aplicaciones que utiliza habitualmente. Es más, para evitar el acceso físico no autorizado a su equipo, deberán configurarse contraseñas seguras (contraseñas que no puedan adivinarse fácilmente) para cada cuenta de usuario de Windows y también para las redes Wi-Fi a las que se conecte.

Bitdefender comprueba automáticamente las vulnerabilidades de su sistema y le avisa sobre ellas. Se analiza en busca de lo siguiente:

- aplicaciones obsoletas en su equipo.
- Actualizaciones de Windows que faltan.
- contraseñas inseguras de cuentas de usuario de Windows.
- routers y redes inalámbricas que no sean seguras.

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 la opción **Análisis de vulnerabilidades**.
- Mediante la monitorización de vulnerabilidades, puede averiguar y corregir las vulnerabilidades detectadas en la ventana Notificaciones.

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

Analizar su sistema en busca de vulnerabilidades

Para reparar vulnerabilidades del sistema usando la opción Análisis de vulnerabilidades:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **VULNERABILIDADES**, seleccione **Análisis de vulnerabilidades**.
4. Espere a que Bitdefender compruebe su sistema en busca de vulnerabilidades. Para detener el proceso de análisis, haga clic en el botón **Omitir** en la parte superior de la ventana.

- **Actualizaciones críticas de Windows**

  Haga clic en **Ver detalles** para ver la lista de actualizaciones críticas de Windows que no están instaladas actualmente en su equipo.

  Para iniciar la instalación de las actualizaciones seleccionadas, haga clic en **Instalar actualizaciones**. 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.

- **Actualizaciones de aplicaciones**

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

  Haga clic en **Ver detalles** para ver la información sobre la aplicación que necesita actualizarse.

- **Contraseñas débiles de cuentas de Windows**

  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 **Cambiar contraseña al iniciar sesión** para establecer una nueva contraseña para su sistema.

  Haga clic en **Ver detalles** para modificar las contraseñas débiles. Puede elegir entre pedir al usuario 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 @).

- **Redes Wi-Fi vulnerables**

  Haga clic en **Ver detalles** para averiguar más sobre la red inalámbrica a la que está conectado. Si se le recomienda establecer una contraseña más segura para su red doméstica, haga clic en el enlace correspondiente.

  Cuando haya otras recomendaciones, siga las instrucciones que se le proporcionan para asegurarse de que su red doméstica se mantiene a salvo de las miradas indiscretas de los piratas informáticos.

En la esquina superior derecha de la ventana puede filtrar los resultados según sus preferencias.

Usar el control automático de la vulnerabilidad

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

Para revisar y reparar las incidencias detectadas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al Análisis de vulnerabilidades.
3. Puede ver información detallada sobre las vulnerabilidades del sistema detectadas. Dependiendo de la incidencia, para reparar una vulnerabilidad específica haga lo siguiente:
   - Si hay actualizaciones de Windows disponibles, haga clic en **INSTALAR**.
   - Si la actualización automática de Windows está desactivada, haga clic en **ACTIVAR**.
   - Si una aplicación está obsoleta, haga clic en **ACTUALIZAR AHORA** para encontrar un enlace a la página Web de los proveedores desde donde pueda instalar la última versión de esta aplicación.
   - Si una cuenta de usuario de Windows tiene una contraseña débil, haga clic en **CAMBIAR 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 **REPARAR** para desactivarla.
   - Si el router que ha configurado tiene establecida una contraseña vulnerable, haga clic en **CAMBIAR CONTRASEÑA** para acceder a su interfaz, desde donde podrá establecer una contraseña segura.
   - Si la red a la que está conectado presenta vulnerabilidades que podrían poner en riesgo a su sistema, haga clic en **CAMBIAR AJUSTES DE WI-FI**.

Para configurar los ajustes de la monitorización de vulnerabilidades:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **VULNERABILIDADES**.
4. Haga clic en el conmutador correspondiente para activar o desactivar el Análisis de vulnerabilidades.

   Importante
   Para recibir notificaciones automáticas sobre las vulnerabilidades del sistema o de aplicaciones, mantenga activada la opción **Vulnerabilidades**.

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 de aplicaciones
   Compruebe si las aplicaciones 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
   Compruebe si las contraseñas de los routers y 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 propagarse desde unidades extraíbles al PC. Esta es la razón por la que se recomienda deshabilitar esta opción de Windows.

Notificaciones de Asesor de seguridad Wi-Fi

Compruebe si la red inalámbrica doméstica a la que está conectado es segura o no, y si tiene vulnerabilidades. Además, compruebe si la contraseña de su router es lo suficientemente segura, y cómo puede hacer que lo sea aún más.

La mayoría de las redes inalámbricas desprotegidas no son seguras, lo que permite que las miradas indiscretas de los piratas informáticos se posen sobre sus actividades privadas.

Nota

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

Asesor de seguridad Wi-Fi

Mientras viaja, trabaja en un café o espera en el aeropuerto, conectarse a una red inalámbrica pública para hacer pagos o revisar sus mensajes de correo electrónico o cuentas de redes sociales puede ser la solución más rápida. Pero puede haber miradas indiscretas tratando de acceder a sus datos personales, observando cómo se filtra su información a través de la red.

Por datos personales se entienden las contraseñas y nombres de usuario que utiliza para acceder a sus cuentas online, como por ejemplo las de correo electrónico, bancos, o redes sociales, además de los mensajes que envíe.

Por lo general, es más habitual que las redes inalámbricas públicas sean poco fiables, ya que no requieren una contraseña al iniciar la sesión y, si lo hacen, esa contraseña se habrá puesto a disposición de cualquier persona que quisiera conectarse. Por otra parte, pueden constituir redes maliciosas o honeypots que suponen un objetivo para los delincuentes informáticos.

Para protegerle contra los peligros de los puntos de acceso inalámbricos públicos desprotegidos o sin cifrar, el Asesor de seguridad Wi-Fi de Bitdefender analiza el grado de seguridad de una red inalámbrica y, de ser necesario, le recomienda utilizar Bitdefender Safepay™ con la opción Punto de acceso Wi-Fi activada.

El Asesor de seguridad Wi-Fi de Bitdefender le brinda información sobre:

- Redes Wi-Fi domésticas

- Redes Wi-Fi públicas

Activar o desactivar las notificaciones del Asesor de seguridad Wi-Fi

Para desactivar las notificaciones del Asesor de seguridad Wi-Fi:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **VULNERABILIDADES**.
4. Haga clic en el conmutador correspondiente para activar o desactivar las **notificaciones del Asesor de seguridad Wi-Fi**.

Configurar una red Wi-Fi doméstica

Para empezar a configurar su red doméstica:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **VULNERABILIDADES**, seleccione **Asesor de seguridad Wi-Fi**.
4. En la pestaña **Wi-Fi doméstica**, haga clic en el botón **SELECCIONAR WI-FI DOMÉSTICA**.

   Se muestra una lista con las redes inalámbricas a las que se haya conectado hasta ese momento.
5. Elija su red doméstica y, a continuación, haga clic en **SELECCIONAR**.

Si una red doméstica se considera poco fiable o insegura, se muestran recomendaciones de configuración para mejorar su seguridad.

Para eliminar la red inalámbrica que ha establecido como red doméstica, haga clic en el botón **ELIMINAR**.

Wi-Fi Pública

Mientras esté conectado a una red inalámbrica poco fiable o insegura, se activará el perfil de Wi-Fi pública. Al trabajar bajo este perfil, Bitdefender Total Security se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Active Threat Control
- El cortafuego de Bitdefender está activado y se aplican los siguientes ajustes a su adaptador inalámbrico:
  - Modo oculto - ACTIVADO
  - Genérico - DESACTIVADO
  - Tipo de red - Pública
- Se activan los siguientes ajustes de la Protección Web:
  - Analizar SSL
  - Protección contra fraude
  - Protección contra phishing
- Hay disponible un botón que abre Bitdefender Safepay™. En este caso, se activa por defecto la protección de puntos de acceso para redes no seguras.

Revisar la información relativa a las redes Wi-Fi

Para revisar la información relativa a las redes inalámbricas a las que se conecte habitualmente:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **VULNERABILIDADES**, seleccione **Asesor de seguridad Wi-Fi**.
4. En función de la información que necesite, seleccione una de las pestañas: **Wi-Fi domésticas** o **Wi-Fi públicas**.
5. Haga clic en **Ver detalles** junto a la red de la que desea obtener más información.

Hay tres tipos de redes inalámbricas filtradas según su importancia, cada uno de los cuales se identifica mediante un icono:

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es bajo. Esto significa que existe un alto riesgo al usarla y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es moderado. Esto significa que puede presentar vulnerabilidades y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.

La red Wi-Fi es segura - Indica que la red que utiliza es segura. En este caso, puede intercambiar datos confidenciales en sus operaciones online.

Al hacer clic en el enlace **Más detalles** del apartado de cada red, se mostrará la siguiente información:

- **Cifrada** - Aquí puede ver si la red seleccionada está cifrada o no. Las redes sin cifrar pueden dejar expuestos los datos que utilice.
- **Tipo de cifrado** - Aquí puede ver el tipo de cifrado utilizado por la red seleccionada. Algunos tipos de cifrado pueden ser poco fiables. Por lo tanto, le recomendamos encarecidamente que revise la información relativa al tipo de cifrado que se muestra para asegurarse de que está protegido mientras navega por Internet.
- **Canal/Frecuencia** - Aquí puede ver la frecuencia del canal utilizado por la red seleccionada.
- **Seguridad de la contraseña** - Aquí puede ver el grado de seguridad de la contraseña. Tenga en cuenta que las redes que tienen contraseñas vulnerables constituyen un objetivo para los delincuentes informáticos.
- **Tipo de registro** - Aquí puede ver si la red seleccionada está protegida por contraseña o no. Es muy recomendable conectarse únicamente a redes que tengan establecidas contraseñas seguras.
- **Tipo de autenticación** - Aquí puede ver el tipo de autenticación utilizado por la red seleccionada.

Mantenga activada la opción **Notificar** para recibir notificaciones cada vez que su sistema se conecte a esta red.

4.7. Cortafuego

El cortafuegos protege su equipo frente a intentos de conexión no autorizados internos y externos, tanto en la red local como en Internet. Es muy similar a un guardia en su puerta, ya que mantiene un registro de intentos de conexión y decide cuál permitir y cuál bloquear.

El cortafuego de Bitdefender usa un conjunto de reglas para filtrar los datos transmitidos desde y hacia su sistema. Las reglas se agrupan en 2 categorías:

Reglas generales
: Reglas que determinan los protocolos sobre los que se permite la comunicación.

  Se usa un conjunto de reglas predeterminadas que proporcionan una protección óptima. Puede editar las reglas para permitir o denegar conexiones a través de ciertos protocolos.

Reglas de aplicación
: Reglas que determinan cómo puede acceder a los recursos de la red e Internet cada aplicación.

  En condiciones normales, Bitdefender crea automáticamente una regla cada vez que una aplicación intenta acceder a Internet. También puede añadir o editar manualmente las reglas para las aplicaciones.

Dependiendo del tipo de red, la protección del cortafuegos se ajusta al nivel apropiado para cada conexión.

Para saber más sobre las opciones del cortafuego para cada tipo de red y cómo editar la configuración de la red, vea "Administración de ajustes de conexión" (p. 141).

Activar o desactivar la protección del cortafuego

Para activar o desactivar la protección del cortafuego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Active o desactive el Cortafuego mediante el conmutador correspondiente.

Aviso

Apagar el cortafuego sólo debe hacerse como medida temporal, ya que expondría el equipo a conexiones no autorizadas. Vuelva a activar el cortafuego tan pronto como sea posible.

4.7.1. Administración de las reglas del cortafuegos

Reglas generales

Siempre que se transmiten datos por Internet, se utilizan determinados protocolos.

Las reglas generales le permiten configurar los protocolos sobre los que se permite el tráfico. De forma predeterminada, no se muestran las reglas generales al abrir el Cortafuego. Para modificar las reglas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Reglas**.
5. Marque la casilla de verificación **Mostrar reglas generales** en la esquina inferior izquierda de la ventana.

Se muestran las reglas por defecto. Para modificar la prioridad de una regla, haga clic en la flecha correspondiente de la columna **Permiso** y seleccione **Permitir** o **Denegar**.

DNS sobre UDP / TCP
Permitir o bloquear DNS sobre UDP y TCP.

Por defecto, este tipo de conexión está permitido.

Enviar emails
Permitir o denegar el envío de correos electrónicos a través de SMTP.

Por defecto, este tipo de conexión está permitido.

Navegación Web HTTP
Permitir o denegar la navegación Web HTTP.

Por defecto, este tipo de conexión está permitido.

ICMP / ICMPv6 entrante
Permitir o rechazar mensajes ICMP / ICMPv6.

Los mensajes ICMP son frecuentemente usados por los hackers para llevar a cabo ataques contra las redes de equipos. Por defecto, este tipo de conexión es rechazada.

Conexiones de escritorio remoto entrantes
Permitir o denegar el acceso de otros equipos a través de conexiones de Escritorio Remoto.

Por defecto, este tipo de conexión está permitido.

Tráfico HTTP / FTP del Explorador de Windows
Permitir o denegar el tráfico HTTP y FTP desde el Explorador de Windows.

Por defecto, este tipo de conexión es rechazada.

Reglas de aplicación

Para ver y administrar las reglas del cortafuego que controlan el acceso de las aplicaciones a los recursos de red y a Internet:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Reglas**.

Puede ver los programas (procesos) para cada regla del cortafuego que han sido creados en la tabla. Para ver las reglas creadas para una aplicación concreta, simplemente haga doble clic en ella.

Para cada regla se mostrará la siguiente información:

- **Nombre** - el nombre del proceso al que aplican las reglas.
- **Tipo de red**: el proceso y tipos de adaptadores de red a los que se aplica la regla. Las reglas se crean automáticamente para filtrar el tráfico de la red / Internet a través de cualquier adaptador. De forma predeterminada, las reglas se aplican a cualquier red. Puede crear reglas manualmente o editar reglas existentes y así filtrar el acceso a la red/Internet de una

aplicación en un adaptador de red específico (por ejemplo, un adaptador de red Wi-Fi).

- **Protocolo** - el protocolo IP sobre el que se aplica la regla. De forma predeterminada, las reglas se aplican a todos los protocolos.
- **Permiso** - indica si la aplicación tiene acceso o no a la red o a Internet bajo las circunstancias especificadas.

Para administrar las reglas, utilice los botones de encima de la tabla:

- **AÑADIR REGLA** - abre una ventana donde puede crear una nueva regla.
- **ELIMINAR REGLA** - elimina la regla seleccionada.
- **REINICIAR REGLAS** - abre una ventana donde puede optar por eliminar el conjunto de reglas actual y restaurar las predeterminadas.

Añadir / Editar reglas de aplicación

Para añadir o modificar una regla de aplicación, pulse el botón **AÑADIR REGLA** de encima de la tabla o haga clic en una regla actual. Aparecerá una nueva ventana. Siga estos pasos:

En la pestaña **Ajustes** puede aplicar las siguientes modificaciones:

- **Ruta del Programa.** Haga clic en **Explorar** y seleccione la aplicación a la que quiere aplicar la regla.
- **Tipo de red.** Seleccione el tipo de red al que se aplica la regla. Puede cambiar el tipo accediendo al menú desplegable **Tipo de red** y seleccionar uno de los tipos disponibles de la lista.

Tipo de red	Descripción
De confianza	Desactiva el Cortafuego en el respectivo adaptador.
Casa/Oficina	Permite todo el tráfico entre su equipo y los equipos de la red local.
Público	Se filtrará todo el tráfico.
Insegura	Bloquea por completo el tráfico de la red e Internet del adaptador de red correspondiente.

- **Permisos.** Seleccione uno de los permisos disponibles:

Permisos	Descripción
Permitir	Se permitirá el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.
Bloquear	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

En la pestaña **Avanzado** puede personalizar los siguientes ajustes:

- **Dirección local personalizada.** Indique la dirección IP local y el puerto a los que se aplicará la regla.
- **Dirección remota personalizada.** Indique la dirección IP remota y el puerto a los que aplicará la regla.
- **Dirección.** En el menú, seleccione la dirección del tráfico a la que se aplicará la regla.

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

- **Protocolo.** En el menú, seleccione el protocolo IP sobre el que desea aplicar la regla.
  - Si desea aplicar la regla a todos los protocolos, seleccione la casilla **Cualquiera**.
  - Si desea aplicar la regla para TCP, seleccione **TCP**.
  - Se desea aplicar la regla para UDP, seleccione **UDP**.
  - Si desea que la regla se aplique a un protocolo concreto, escriba el número asignado al protocolo que desea filtrar en el campo editable en blanco.

> **Nota**
>
> Los números de los protocolos IP están asignados por la Internet Assigned Numbers Authority (IANA). Puede encontrar una lista completa

de los números asignados a los protocolos IP en http://www.iana.org/assignments/protocol-numbers.

Administración de ajustes de conexión

Para cada conexión de red puede configurar zonas especiales de confianza o de no confianza.

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

Una zona de no confianza es un dispositivo que no desea que se comunique con su equipo.

Para ver y administrar las zonas de los adaptadores de red:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Adaptadores**.

Los adaptadores de red con conexiones activas y las zonas actuales, en su caso, se muestran en esta pestaña.

Para cada zona se mostrará la siguiente información:

- **Tipo de red** - el tipo de red al que se conecta el equipo.
- **Modo Oculto** - indica si quiere que otros ordenadores detecten a su equipo o no.

  Para configurar el modo silencioso, seleccione la opción deseada del menú desplegable correspondiente.

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

- **Genérico** - indica las reglas genéricas que son aplicadas a esta conexión.

  Si la dirección IP en un adaptador de red se cambia, Bitdefender modificará el tipo de red en consecuencia. Si quiere mantener el mismo tipo, seleccione **Sí** en el menú desplegable correspondiente.

Añadir/Modificar excepciones

Para añadir o modificar una excepción, haga clic en el enlace **Excepciones de red** de encima de la tabla. Aparecerá una nueva ventana mostrando los adaptadores disponibles conectados a la red. Siga estos pasos:

1. Seleccione la dirección IP del equipo que quiere añadir, o escriba una dirección o rango de direcciones en la caja de texto proporcionada.
2. Seleccione el permiso:
   - **Permitir** - para permitir todo el tráfico entre su equipo y el equipo seleccionado.
   - **Bloquear** - para bloquear todo el tráfico entre su equipo y el equipo seleccionado.
3. Haga clic en el botón + para añadir la excepción y cerrar la ventana.

   Si desea eliminar una dirección IP, haga clic en el botón correspondiente y cierre la ventana.

Configuración de opciones avanzadas

Para configurar los ajustes avanzados del cortafuego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Configuración**.

La siguiente característica puede activarse o desactivarse:

- **Bloquear análisis de puertos en la red** - detecta y bloquea los intentos de averiguar qué puertos están abiertos.

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

Configuración de la intensidad de la alerta

Bitdefender Total Security ha sido diseñado para ser lo más discreto posible. Bajo condiciones normales, no tiene que tomar decisiones sobre si permitir o rechazar conexiones o acciones que intenten realizar las aplicaciones que se ejecutan en su sistema.

Si quiere tener control total sobre la toma de decisiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la ventana **General**, active el **Modo paranoico** haciendo clic en el conmutador correspondiente.

> **Nota**
> Cuando el modo paranoico está activo, las características Autopilot y Perfiles se desactivan automáticamente.
> El **Modo Paranoico** se puede utilizar junto con el **Modo Batería**.

Mientras esté activo el modo paranoico, se le preguntará por la acción a aplicar cada vez que se produzca una de las siguientes situaciones:

- Una aplicación intenta conectarse a Internet.
- Una aplicación intenta ejecutar una acción considerada sospechosa por el Active Threat Control.

La alerta contiene información detallada sobre la aplicación y el comportamiento detectado. Seleccione si desea **Permitir** o **Rechazar** la acción a aplicar mediante el botón correspondiente.

4.8. Protección contra ransomware

El ransomware es un software malicioso que ataca a los sistemas vulnerables y los bloquea, con el fin de solicitar dinero al usuario a cambio de permitirle recuperar el control de su sistema. Este software malicioso actúa astutamente, mostrando mensajes falsos para que el usuario entre en pánico, instándole a efectuar el pago solicitado.

Dicha infección puede propagarse mediante spam, al descargar archivos adjuntos, o por visitar sitios Web infectados e instalar aplicaciones maliciosas sin que el usuario se percate de lo que está sucediendo en su sistema.

El ransomware puede presentar cualquiera de los siguientes comportamientos que impiden que el usuario acceda a su sistema:

- Cifrar archivos confidenciales y personales sin dar la posibilidad de descifrarlos hasta que la víctima pague un rescate.
- Bloquear la pantalla del equipo y mostrar un mensaje pidiendo dinero. En este caso, no se cifra ningún archivo y simplemente se fuerza al usuario a que efectúe el pago.
- Bloquear la ejecución de aplicaciones.

Gracias a la última tecnología, la Protección contra ransomware de Bitdefender garantiza la integridad del sistema mediante la protección contra daños de las áreas críticas del sistema sin afectar al mismo. No obstante, puede que también desee proteger sus archivos personales, como documentos, fotos, películas o los archivos que tiene almacenados en la nube.

Activación y desactivación de la Protección contra ransomware

Para desactivar el módulo de Protección contra ransomware:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.
4. Haga clic en el conmutador correspondiente para activar o desactivar la **Protección contra ransomware**.

Cada vez que una aplicación intente acceder a un archivo protegido, aparecerá una ventana emergente de Bitdefender. Puede permitir o denegar el acceso.

Proteger los archivos personales de los ataques de ransomware

Si desea poner a buen recaudo sus archivos personales:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.
4. Haga clic en el botón **AÑADIR**.
5. Acceda a la carpeta que desee proteger y, a continuación, haga clic en **Aceptar** para añadir la carpeta seleccionada al entorno de protección.

Por defecto, las carpetas Documentos, Imágenes, Documentos públicos e Imágenes públicas están protegidas contra ataques de malware.

> **Nota**
> Se pueden proteger carpetas personalizadas solo para los usuarios actuales. Los archivos del sistema y de aplicaciones no se pueden añadir a las excepciones.

Configuración de aplicaciones de confianza

Se desactiva la Protección contra ransomware para determinadas aplicaciones, pero solo se añadirán a la lista las de su confianza.

Para añadir aplicaciones de confianza a las exclusiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones de confianza**.
4. Haga clic en **Añadir** y, a continuación, escoja las aplicaciones que desee proteger.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada al entorno de protección.

Configuración de aplicaciones bloqueadas

Puede que las aplicaciones que intenten cambiar o borrar archivos protegidos se identifiquen como potencialmente poco fiables y se añadan a la lista de aplicaciones bloqueadas. Si se bloquease una aplicación y estuviese seguro de que su comportamiento es el adecuado, puede excluirla siguiendo estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones bloqueadas**.
4. Haga clic en **Permitir** y escoja la aplicación que considera segura.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada a la lista de confianza.

Protección en el arranque

Se sabe que muchas aplicaciones de malware se ponen en funcionamiento al arrancar el sistema, lo que puede dañar seriamente una máquina. La Protección en el arranque de Bitdefender analiza todas las áreas críticas del sistema antes de que se carguen todos los archivos, con un impacto nulo en el sistema. Al mismo tiempo, se proporciona protección para ciertos ataques que se basan en la pila o en la ejecución de heap code, inyecciones de código o enlaces dentro de ciertas bibliotecas dinámicas esenciales.

Para desactivar la protección en el arranque:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono ⚙ de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.
4. Haga clic en el conmutador correspondiente para activar o desactivar la **Protección en el arranque**.

4.9. Seguridad Safepay para las transacciones online

El PC se está convirtiendo rápidamente en la herramienta para compras y banca electrónica. Pagar facturas, transferir dinero, comprar prácticamente todo lo que pueda imaginar nunca ha sido más fácil y rápido.

Esto supone enviar información personal, de cuenta y datos de la tarjeta de crédito, contraseñas y otro tipo de información privada a través de Internet, en otras palabras, exactamente el tipo de información en la que los cibercriminales están interesados. Los hackers son implacables en sus esfuerzos para robar esta información, por lo que nunca se es demasiado cuidadoso a la hora de proteger las transacciones en línea.

Bitdefender Safepay™ es sobre todo un navegador protegido, un entorno sellado que está diseñado para mantener privadas y seguras sus operaciones de banca online, compras online y cualquier otro tipo de transacción online.

Para la mejor protección de la privacidad, se ha integrado el Gestor de contraseñas de Bitdefender en Bitdefender Safepay™, con el fin de proteger sus credenciales siempre que desee acceder a ubicaciones privadas online. Para más información, por favor vea *"Protección del Gestor de contraseñas para sus credenciales"* (p. 152).

Bitdefender Safepay™ ofrece las siguientes opciones:

- Bloquea el acceso a su escritorio y cualquier intento de tomar capturas de su pantalla.
- Protege sus contraseñas secretas mientras navega por Internet con el Gestor de contraseñas.
- Viene con un teclado virtual que, cuando se utiliza, hace imposible a los hackers leer sus pulsaciones en el teclado.
- Es completamente independiente de sus otros navegadores.
- Viene con una función de protección de punto de acceso para cuando su equipo esté conectado a redes Wi-Fi no seguras.

- Acepta marcadores y le permite navegar entre sus sitios favoritos de banca y compras.
- No está limitado a banca electrónica y compras por Internet. Puede abrirse cualquier sitio Web en Bitdefender Safepay™.

Utilizar Bitdefender Safepay™

Por omisión, Bitdefender detecta cuando navega hacia una página de un banco online o a una tienda online en cualquier navegador de su equipo y le pide que la lance en Bitdefender Safepay™.

Para acceder a la interfaz principal de Bitdefender Safepay™, utilice uno de los siguientes métodos:

- Desde la interfaz de Bitdefender:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el botón de acción **Safepay**.
- En Windows:
  - En **Windows 7**:
    1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
    2. Haga clic en **Bitdefender**.
    3. Haga clic en **Bitdefender Safepay™**.
  - En **Windows 8 y Windows 8.1**:

    Localice Bitdefender Safepay™ desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender Safepay" en la pantalla Inicio) y luego haga clic en el icono.
  - En **Windows 10**:

    Escriba "Bitdefender Safepay™" en el cuadro de búsqueda de la barra de tareas y haga clic en su icono.

Nota

Si el plugin Adobe Flash Player no está instalado o está obsoleto, se mostrará un mensaje de Bitdefender. Haga clic en el botón correspondiente para continuar

Una vez completado el proceso de instalación, tendrá que reabrir manualmente el navegador Bitdefender Safepay™ para continuar su trabajo.

Si está acostumbrado a los navegadores Web, no tendrá ningún problema utilizando Bitdefender Safepay™ - se parece y se comporta igual que cualquier navegador:

- introduzca las URLs a las que desea ir en la barra de direcciones.
- añada pestañas para visitar múltiples sitios Web en la ventana de Bitdefender Safepay™ haciendo clic en .
- navegue atrás y hacia delante y refresque las páginas usando respectivamente.
- acceda a los ajustes de Bitdefender Safepay™ haciendo clic en y seleccionando **Ajustes**.
- Proteja sus contraseña con el Gestor de contraseñas haciendo clic en .
- administre sus marcadores haciendo clic junto a la barra de dirección.
- abra el teclado virtual haciendo clic en .
- aumente o disminuya el tamaño del navegador pulsando simultáneamente **Ctrl** y las teclas **+/-** del teclado numérico.
- vea información sobre su producto Bitdefender haciendo clic en y eligiendo **Acerca de**.
- imprima la información importante haciendo clic .

Nota
Para cambiar entre el escritorio de Windows y el de Bitdefender Safepay™, pulse las teclas **Alt+Tab**, o haga clic en el botón **Minimizar**.

Configuración de ajustes

Haga clic en y seleccione **Ajustes** para configurar Bitdefender Safepay™:

- En los **Ajustes generales** puede configurar lo siguiente:

  Comportamiento de Bitdefender Safepay™
  Escoja qué es lo que sucederá cuando acceda a una tienda online o a un banco por Internet en su navegador Web habitual:
  - Abrir automáticamente los sitios Web en Safepay.

- Recomendarme usar Safepay.
- No recomendarme usar Safepay.

Lista de dominios

Elija cómo se comportará Bitdefender Safepay™ cuando visite sitios Web de dominios específicos en su navegador habitual añadiéndolos a la lista de dominios y seleccionando un comportamiento para cada uno:

- Abrir automáticamente en Bitdefender Safepay™.
- Hacer que Bitdefender le pregunte qué hacer cada vez.
- Nunca utilizar Bitdefender Safepay™ al visitar una página del dominio en un navegador habitual.

Bloqueo de ventanas emergentes

Puede decidir bloquear las ventanas emergentes haciendo clic en el conmutador.

También puede crear una lista de sitios Web en los que permitir las ventanas emergentes. La lista debería contener únicamente sitios web en los que confíe plenamente

Para añadir un sitio a la lista, escriba su dirección en el campo correspondiente y haga clic en **Añadir dominio**.

Para eliminar un sitio Web de la lista, seleccione la X correspondiente a la entrada deseada.

Activar la protección Hotspot

Activando esta característica, puede habilitar una capa adicional de protección cuando se conecta a redes Wi-Fi no seguras.

Acceda a "Protección Hotspot para redes no seguras" (p. 151) para obtener más información.

- En el área **Ajustes avanzados** hay disponibles las siguientes opciones:

Administrar plugins

Puede elegir si desea habilitar o deshabilitar determinados plugins en Bitdefender Safepay™.

Administrar certificados

Puede importar certificados desde su sistema a un almacén de certificados.

Seleccione **Importar certificados** y siga el asistente para utilizar los certificados en Bitdefender Safepay™

Iniciar automáticamente el Teclado virtual en los campos de contraseñas
Cuando seleccione un campo de contraseña, aparecerá automáticamente el teclado virtual.

Utilice el conmutador correspondiente para activar o desactivar la función.

Administración de marcadores

Si ha deshabilitado la detección automática para algunos o todos los sitios Web, o Bitdefender simplemente no detecta ciertas sitios Web, puede añadir marcadores a Bitdefender Safepay™ para poder abrir con facilidad sus sitios Web favoritos en el futuro.

Siga estos pasos para añadir una URL a los marcadores de Bitdefender Safepay™:

1. Haga clic en el icono junto a la barra de direcciones para abrir la página de marcadores.

   Nota
   La página de marcadores aparece abierta por omisión cuando inicia Bitdefender Safepay™.

2. Haga clic en el botón **+** para añadir un nuevo marcador.
3. Introduzca la URL y el título del marcador y haga clic en **Crear**. Marque la opción **Abrir automáticamente los sitios Web en Safepay** si desea que la página marcada se abra con Bitdefender Safepay™ cada vez que acceda a ella. La URL también se añade a la lista de dominios en la página Ajustes.

Protección Hotspot para redes no seguras

Cuando utiliza Bitdefender Safepay™ mientras está conectado a una red Wi-Fi no segura (por ejemplo, un punto de acceso público) la característica de protección en punto de acceso ofrece una capa extra de seguridad. Este servicio encripta la comunicación con Internet en conexiones no seguras, ayudándole a mantener su privacidad sin importar a qué tipo de red se encuentre conectado.

La protección Hotspot funciona solo si su equipo está conectado a una red no segura.

La conexión segura se iniciará y se le mostrará un mensaje en la ventana de Bitdefender Safepay™ cuando se establezca la conexión. El símbolo aparece delante de la URL en la barra de direcciones para ayudarle a identificar fácilmente las conexiones seguras.

Puede que tenga que confirmar la acción.

4.10. Protección del Gestor de contraseñas para sus credenciales

Usamos nuestros equipos para comprar online o pagar nuestras facturas, para conectarnos a plataformas de redes sociales o iniciar sesión con aplicaciones de mensajería instantánea.

¡Pero como todo el mundo sabe, no siempre es fácil recordar una contraseña!

Y si no tenemos cuidado mientras navegamos online, nuestra información privada, como nuestra dirección de correo, nuestro ID de mensajería instantánea o los datos de nuestra tarjeta de crédito pueden verse comprometidos.

Guardar sus contraseñas o sus datos personales en una hoja de papel o en el equipo puede ser peligroso porque pueden acceder a ellos personas que quieran robar y usar esa información. Y recordar todas las claves que haya establecido para sus cuentas online o para sus sitios Web favoritos no es una tarea fácil.

Por consiguiente, ¿hay alguna manera de asegurar que podamos encontrar nuestras contraseñas siempre que las necesitemos? ¿Y podamos descansar tranquilos sabiendo que nuestras contraseñas secretas están siempre a salvo?

El Gestor de contraseñas le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

Utilizando una única contraseña maestra para acceder a sus credenciales, el Gestor de contraseñas le facilita mantener sus contraseñas a salvo en un Wallet.

Para ofrecer la mejor protección para sus actividades online, el Gestor de contraseñas se integra con Bitdefender Safepay™ y proporciona una solución única para las distintas formas en las que puede comprometerse su información privada.

El Gestor de contraseñas protege la siguiente información privada:

- Información personal, tal como la dirección de e-mail o el número de teléfono
- Credenciales de inicio de sesión en sitios Web
- Información de cuentas bancarias o números de tarjetas de crédito
- Datos de acceso a cuentas de correo
- Contraseñas para aplicaciones
- Contraseñas para las redes Wi-Fi

Configuración del Gestor de contraseñas

Una vez finalizada la instalación y abierto el navegador, se le notificará a través de una ventana emergente que puede utilizar Wallet para conseguir una experiencia de navegación más sencilla.

El Wallet de Bitdefender es el lugar donde puede guardar sus datos personales.

Haga clic en **Explorar** para iniciar el asistente de configuración de Wallet. Siga el asistente para completar el proceso de configuración.

Pueden realizarse dos tareas durante este paso:

- Cree una nueva base de datos de Wallet para proteger sus contraseñas.

  Durante el proceso de instalación, se le pedirá que proteja Wallet con una contraseña maestra. La contraseña debería ser segura y contener al menos 7 caracteres.

  Para crear una contraseña segura utilice al menos un número o símbolo, y un carácter en mayúsculas. Una vez que haya establecido una contraseña, cualquiera que desee acceder a Wallet tendrá primero que proporcionar la contraseña.

  Después de establecer la contraseña maestra, se le brinda la posibilidad de sincronizar la información del Wallet en la nube, para que pueda utilizarlo en todos sus dispositivos.

  Al final del proceso de configuración, se activan los siguientes ajustes por omisión:

  - **Guardar las credenciales automáticamente en Wallet**.
  - **Pedir mi contraseña maestra cuando inicie sesión en mi equipo.**.

- **Autocompletar siempre las credenciales de inicio de sesión**.
- **Preguntar mis opciones de completado cuando visito una página con formularios**.

- Importe una base de datos existente si ya ha utilizado Wallet previamente en su sistema.

Exportar la base de datos de Wallet

Para exportar la base de datos de su Wallet:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Exportar Wallet**.
4. Siga los pasos para exportar la base de datos de Wallet a una ubicación en su sistema.

Nota
Para que el enlace **Exportar Wallet** esté disponible, tiene que estar abierto el Wallet.

Crear una nueva base de datos de Wallet

Para crear una nueva base de datos de Wallet:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Crear nuevo Wallet**.
4. En el área **Inicio de cero**, haga clic en **Crear nuevo**.
5. Introduzca la información requerida en los campos correspondientes.
   - Etiqueta de Wallet: escriba un nombre único para su base de datos de Wallet.
   - Contraseña maestra: introduzca una contraseña para su Wallet.
   - Repetir contraseña: vuelva a escribir la contraseña que estableció.

- Pista: escriba una pista para recordar la contraseña.

6. Haga clic en **Continuar**.
7. En este paso puede optar por almacenar su información en la nube. Si selecciona Sí, la información bancaria permanecerá almacenada localmente en su dispositivo. Elija la opción deseada y, a continuación, haga clic en **Continuar**.
8. Seleccione el navegador Web desde el que desea importar las credenciales.
9. Haga clic en **Finalizar**.

Sincronización de sus Wallets en la nube

Para activar o desactivar la sincronización de Wallets en la nube:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la base de datos de Wallet que desee en la sección **Mis Wallets** y, a continuación, haga clic en el botón **AJUSTES**.
5. Elija la opción que desee en la ventana que aparece y, a continuación, haga clic en **Guardar**.

Nota
Para que el botón **AJUSTES** esté disponible, el Wallet tiene que estar abierto.

Administrar sus credenciales de Wallet

Para administrar sus contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Abrir Wallet**.
4. Seleccione la base de datos de Wallet que desee en la pestaña **Wallets** y, a continuación, haga clic en el botón **ABRIR**.

5. Escriba la contraseña maestra y, a continuación, haga clic en **Aceptar**.

Aparecerá una nueva ventana. Seleccione la categoría deseada desde la parte superior de la ventana:

- Identidad
- Sitios Web
- Banca online
- Direcciones
- Aplicaciones
- Redes Wi-Fi

Añadir/Modificar las credenciales

- Para añadir una contraseña nueva, escoja arriba la categoría deseada, haga clic en **+ Añadir elemento**, inserte la información en los campos correspondientes y haga clic en el botón Guardar.
- Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**.
- Para eliminar una entrada, selecciónela, haga clic en el botón **Editar** y seleccione **Eliminar**.

Activar o desactivar la protección del Gestor de contraseñas

Para activar o desactivar la protección del Gestor de contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Utilice el conmutador correspondiente para activar o desactivar el Gestor de contraseñas.

Administración de los ajustes del Gestor de contraseñas

Para configurar en detalle la contraseña maestra:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **Ajustes de seguridad**.

Tiene las siguientes opciones a su disposición:

- **Pedir mi contraseña maestra cuando inicie sesión en mi PC** - se le pedirá que escriba su contraseña maestra cuando acceda al equipo.
- **Pedir mi contraseña maestra cuando abra mi navegador y apps** - se le pedirá que escriba su contraseña maestra cuando acceda a un navegador o a una aplicación.
- **Bloquear automáticamente Wallet cuando deje mi PC desatendido** - se le pedirá que escriba su contraseña maestra cuando vuelva a su equipo tras 15 minutos.

! **Importante**
Asegúrese de recordar su contraseña maestra o guardar registro de ella en un lugar seguro. Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para recibir ayuda.

Mejore su experiencia

Para seleccionar los navegadores o las aplicaciones donde quiera integrar el Gestor de contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **Plugins**.

   Marque una aplicación para usar el Gestor de contraseñas y mejorar su experiencia:

   - Internet Explorer

- Mozilla Firefox
- Google Chrome
- Safepay
- Skype

Configurar Autocompletar

La característica Autocompletar facilita conectar con sus sitios Web favoritos o iniciar sesión en sus cuentas online. La primera vez que introduzca sus credenciales de acceso e información personal en su navegador Web, se protegerán automáticamente en Wallet.

Para configurar las opciones de **Autocompletar**:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **Configuración de autocompletar**.
5. Configure de las opciones siguientes:
   - **Autocompletar credenciales de inicio de sesión**:
     - **Autocompletar credenciales de inicio de sesión siempre** - las credenciales se introducen automáticamente en el navegador.
     - **Permitirme elegir cuándo deseo autocompletar mis credenciales de inicio de sesión** - puede elegir cuándo rellenar automáticamente las credenciales en el navegador.
   - **Configurar cómo protege Wallet sus credenciales**:
     - **Guardar las credenciales automáticamente en Wallet** - las credenciales de inicio de sesión y otra información de identificación, como sus datos personales y de tarjetas de crédito, se guardan y actualizan automáticamente en Wallet.
     - **Preguntarme siempre** - se le preguntará cada vez que quiera añadir sus credenciales a Wallet.

- **No guardar, actualizaré la información manualmente** - las credenciales pueden añadirse únicamente de forma manual en Wallet.

- **Autocompletar formularios**:
  - **Preguntar mis opciones de completado cuando visito una página con formularios** - aparecerá una ventana emergente con las opciones de completado cada vez que Bitdefender detecte que desea realizar un pago online o un registro.

Administrar la información del Gestor de contraseñas desde su navegador

Puede administrar fácilmente la información del Gestor de contraseñas directamente desde su navegador, para que tenga a mano todos sus datos importantes. El complemento Wallet de Bitdefender es compatible con los siguientes navegadores: Google Chrome, Internet Explorer y Mozilla Firefox, y también va integrado en Safepay.

Para acceder a la extensión Wallet de Bitdefender, abra su navegador Web, permita que se instale el complemento y haga clic en el icono de la barra de herramientas.

La extensión Wallet de Bitdefender contiene las siguientes opciones:

- Abrir Wallet - abre Wallet.
- Bloquear Wallet - bloquea Wallet.
- Sitios Web - abre un submenú con todos los inicios de sesión en sitios Web almacenados en Wallet. Haga clic en **Añadir sitio Web** para añadir nuevos sitios Web a la lista.
- Rellenar formularios - abre un submenú que contiene la información añadida por usted para una categoría determinada. Desde aquí puede añadir nuevos datos a su Wallet.
- Generador de contraseñas: le permite generar contraseñas aleatorias que puede utilizar para cuentas nuevas o existentes. Haga clic en **Mostrar ajustes avanzados** para personalizar la complejidad de la contraseña.
- Ajustes: abre la ventana de ajustes del Gestor de contraseñas.
- Informar de un problema: informe de cualquier problema que encuentre con el Gestor de contraseñas de Bitdefender.

4.11. Asesor parental

El Asesor parental le permite controlar el acceso a Internet y a aplicaciones concretas para cada dispositivo en el que esté instalada esta característica. Una vez que haya configurado el Asesor parental, puede averiguar fácilmente lo que está haciendo su hijo en los dispositivos que utiliza y dónde ha estado en las últimas 24 horas. Además, para ayudarle a conocer mejor lo que está haciendo su hijo, la app le brinda información estadística sobre sus actividades e intereses.

Todo lo que necesita es un ordenador con acceso a Internet y un navegador web.

Puede configurar el Asesor parental para bloquear:

- páginas web con contenido inadecuado.
- aplicaciones como juegos, chat, aplicaciones de intercambio de archivos u otros.
- determinados contactos a los que no se les permite comunicarse por teléfono con su hijo.

Compruebe las actividades de sus hijos y cambie los ajustes del Asesor parental usando cuenta Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet.

Acceso al Asesor parental - MIS HIJOS

Una vez que acceda a la sección del Asesor parental, tendrá a su disposición la ventana **MIS HIJOS**. Aquí puede ver y modificar todos los perfiles que haya creado para sus hijos. Los perfiles se muestran como tarjetas de perfil, lo que le permite administrarlos rápidamente y comprobar su estado de un vistazo.

En cuanto cree un perfil, podrá comenzar a personalizar los ajustes más detallados para supervisar y controlar el acceso de sus hijos a Internet y a aplicaciones concretas.

Puede acceder a los ajustes del Asesor parental desde su Bitdefender Central en cualquier equipo o dispositivo móvil conectado a Internet.

Acceda a su cuenta Bitdefender.

- En cualquier dispositivo con acceso a Internet:
  1. Acceda a Bitdefender Central.

2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Seleccione el módulo **Asesor parental**.
4. En la ventana **MIS HIJOS** que aparece puede administrar y configurar los perfiles del Asesor parental para cada dispositivo.

- Desde la interfaz de su Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **Asesor parental**, seleccione **Configurar**.

   Se le redirigirá a la página Web de cuenta Bitdefender. Asegúrese de que ha iniciado sesión con sus credenciales.
4. Seleccione el módulo **Asesor parental**.
5. En la ventana **MIS HIJOS** que aparece puede administrar y configurar los perfiles del Asesor parental para cada dispositivo.

> **Nota**
> Asegúrese de haber iniciado sesión en el equipo con cuenta de administrador. Solo pueden acceder y configurar el Asesor parental los usuarios con derechos administrativos en el sistema (administradores del sistema).

Adición del perfil de su hijo

Para empezar a supervisar las actividades de su hijo, tiene que configurar un perfil e instalar el agente del Asesor parental de Bitdefender en los dispositivos que éste utiliza.

Para añadir el perfil de su hijo al Asesor parental:

1. Acceda al panel del Asesor parental desde Bitdefender Central.
2. Haga clic en **AÑADIR PERFIL** en el lado derecho de la ventana **MIS HIJOS**.
3. Indique la información correspondiente en los campos, como por ejemplo: nombre, sexo y fecha de nacimiento y, a continuación, haga clic en **CONTINUAR**.

Basándose en los estándares de desarrollo de los niños, al establecer la fecha de nacimiento de su hijo se cargan automáticamente unas especificaciones que se consideran apropiadas para su edad.

4. Si el dispositivo de su hijo ya tiene instalado Bitdefender Total Security, seleccione su dispositivo en la lista y, a continuación, haga clic en **CONTINUAR**.

   Si el dispositivo de su hijo no tiene un producto Bitdefender con la función de Asesor parental incluida, haga clic en **Añadir un nuevo dispositivo**. Seleccione el sistema operativo de su dispositivo y haga clic en **CONTINUAR**.

   Escriba la dirección de correo electrónico a la que debemos enviar el enlace de descarga para la instalación de la aplicación del Asesor parental de Bitdefender.

   En los dispositivos basados en Windows, debe descargarse e instalarse el Bitdefender Total Security que ha incluido en su suscripción. En los dispositivos Android, debe descargarse e instalarse el agente del Asesor parental de Bitdefender.

Asignación del mismo perfil a varios dispositivos

Puede asignar el mismo perfil a varios dispositivos pertenecientes a un mismo niño, con el fin de aplicar las mismas restricciones.

Para asignar un perfil a varios dispositivos:

1. Acceda a Bitdefender Central.
2. Seleccione el módulo Asesor parental.
3. Haga clic en el icono ⋮ de la tarjeta del perfil deseado y, a continuación, seleccione **Editar**.
4. Haga clic en el signo + en cada uno de los dispositivos disponibles que desee asignar al perfil.

   Si el dispositivo de su hijo no tiene un producto Bitdefender con la función de Asesor parental incluida, haga clic en **Añadir un nuevo dispositivo**. Seleccione el sistema operativo de su dispositivo y haga clic en **CONTINUAR**.

   Escriba la dirección de correo electrónico a la que debemos enviar el enlace de descarga para la instalación de la aplicación del Asesor parental

de Bitdefender. Compruebe el correo electrónico y haga clic en el enlace proporcionado para instalar el agente.

Tras finalizar el proceso de instalación en el nuevo dispositivo, selecciónelo en la lista para aplicar el perfil.

5. Seleccionar **GUARDAR**.

Vincular el Asesor parental a Bitdefender Central

Para supervisar la actividad online de su hijo en Android, debe vincular el dispositivo de éste con su cuenta Bitdefender iniciando sesión en la cuenta desde la app.

Para vincular el dispositivo a cuenta Bitdefender:

1. Seleccione el botón de **Google Play** que aparece en el mensaje de correo electrónico enviado por nuestro servidor y, a continuación, instale la app.

   Si no escogió en cuenta Bitdefender enviar un enlace de descarga a la dirección de correo electrónico de su hijo, acceda a Google Play y busque la app Asesor parental de Bitdefender.

2. Abra la app del Asesor parental.
3. Lea el **Acuerdo de licencia de usuario final** y, a continuación, toque **CONTINUAR**.
4. Inicie sesión en su cuenta Bitdefender existente.

   Si no posee una cuenta, elija crear una nueva mediante la opción correspondiente.

5. Active los derechos de administrador de dispositivos para la app tocando **ACTIVAR**.

   Esto evitará que su hijo desinstale el agente del Asesor parental.

6. Toque **Activar acceso a la utilización** y seleccione la casilla de verificación correspondiente.

Monitorización de la actividad de su hijo

Bitdefender le ayuda a supervisar lo que hacen sus hijos online.

De esta manera, siempre puede saber exactamente qué sitios Web ha visitado, qué aplicaciones ha usado o qué actividades han sido bloqueadas por el Asesor parental.

Dependiendo de los ajustes que realice, los informes pueden contener información detallada para cada evento, como por ejemplo:

- El estado del evento.
- La gravedad de la notificación.
- El nombre del dispositivo.
- La fecha y hora en que ocurrió el evento.

Para monitorizar el tráfico de Internet, las aplicaciones que se ha accedido o la actividad en Facebook de su hijo:

1. Acceda al panel del Asesor parental desde Bitdefender Central.
2. Seleccione la tarjeta de dispositivo deseada.

   En la ventana de **Panel de Control** puede ver la información que le interesa.

Configurar los Ajustes generales

Por defecto, cuando el Asesor parental está activado se registran las actividades de sus hijos.

Para recibir notificaciones por correo electrónico:

1. Acceda al panel del Asesor parental desde Bitdefender Central.
2. Haga clic en el icono de la esquina superior derecha.
3. Active la opción correspondiente para recibir informes de actividad.
4. Introduzca la dirección e-mail a la que desea que se envíen las notificaciones.
5. Ajuste la frecuencia seleccionando: diario, semanal o mensual.
6. Recibir notificaciones por correo para lo siguiente:
   - Páginas Web bloqueadas
   - App bloqueadas
   - Áreas restringidas
   - SMS de un contacto bloqueado
   - Llamada recibida de un número de teléfono bloqueado
   - Desinstalación de la app de Facebook del Asesor parental

7. Haga clic en **GUARDAR**.

Edición de un perfil

Para modificar un perfil existente:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Asesor parental**.
3. Haga clic en el icono ⋮ de la tarjeta del perfil deseado y, a continuación, seleccione **Editar**.
4. Tras personalizar los ajustes deseados, seleccione **GUARDAR**.

Eliminación de un perfil

Para eliminar un perfil existente:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Asesor parental**.
3. Haga clic en el icono ⋮ de la tarjeta del perfil deseado y, a continuación, seleccione **Eliminar**.

Configuración de perfiles del Asesor parental

Para empezar a supervisar a su hijo es preciso asignar un perfil al dispositivo en el que se ha instalado el agente del Asesor parental de Bitdefender.

Después de añadir un perfil para su hijo, puede personalizar los ajustes más detallados para supervisar y controlar el acceso a Internet y a aplicaciones concretas.

Para empezar a configurar un perfil, seleccione la tarjeta del perfil deseado en la ventana **MIS HIJOS**.

Haga clic en una pestaña para configurar la característica correspondiente del Asesor parental para el dispositivo:

- Panel de Control - muestra todas las actividades, intereses, lugares y comunicaciones con los amigos desde el día en curso.
- Actividades - le permite bloquear el acceso a ciertas aplicaciones, como juegos, software de mensajería, películas, etc.

- Intereses - le permite filtrar la navegación Web.
- Amigos - aquí puede especificar qué contactos de la lista de su hijo tienen permiso para hablar con él por teléfono.
- Lugares - aquí puede establecer los lugares que son seguros o no para su hijo.
- Social - le permite bloquear el acceso a las redes sociales.

Panel de Control

La ventana de Panel de Control le proporciona información detallada sobre las actividades de sus hijos durante las últimas 24 horas, dentro y fuera de casa.

Dependiendo de la actividad, la ventana del panel de control puede incluir información acerca de lo siguiente:

- **Lugares** - aquí puede ver los lugares donde estuvo su hijo durante el día.
- **Intereses** - aquí puede ver información sobre qué categorías de sitios Web visita su hijo. Haga clic en el enlace **Revisar contenidos inapropiados** para permitir o denegar el acceso a determinados intereses.
- **Relaciones sociales** - aquí puede ver los contactos que se han comunicado con su hijo. Haga clic en el enlace **Amigos** para seleccionar los contactos con los que su hijo puede comunicarse o no.
- **Aplicaciones** - aquí puede ver las aplicaciones que utilizó su hijo. Haga clic en el enlace **Revisar las restricciones de apps** para bloquear o permitir el acceso a determinadas aplicaciones.
- **Actividad de todo el día** - aquí puede ver el tiempo invertido en Internet de todos los dispositivos asignados a su hijo, y la ubicación donde se encontraba activo. La información recogida pertenece al día en curso. Haga clic en el enlace **Establecer tiempo de sueño** para indicar las horas durante las que el seguimiento de actividades pasará automáticamente al modo de espera.

Nota

Para obtener información detallada, haga clic en la opción deseada del lado derecho de cada sección.

Actividades

La ventana de actividades le ayuda a bloquear la ejecución de aplicaciones. Se pueden bloquear juegos, medios de comunicación y software de mensajería, así como otras categorías de software.

El módulo se puede activar o desactivar mediante el conmutador correspondiente.

Para configurar el Control de Aplicaciones para una cuenta de usuario específica:

1. Se mostrará una lista con tarjetas. Las tarjetas representan las apps que usa su hijo.
2. Seleccione la tarjeta con la app que desea que su hijo deje de usar.

   El símbolo de marca de verificación que aparece indica que su hijo no podrá utilizar la app.

Intereses

La ventana de intereses le ayuda a bloquear los sitios Web con contenidos inapropiados. Se pueden bloquear sitios Web de vídeos, juegos, medios de comunicación y software de mensajería, así como otras categorías de contenidos negativos.

El módulo se puede activar o desactivar mediante el conmutador correspondiente.

Dependiendo de la edad establecida para su hijo, la lista de intereses viene por defecto con una serie de categorías activadas. Para permitir o denegar el acceso a una determinada categoría, haga clic en ella.

El símbolo de marca de verificación que aparece indica que su hijo no podrá acceder a los contenidos relacionados con una determinada categoría.

Permitir o bloquear un sitio Web

Para permitir o restringir el acceso a determinadas páginas Web, hay que añadirlas a la lista de exclusiones de la siguiente manera:

1. Haga clic en el botón **ADMINISTRAR**.
2. Escriba la página Web que desea permitir o bloquear en el campo correspondiente.

3. Seleccione **Permitir** o **Bloquear**.
4. Haga clic en **Finalizar** para guardar los cambios.

Amigos

La ventana Amigos le brinda la posibilidad de especificar qué amigos de la lista de su hijo tienen o no permiso para hablar con él por teléfono.

Para restringir un número de teléfono concreto de un amigo, primero deberá añadir el número de teléfono de su hijo a su perfil:

1. Seleccione la pestaña del **Asesor parental** en Bitdefender Central.
2. Haga clic en el icono ⋮ de la tarjeta del perfil deseado y, a continuación, seleccione **Editar**.
3. Escriba el número de teléfono de su hijo en el campo correspondiente y, a continuación, haga clic en **GUARDAR**.
4. Seleccione el perfil del hijo para el que desea establecer restricciones.
5. Seleccione la pestaña **Amigos**.

   Se mostrará una lista con tarjetas. Las tarjetas corresponden a los contactos del teléfono de su hijo.
6. Seleccione la tarjeta con el número de teléfono que desee bloquear.

   El símbolo de marca de verificación que aparece indica que el número de teléfono seleccionado no podrá ponerse en contacto con su hijo.

Para bloquear los números de teléfono desconocidos, active el conmutador **Bloquear la comunicación con números no identificados**.

Lugares

Ver la ubicación actual del dispositivo en Google Maps. La ubicación se actualiza cada cinco segundos, por lo que puede seguirle la pista si está en movimiento.

La precisión de la ubicación depende de cómo pueda determinarla Bitdefender:

- Si está activado el GPS en el dispositivo, su ubicación puede señalarse con un par de metros de margen siempre que se encuentre en el alcance de los satélites GPS (es decir, no dentro de un edificio).

- Si el dispositivo está en interior, su localización puede determinarse con un margen de decenas de metros si la conexión Wi-Fi está activada y hay redes inalámbricas disponibles a su alcance.
- De lo contrario, la ubicación se determinará utilizando únicamente información de la red móvil, que ofrece una precisión de varios cientos de metros.

Configuración de la ubicación

Para asegurarse de que su hijo va a ciertos lugares, puede crear una lista de lugares seguros y peligrosos.

Para configurar una ubicación:

1. Haga clic en **Dispositivos** en el marco que tiene en la ventana **Lugares**.
2. Haga clic en **ESCOGER DISPOSITIVOS** y, a continuación, seleccione el dispositivo que desea configurar.
3. En la ventana **Zonas**, haga clic en el botón **AÑADIR ZONA**.
4. Elija el tipo de lugar, **SEGURO** o **RESTRINGIDO**.
5. Escriba un nombre válido para la zona a la que su hijo tiene permiso para ir o no.
6. Establezca el rango que debe aplicarse para la supervisión en la barra **Radio**.
7. Haga clic en **AÑADIR ZONA** para guardar sus ajustes.

Social

El Asesor parental supervisa la cuenta de Facebook de su hijo y le informa de las principales actividades que éste lleva a cabo.

Estas actividades online se comprueban y se le avisa si se demuestra que son una amenaza para la privacidad de su hijo.

Los elementos monitorizados de la cuenta online incluyen:

- Información de cuenta
- Páginas de Me gusta
- fotos subidas

Para configurar la protección de Facebook para una cuenta de usuario determinada, escriba la dirección de correo electrónico de la cuenta de su hijo que supervisa y, a continuación, haga clic en **ENVIAR**.

Informe a su hijo de sus intenciones y pídale que haga clic en el botón **PROTEGER CUENTA** que se le ha enviado a su correo electrónico.

Para acceder a la cuenta de Facebook supervisada, haga clic en el enlace **Ver en Facebook**.

Para detener la monitorización de la cuenta de Facebook, utilice el botón **DESVINCULAR CUENTA** de la parte superior.

Para que se le avise mediante correo electrónico si su hijo elimina la app Asesor parental de su dispositivo, marque la casilla de verificación correspondiente.

4.12. Antirrobo de Dispositivos

El robo de portátiles es un gran problema que afecta a particulares y empresas por igual. Más que perder el hardware en sí, la información que se pierde con él puede causar daños significativos, tanto financieros como emocionales.

Aún sólo unas pocas personas siguen los pasos adecuados para proteger su importante información personal, financiera y empresarial en caso de robo o pérdida.

Antirrobo de Bitdefender le ayuda a estar mejor preparado para un problema como este, permitiéndole localizar o bloquear remotamente su portátil e incluso borrar toda la información que haya él si tuviera que desprenderse de su portátil contra su voluntad.

Para utilizar las características de Anti-Theft, se deben cumplir los siguientes requisitos:

- Los comandos solo pueden enviarse desde la cuenta de Bitdefender.
- El portátil debe estar conectado a Internet para recibir los comandos.

Las características de Anti-Theft funcionan de la siguiente manera:

Localizar

Vea la ubicación de su dispositivo en Google Maps.

La precisión de la ubicación depende de cómo Bitdefender sea capaz de determinarla. La ubicación se determina con una precisión de decenas

de metros si el Wi-Fi está habilitado en su portátil y hay redes inalámbricas a su alcance.

Si el portátil está conectado a una red de cable LAN sin un punto Wi-Fi disponible, la ubicación se determinará basándose en la dirección IP, que es considerablemente menos precisa.

Alerta
Envíe una alerta remota al dispositivo.

Esta característica solo está disponible en dispositivos móviles.

Bloquear
Bloquee su portátil y establezca un PIN de cuatro dígitos para desbloquearlo. Cuando envía el comando **Bloquear**, se reinicia el sistema y solo es posible volver a iniciar sesión en Windows tras introducir el PIN que ha establecido.

Si desea que Bitdefender tome fotos de la persona que intenta acceder a su portátil, marque la casilla de verificación correspondiente. Las instantáneas se realizan mediante la cámara frontal y se muestran junto a su fecha y hora en el panel de control de Antirrobo. Solo se guardarán las dos últimas fotos.

Esta acción solo está disponible en portátiles que posean una cámara frontal.

Borrar
Elimine toda la información de su sistema. Cuando envía el comando **Borrar**, se reinicia el portátil y se borra la información de todas las particiones del disco duro.

Mostrar IP
Muestra la última dirección IP del dispositivo seleccionado. Haga clic en **MOSTRAR IP** para que se vea.

Anti-Theft se activa después de la instalación y puede accederse a él exclusivamente a través de su cuenta en Bitdefender desde cualquier dispositivo conectado a Internet, en cualquier parte.

Usar las características Antirrobo

Para acceder a las características Antirrobo, haga uso de una de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Antirrobo**.
3. En la ventana de Bitdefender Central que se abre, haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.

- En cualquier dispositivo con acceso a Internet:

1. Abra un navegador Web y acceda a: https://central.bitdefender.com.
2. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
3. Seleccione el panel **Mis dispositivos**.
4. Haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.
5. Seleccione la característica que desea usar:

   Mostrar IP - Muestra la última dirección IP de su dispositivo.
   Localizar - muestra la ubicación de su dispositivo en Google Maps.

   Alerta: envía una alerta al dispositivo.

   Bloquear - Bloquea su portátil y establece un código PIN para desbloquearlo.

   Borrar - Borra todos los datos de su portátil.

   Importante
   Después de borrar un dispositivo, todas las características de Anti-Theft dejan de funcionar.

4.13. USB Immunizer

La opción de Autorun integrada en el sistema operativo Windows es una herramienta muy útil que permite a los equipos ejecutar automáticamente un archivo de un medio conectado a él. Por ejemplo, las instalaciones de software pueden comenzar automáticamente cuando se inserta un CD en la unidad óptica.

Desgraciadamente, esta opción puede también utilizarla el malware para ejecutarse automáticamente e infiltrarse en su equipo desde un medio

reescribible como una unidad flash USB y tarjetas conectadas mediante lectores de tarjetas. En los últimos años se han producido numerosos ataques basados en la autoejecución.

Con el inmunizador USB puede evitar que ninguna unidad flash formateada con NTFS, FAT32 o FAT vuelva a ejecutar malware nunca más. Una vez que el dispositivo USB está inmunizado, el malware no puede volver a configurarlo para ejecutar cierta aplicación cuando el dispositivo se conecte a un equipo con Windows.

Para inmunizar un dispositivo USB:

1. Conecte la unidad flash a su equipo.
2. Examine su equipo para localizar el dispositivo de almacenamiento extraíble y haga clic con el botón derecho en su icono.
3. En el menú contextual, escoja **Bitdefender** y seleccione **Inmunizar esta unidad**.

> **Nota**
> Si la unidad ya se inmunizó, aparecerá el mensaje **El dispositivo USB está protegido contra malware de ejecución automática** en vez de la opción Inmunizar.

Para evitar que su equipo ejecute malware desde dispositivos USB no inmunizados, desactive la opción de autoarranque del dispositivo. Para más información, por favor vea "Usar el control automático de la vulnerabilidad" (p. 130).

5. OPTIMIZACIÓN DEL SISTEMA

5.1. Herramientas

Bitdefender incluye una sección de Herramientas que le ayuda a mantener la integridad de su sistema. Las herramientas de mantenimiento que se ofrecen son muy importantes para mejorar el rendimiento de su sistema y administrar eficientemente el espacio de los discos duros.

Bitdefender incluye las siguientes opciones de Optimización de PC:

- Optimizador en un clic analiza y mejora la velocidad de su sistema ejecutando múltiples tareas con solo hacer clic en un botón.
- El Optimizador de inicio reduce el tiempo de inicio del sistema al evitar la carga de las aplicaciones innecesarias cuando arranca el equipo.
- Limpieza de disco identifica las carpetas y archivos más grandes que no se hayan utilizado desde hace mucho tiempo.

Optimizar la velocidad de su sistema con un solo clic

Problemas como los fallos de disco duro, archivos inútiles en el registro y el historial del navegador, pueden ralentizar el trabajo de su equipo, hasta el punto de resultarle molesto. Todo esto se puede solucionar ahora con solo hacer clic en un botón.

El Optimizador en un clic le permite identificar y eliminar archivos inútiles, mediante la ejecución de múltiples tareas de limpieza simultáneas.

Para iniciar el proceso del Optimizador en un clic:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Optimizador en un clic**.
   a. **Analizando**

      Espere a que Bitdefender termine la búsqueda de problemas en el sistema.

      - Limpieza de disco - Identifica las carpetas y archivos grandes que ya no utilice.

- Limpieza del registro - identifica entradas obsoletas o no válidas en el registro de Windows.
- Limpieza de datos privados - identifica los archivos temporales de Internet y cookies, caché del navegador e historial.

Se muestra el número de problemas encontrados. Haga clic en el enlace **Ver detalles** para revisarlos antes de continuar con el proceso de limpieza. Haga clic en **OPTIMIZAR** para continuar.

b. **Optimización**

Espere a que Bitdefender termine de optimizar su sistema.

c. **Incidencias**

Aquí es donde puede ver el resultado de la operación.

Si desea información completa sobre el proceso de optimización, haga clic en el botón **VER INFORME DETALLADO**.

Optimización del tiempo de arranque de su PC

La prolongación del tiempo de arranque del sistema es un problema real debido a que hay aplicaciones configuradas para ejecutarse sin que sean necesarias. Esperar varios minutos a que arranque su sistema puede costarle un tiempo y productividad valiosos.

La ventana del Optimizador de inicio muestra qué aplicaciones se ejecutan durante el inicio del sistema y le permite administrar su comportamiento en este punto.

Para ejecutar el proceso del Optimizador de inicio:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Optimizador de inicio**.

   a. **Seleccione las aplicaciones**

   Puede ver una lista de las aplicaciones que se ejecutan al arrancar el sistema. Seleccione las que desea bloquear o retrasar en el inicio.

   b. **Elección de la comunidad**

   Vea lo que otros usuarios de Bitdefender han decidido hacer con la aplicación que ha seleccionado.

c. **Hora de arranque del sistema**

Fíjese en el control deslizante de la parte superior de la ventana para ver el tiempo de ejecución en el arranque requerido tanto por su sistema como por las aplicaciones seleccionadas.

Es necesario reiniciar el sistema para poder recopilar la información sobre el tiempo de arranque del sistema y de las aplicaciones.

d. **Estado de arranque**

- **Activar.** Seleccione esta opción cuando desee que una aplicación empiece a ejecutarse en el arranque del sistema. Esta opción está activada por omisión.
- **Posponer.** Seleccione esta opción para posponer la ejecución de un programa en el arranque del sistema. Esto significa que las aplicaciones seleccionadas se ejecutarán con un retraso de cinco minutos después de que el usuario inicie sesión en el sistema. La funcionalidad **Posponer** está predefinida y no la puede configurar el usuario.
- **Desactivar.** Seleccione esta opción para desactivar un programa que se ejecute en el arranque del sistema.

e. **Resultados**

Se muestra información como el tiempo estimado de arranque del sistema después de posponer o desactivar los programas.

Puede que sea necesario reiniciar el sistema para poder ver toda esta información.

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

Nota
En caso de que su suscripción haya caducado o decida desinstalar Bitdefender, los programas cuyo arranque decidiera posponer en el inicio se restaurarán a sus valores de arranque por defecto.

Optimizar su disco

Las carpetas y archivos innecesarios que consumen espacio en su disco pueden conducir a la ralentización del sistema. Por lo tanto, es recomendable que realice limpiezas periódicamente para mejorar la velocidad de su sistema.

La Limpieza de disco de Bitdefender le ayuda a liberar espacio en disco mediante la identificación de las carpetas y archivos grandes que ya no utilice.

Para empezar a limpiar su sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Limpieza de disco**.
3. Aparecerá una ventana que muestra información acerca de lo que puede hacer Limpieza de disco para que su sistema recupere espacio para nuevos datos. Haga clic en **CONTINUAR**.

   a. **Dispositivos y unidades**

      Puede ver una lista de los discos disponibles. Además de los discos de Windows, se analizan y se muestran en la lista los discos duros externos y los dispositivos USB. Haga clic en **VER** para tener acceso a las carpetas pertenecientes a la ubicación seleccionada. Haga clic en **ANALIZAR** en el apartado del disco que desee limpiar.

   b. **Analizar unidad**

      Se analiza la unidad seleccionada. Espere a que Bitdefender termine la búsqueda de carpetas y archivos grandes.

   c. **Incidencias**

      Aquí es donde puede ver los resultados de la operación divididos en carpetas. En la parte izquierda de la ventana, se puede apreciar un gráfico circular que muestra la cantidad de espacio de disco utilizado. Mueva el ratón por encima para ver el nombre de sus archivos y cuánto espacio ocupan.

      Para navegar por las carpetas de esa ubicación del sistema, selecciónelas a la derecha de la ventana. Para ver el contenido de una carpeta en una ventana independiente, seleccione **Mostrar en el Explorador de archivos**.

      Arrastre los archivos que desee eliminar a la parte inferior de la ventana. Haga clic en **VER** si desea revisar los archivos que ha elegido borrar. Haga clic en **BORRAR PERMANENTEMENTE** para comenzar el proceso de borrado.

      Confirme su elección.

5.2. Perfiles

Las actividades de trabajo diarias, ver películas o utilizar juegos pueden provocar que el sistema se ralentice, especialmente si se están ejecutando de manera simultánea con los procesos de actualización de Windows y las tareas de mantenimiento. Con Bitdefender, ahora puede elegir y aplicar su perfil preferido, lo que lleva a cabo los ajustes del sistema adecuados para aumentar el rendimiento de las aplicaciones específicas instaladas.

Bitdefender ofrece los siguientes perfiles:

- Perfil de Trabajo
- Perfil de Películas
- Perfil de Juego
- Perfil de redes Wi-Fi públicas
- Perfil del modo Batería

Si decide no utilizar los **Perfiles**, se activa un perfil por defecto denominado **Estándar** que no aporta optimización a su sistema.

Según su actividad, se aplican los siguientes ajustes del producto cuando se activa el perfil de trabajo, juego o ver películas:

- Todas las alertas y ventanas emergentes de Bitdefender quedan desactivadas.
- Se pospone la actualización automática.
- Se posponen los análisis programados.
- Se deshabilita el Asesor de búsquedas.
- Las Ofertas especiales y notificaciones del producto están desactivadas.

Según su actividad, se aplican los siguientes ajustes del sistema cuando se activa el perfil de trabajo, juego o ver películas:

- Se posponen las actualizaciones automáticas de Windows.
- Se deshabilitan las ventanas emergentes y alertas de Windows.
- Se suspenden los programas innecesarios en segundo plano.
- Se ajustan los efectos visuales para un mejor rendimiento.
- Se posponen las tareas de mantenimiento.

- Se ajusta la configuración del plan de energía.

Al trabajar bajo el perfil de redes Wi-Fi públicas, Bitdefender Total Security se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Active Threat Control
- El cortafuego de Bitdefender está activado y se aplican los siguientes ajustes a su adaptador inalámbrico:
  - Modo oculto - ACTIVADO
  - Genérico - DESACTIVADO
  - Tipo de red - Pública
- Se activan los siguientes ajustes de la Protección Web:
  - Analizar SSL
  - Protección contra fraude
  - Protección contra phishing

Perfil de Trabajo

La ejecución de varias tareas en el trabajo, como el envío de mensajes de correo electrónico, mantener una videoconferencia con sus compañeros o trabajar con aplicaciones de diseño puede afectar al rendimiento del sistema. El Perfil de trabajo se ha diseñado para ayudarle a mejorar su eficiencia en el trabajo, desactivando algunos de sus servicios en segundo plano y tareas de mantenimiento.

Configuración del Perfil de trabajo

Para configurar las acciones a llevar a cabo en el Perfil de trabajo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.

5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en aplicaciones de trabajo
   - Optimizar los ajustes del producto para el perfil de Trabajo
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir aplicaciones manualmente a la lista del Perfil de trabajo

Si Bitdefender no entra automáticamente en el Perfil de trabajo cuando ejecute cierta aplicación de trabajo, puede añadirla manualmente a la **Lista de aplicaciones**.

Para añadir aplicaciones manualmente a la lista de aplicaciones en el Perfil de trabajo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
5. En la ventana **PERFIL DE TRABAJO**, haga clic en el enlace **Lista de aplicaciones**.
6. Haga clic en **Añadir** para añadir una nueva aplicación a la **Lista de aplicaciones**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

Perfil de Películas

Mostrar vídeo de alta calidad, como por ejemplo películas de alta definición, requiere unos recursos del sistema significativos. El Perfil de películas ajusta

la configuración del sistema y del producto para que pueda disfrutar de una experiencia cinematográfica óptima y sin interrupciones.

Configuración del Perfil de películas

Para configurar las acciones a llevar a cabo en el Perfil de películas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en reproductores de vídeo
   - Optimizar los ajustes del producto para el perfil de Películas
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para películas
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir reproductores de vídeo manualmente a la lista del Perfil de películas

Si Bitdefender no entra automáticamente en el Perfil de películas cuando ejecute cierta aplicación de reproducción de vídeo, puede añadirla manualmente a la **Lista de reproductores**.

Para añadir reproductores de vídeo manualmente a la lista de reproductores en el Perfil de películas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.

4. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
5. En la ventana **PERFIL DE PELÍCULAS**, haga clic en el enlace **Lista de reproductores**.
6. Haga clic en **Añadir** para añadir una nueva aplicación a la **Lista de reproductores**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

Perfil de Juego

Disfrutar de una experiencia de juego ininterrumpido supone reducir la carga del sistema y disminuir cualquier posible retraso. Recurriendo a la heurística de comportamientos y a una lista de juegos conocidos, Bitdefender puede detectar automáticamente los juegos que se ejecuten y optimizar los recursos del sistema para que pueda disfrutar de su pausa para jugar.

Configuración del Perfil de juego

Para configurar las acciones que desea llevar a cabo en el Perfil de juego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en los juegos
   - Optimizar los ajustes del producto para el perfil de Juego
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para juegos
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir juegos manualmente a la Lista de Juegos

Si Bitdefender no entra automáticamente en el Perfil de juego cuando ejecute cierto juego o aplicación, puede añadir manualmente la aplicación a la **Lista de juegos**.

Para añadir juegos manualmente a la lista de juegos en el Perfil de juego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
5. En la ventana **PERFIL DE JUEGO**, haga clic en el enlace **Lista de juegos**.
6. Haga clic en **Añadir** para añadir un nuevo juego a la **Lista de juegos**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable del juego, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

Perfil de redes Wi-Fi públicas

Enviar correos electrónicos, escribir credenciales confidenciales o efectuar compras online mientras se está conectado a redes inalámbricas poco fiables puede poner en riesgo sus datos personales. El perfil de redes Wi-Fi públicas adapta los ajustes del producto para darle la posibilidad de realizar pagos online y hacer uso de información confidencial en un entorno protegido.

Configuración del perfil de redes Wi-Fi públicas

Para configurar Bitdefender de forma que aplique los ajustes del producto mientras está conectado a una red inalámbrica poco fiable:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del perfil de redes Wi-Fi públicas.

5. Deje marcada la casilla de verificación **Adapta los ajustes del producto para aumentar la protección cuando se conecta a una red Wi-Fi pública poco fiable**.
6. Haga clic en **Guardar**.

Perfil del modo Batería

El perfil del modo Batería está especialmente diseñado para usuarios de portátiles y tablets. Su objetivo es reducir al mínimo tanto el impacto del sistema como de Bitdefender en el consumo de energía cuando el nivel de carga de la batería esté por debajo del establecido por omisión o del que usted determine.

Configuración del perfil del modo Batería

Para configurar el perfil del modo Batería:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del perfil del modo Batería.
5. Elija los ajustes del sistema a aplicar marcando las siguientes opciones:
   - Optimizar los ajustes del producto para el modo Batería.
   - Posponer los programas en segundo plano y las tareas de mantenimiento.
   - Posponga las actualizaciones automáticas de Windows.
   - Adaptar los ajustes del plan de energía para el modo Batería.
   - Deshabilitar los dispositivos externos y los puertos de red.
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Escriba un valor válido en el cuadro de número o selecciónelo con las teclas de flecha arriba y abajo para especificar cuándo debe empezar a funcionar el sistema en modo Batería. Por defecto, el modo se activa cuando el nivel de carga de la batería cae por debajo del 30%.

Cuando Bitdefender opera en el perfil del modo Batería, se aplican los siguientes ajustes del producto:

- Se pospone la actualización automática de Bitdefender.
- Se posponen los análisis programados.
- Se desactiva el Widget de seguridad.

Bitdefender detecta cuándo su portátil pasa a la alimentación con batería y, en función del nivel de carga de ésta, entra automáticamente en modo Batería. De la misma forma, Bitdefender sale automáticamente del modo Batería cuando detecta que el portátil ya no está siendo alimentado con la batería.

Optimización en tiempo real

La Optimización en tiempo real de Bitdefender es un plugin que mejora el rendimiento de su sistema discretamente, en segundo plano, asegurándose de que no se vea interrumpido mientras esté en un modo de perfil. Dependiendo de la carga de la CPU, el plugin monitoriza todos los procesos, centrándose en los que suponen una carga mayor, para adaptarlos a sus necesidades.

Para activar o desactivar la Optimización en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Utilice el conmutador correspondiente para activar o desactivar la Optimización en tiempo real.

6. RESOLUCIÓN DE PROBLEMAS

6.1. Resolución de incidencias comunes

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.

- "Mi sistema parece que se ejecuta lento" (p. 186)
- "El análisis no se inicia" (p. 188)
- "Ya no puedo usar una aplicación" (p. 191)
- "Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online" (p. 192)
- "Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware" (p. 193)
- "Cómo actualizo Bitdefender en una conexión de internet lenta" (p. 198)
- "Los servicios de Bitdefender no responden" (p. 199)
- "El Filtro antispam no funciona correctamente" (p. 199)
- "El Autorrellenado de mi Wallet no funciona" (p. 204)
- "La desinstalación de Bitdefender ha fallado" (p. 205)
- "Mi sistema no se inicia tras la instalación de Bitdefender" (p. 207)

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 "*Pedir ayuda*" (p. 290).

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. 80).

- **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. 3).

- **Ha instalado aplicaciones que no utiliza**.

  Cualquier equipo tiene programas o aplicaciones que no utiliza. Y muchos programas no deseados se ejecutan en segundo plano ocupando espacio en disco y memoria. Si no utiliza un programa, desinstálelo. Esto también vale para otro software preinstalado o aplicación de evaluación que olvidó desinstalar.

  > **Importante**
  > Si sospecha que un programa o una aplicación forma parte esencial de su sistema operativo, no lo elimine y contacte con el departamento de Atención al cliente de Bitdefender para recibir asistencia.

- **Su sistema puede estar infectado**.

  La velocidad y el comportamiento general de su sistema puede verse afectado por el malware. Spyware, virus, troyanos y adware pasan todos factura al rendimiento de su equipo. Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana. Se recomienda utilizar el análisis de sistema Bitdefender porque analiza todo los tipos de malware que amenazan la seguridad de su sistema.

  Para iniciar el análisis del sistema:

  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el enlace **VER MÓDULOS**.
  3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.

4. Siga los pasos del asistente.

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:

  1. Desinstalar Bitdefender completamente del sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
       c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena
          - Wallets
          - Blindaje de Archivos
       d. Haga clic en **CONTINUAR**.
       e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
       d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

e. Haga clic en **CONTINUAR**.

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

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

f. Haga clic en **CONTINUAR**.

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

2. Reinicie su producto Bitdefender.

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

En este caso:

1. Eliminar las otras soluciones de seguridad. Para más información, por favor vea "¿Cómo desinstalo otras soluciones de seguridad?" (p. 80).
2. Desinstalar Bitdefender completamente del sistema:

- En **Windows 7**:

a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.

b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

d. Haga clic en **CONTINUAR**.

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

- En **Windows 8 y Windows 8.1**:

a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

e. Haga clic en **CONTINUAR**.

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

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

f. Haga clic en **CONTINUAR**.

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

3. Reinicie su producto Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

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.

Tras instalar Bitdefender puede encontrarse con 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 se produce cuando el Active Threat Control identifica erróneamente algunas aplicaciones como maliciosas.

Active Threat Control es un módulo de Bitdefender que monitoriza constantemente las aplicaciones que se ejecutan en su sistema e informa de aquellas con comportamientos potencialmente maliciosos. Dado que esta característica se basa en un sistema heurístico, pueden darse casos en los que el Active Threat Control informe sobre aplicaciones legítimas.

Si se produce esta situación, puede evitar que el Active Threat Control monitorice la aplicación correspondiente.

Para añadir el programa a la lista de exclusiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **Exclusiones**.
5. Haga clic en el menú de acordeón **Lista de procesos excluidos del análisis**. En la ventana que aparece puede administrar las exclusiones de procesos de Active Threat Control.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **AÑADIR**.
   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 Threat 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. 290).

Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online

Bitdefender ofrece una experiencia de navegación Web segura filtrando todo el tráfico de Internet y bloqueando cualquier contenido malicioso. No obstante, es posible que Bitdefender considere peligrosa una aplicación online o un sitio Web seguros, lo que hará que el análisis de tráfico HTTP de Bitdefender los bloquee erróneamente.

En caso de que la misma página o aplicación se bloqueen en repetidas ocasiones, se pueden añadir a una lista blanca para que los motores de Bitdefender no las analicen, lo que garantiza una experiencia de navegación Web sin problemas.

Para añadir un sitio Web a la **Lista blanca**:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN WEB**.
4. Haga clic en el enlace **Lista blanca**.
5. Proporcione la dirección del sitio Web o aplicación online bloqueada en el campo correspondiente y haga clic en **Añadir**.
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Solo debe añadir a esta lista aplicaciones y sitios Web en los que confíe plenamente. Éstos se excluirán del análisis por parte de los siguientes motores: malware, phishing y fraude.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Para mantener su sistema a salvo de situaciones desafortunadas, Bitdefender le da la posibilidad de proteger sus archivos personales.

Cuando una aplicación intente cambiar o eliminar alguno de sus archivos protegidos, se considerará poco fiable y Bitdefender bloqueará su funcionamiento.

En caso de que se añada alguna aplicación a la lista de aplicaciones que no son de fiar y que esté seguro de que no hay problema en usarla, siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones bloqueadas**.
4. Haga clic en **Permitir** y escoja la aplicación que considera segura.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada a la lista de confianza.

No puedo conectarme a Internet

Tras instalar Bitdefender, quizás note que algún programa o navegador Web ya no pueden conectarse a Internet o acceder a servicios de red.

En este caso, la mejor solución es configurar Bitdefender para permitir automáticamente las conexiones hacia y desde la aplicación de software correspondiente:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Reglas**.
5. Para añadir una regla de aplicación, haga clic en el botón **AÑADIR REGLA**.
6. Aparece una nueva ventana en la que puede añadir los detalles. Asegúrese de seleccionar todos los tipos de red disponibles y, en la sección de **Permiso**, seleccione **Permitir**.

Cierre Bitdefender, abra la aplicación de software y vuelva a intentar conectarse a Internet.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

No puedo acceder a un dispositivo en mi red

Dependiendo de la red en la que esté conectado, el cortafuego de Bitdefender puede bloquear la conexión entre su sistema y otro dispositivo (como otro equipo o una impresora). En consecuencia es posible que no pueda compartir o imprimir archivos.

En este caso, la mejor solución es configurar Bitdefender para permitir automáticamente las conexiones desde y hacia el dispositivo correspondiente. Para cada conexión de red puede configurar una zona especial de confianza.

Una zona de confianza es un dispositivo en el que confía plenamente. Todo el tráfico entre su equipo y el dispositivo de confianza está permitido. Para

compartir recursos con dispositivos específicos, tales como computadoras o impresoras, agréguelos como zonas de confianza.

Para añadir una zona de confianza en sus adaptadores de red:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Seleccione la pestaña **Adaptadores**.
5. Para añadir una zona, haga clic en el enlace **Excepciones de red**.
6. Escriba la dirección IP del equipo o de la impresora que desea añadir en el campo correspondiente.
7. En la columna **Adaptador**, seleccione **De confianza**.
8. Vaya a **Permiso** y seleccione **Permitir**.
9. Haga clic en el botón + para añadir la excepción y cerrar la ventana.

Si todavía no puede conectarse al dispositivo, Bitdefender no puede ser el causante de su problema.

Comprobar otras causas potenciales, como las siguientes:

- El cortafuego en otro equipo puede bloquear los archivos e impresoras compartidos con su equipo.
  - Si se está utilizando Firewall de Windows, puede configurarse para que permita compartir archivos e impresoras de la siguiente forma:
    - En **Windows 7**:
      1. Haga clic en **Inicio**, vaya al **Panel de control** y seleccione **Sistema y seguridad**.
      2. Vaya a **Windows Firewall** y haga clic en **Permitir un programa a través de Firewall de Windows**.
      3. Marque la casilla de verificación **Compartir archivos e impresoras**.
    - En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Sistema y seguridad**, vaya a **Windows Firewall** y seleccione **Permitir una app a través de Firewall de Windows**.
3. Marque la casilla de verificación **Compartir archivos e impresoras** y haga clic en **Aceptar**.

- En **Windows 10**:
  1. Escriba "Permitir una aplicación a través de Firewall de Windows" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
  2. Haga clic en **Cambiar configuración**.
  3. En la lista **Aplicaciones y características permitidas**, marque la casilla de verificación **Compartir archivos e impresoras** y haga clic en **Aceptar**.
- Si utiliza otro programa de cortafuego, por favor, consulte su documentación o archivo de ayuda.

- Condiciones generales que pueden impedir el uso o la conexión a la impresora compartida:
  - Puede necesitar iniciar sesión con una cuenta de Administrador de Windows para acceder a la impresora compartida.
  - Se establecen los permisos para permitir el acceso a la impresora compartida a los equipos y a los usuarios solamente. Si esta compartiendo su impresora, compruebe los permisos establecidos para esta impresora para ver si el usuario de otro equipo tiene permitido el acceso a la impresora. Si esta intentando conectarse a una impresora compartida, compruebe con el usuario del otro equipo si tiene permisos para conectarse a la impresora.
  - La impresora conectada a su equipo o a otro equipo no está compartida.
  - La impresora compartida no está agregada en el equipo.

> **Nota**
> Para aprender como administrar una impresora compartida (compartir una impresora, establecer o eliminar permisos para una impresora, conectar

una impresora de red o compartir impresora), diríjase a la Ayuda de Windows y Centro de Soporte (en el menú Inició, haga clic en **Ayuda y soporte técnico**).

- El acceso a la impresora de la red puede estar restringido a equipo e usuarios solamente. Debería comprobar con el administrador de red si tiene permisos para conectarse con esta impresora.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

Mi conexión a Internet es lenta

Esta situación puede aparecer después de instalar Bitdefender. La incidencia puede ser causada por errores en la configuración del cortafuego de Bitdefender.

Para resolver esta situación:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.
4. Haga clic en el conmutador correspondiente para desactivar el **Cortafuego**.
5. Compruebe si su conexión a Internet ha mejorado al deshabilitar el cortafuego de Bitdefender.
   - Si tiene una conexión a Internet lenta, el problema puede que no esté causado por Bitdefender. Debe contactar con su Proveedor de Servicios de Internet para verificar si la conexión funciona correctamente.

     Si recibe una confirmación de su Proveedor de Servicios de Internet que la conexión está activa y la incidencia continua, contacto con Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).
   - Si tras desactivar el cortafuego de Bitdefender la conexión a Internet mejora:
     a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
     b. Haga clic en el enlace **VER MÓDULOS**.

c. Seleccione el icono de la esquina superior derecha del módulo **CORTAFUEGO**.

d. En la pestaña de **Ajustes**, haga clic en el conmutador para desactivar **Bloquear análisis de puertos en la red**.

e. Acceda a la pestaña **Adaptadores** y seleccione su conexión a Internet.

f. En la columna **Tipo de red** seleccione **Hogar/Oficina**.

g. En la columna **Modo oculto** seleccione **ACTIVADO**. Ponga la columna **Genérico** en **Activado**.

h. Cierre Bitdefender, reinicie el sistema y compruebe la velocidad de conexión a Internet.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

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:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
3. Junto a **Reglas de proceso de actualización**, seleccione **Preguntar antes de descargar** en el menú desplegable.
4. Vuelva a la ventana principal y haga clic en el botón de acción **Actualizar** de la interfaz de Bitdefender.
5. Seleccione solo **Actualizaciones de firmas** y haga clic en **Aceptar**.
6. Bitdefender descargará e instalará solo las actualizaciones de firmas de malware.

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:

- 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. 80).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 290).

El Filtro antispam no funciona correctamente

Este articulo le ayuda a solucionar los siguientes problemas con el funcionamiento del Filtro Antispam de Bitdefender:

- Un número de mensajes de correo legítimos están marcados como [spam].
- Algunos mensajes spam no están marcados de acuerdo con el filtro spam.
- El filtro antispam no ha detectado ningún mensaje antispam.

Los mensajes legítimos se han marcado como [spam]

Mensajes Legítimos están marcados como [spam] simplemente porque el filtro Antispam de Bitdefender los ve como spam. Normalmente puede solventar este problema adecuando la configuración del filtro Antispam.

Bitdefender automáticamente añade los destinatarios de su mensajes de correo a la lista de Amigos. Los mensajes de correo recibidos de los contacto que estan en la lista de Amigos son considerados como legítimos. Estos no son verificados por el filtro antispam y, así, no serán marcados nunca como [spam].

La configuración automática de la lista de Amigos no previene la detección de errores que pueden ocurrir en estas situaciones:

- Puede recibir muchos correos comerciales como resultado de suscribirse en varias páginas web. En esta caso, la solución en añadir la dirección de correo de la cual recibe tales mensajes a la lista de Amigos.
- Una parte significativa de sus correos legítimos es de gente con los cuales nunca antes se ha contactado, como clientes, posibles socios comerciales y otros. Se requieren otras soluciones en este caso.

  Si está utilizando uno de los clientes de correo que Bitdefender integra, Indique detección de errores.

> **Nota**
> Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, por favor diríjase a "Clientes de correo electrónico y protocolos soportados" (p. 112).

Añadir contactos a la lista de Amigos

Si esta utilizando un cliente de correo compatible, puede añadir fácilmente los remitentes de los mensajes legítimos a la lista de Amigos. Siga estos pasos:

1. En su cliente de correo, seleccionar el mensaje de correo del remitente que desea añadir a la lista de Amigos.
2. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender.

3. Puede pedir que admita las direcciones añadidas a la lista de Amigos. Seleccione **No volver a mostrar este mensaje** y haga clic en**Aceptar**.

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

Si esta utilizando un cliente de correo diferente, puede añadir contactos a lista de Amigos desde la interfaz de Bitdefender. Siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTISPAM**, seleccione **Gestionar amigos**.

   Aparece una ventana de configuración.
4. Escriba la dirección de correo electrónico en la que siempre desee recibir mensajes de correo electrónico y haga clic en **Añadir**. Puede añadir tantas direcciones de correo electrónico como desee.
5. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Indican errores de detección

Si está utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando qué mensajes de correo no deben ser marcados como [spam]). Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione el mensaje legítimos incorrecto marcado como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender para añadir los remitentes a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
5. Haga clic en el botón **No es spam** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la

ventana del cliente de correo). El mensaje de correo electrónico se moverá a la carpeta Bandeja de entrada.

No se han detectado muchos mensajes de spam

Si está recibiendo muchos mensajes spam que no están marcados como [spam], debe configurar el filtro antispam de Bitdefender, con el fin de mejorar su eficiencia.

Pruebe las siguientes soluciones:

1. Si está utilizando uno de los clientes de correo que Bitdefender integra, Indique mensajes spam no detectados.

   Nota

   Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, por favor diríjase a "Clientes de correo electrónico y protocolos soportados" (p. 112).

2. Añadir spammers a la lista de Spammers. Los mensajes de correo recibidos de las direcciones que están en la lista de Spammer son marcados automáticamente como [spam].

Indicar mensajes de spam no detectados

Si esta utilizando un cliente de correo compatible, puede indicar fácilmente que mensajes de correo deben ser detectados como spam. Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta Bandeja de Entrada.
3. Seleccione los mensajes spam no detectados.
4. Haga clic en el botón **Es spam** en la barra antispam de Bitdefender (localizada normalmente en la parte superior de la ventana del cliente de correo). Inmediatamente serán marcados como [spam] y trasladados a la carpeta de correo no deseado.

Añade spammers a la lista de Spammers

Si esta utilizando cliente de correo compatible, puede fácilmente añadir los remitentes de los mensajes spam a la lista de Spammers. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione los mensajes marcados como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir Spammer** en la barra de herramientas antispam de Bitdefender.
5. Puede pedir que reconozca las direcciones añadidas a la Lista de Spammers. Seleccione **No volver a mostrar este mensaje** y haga clic en**Aceptar**.

Si está utilizando un cliente de correo diferente, puede añadir manualmente spammers a la Lista de spammers desde la interfaz de Bitdefender. Es conveniente hacerlo sólo cuando ha recibido bastantes mensajes sapm desde la misma de dirección de correo. Siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTISPAM**, seleccione **Gestionar emisores de spam**.

   Aparece una ventana de configuración.
4. Escriba la dirección de correo electrónico del spammer y luego haga clic en **Añadir**. Puede añadir tantas direcciones de correo electrónico como desee.
5. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

El Filtro antispam no detecta ningún mensaje de spam

Si no se marca el mensaje spam como [spam], esto debe ser un problema con el filtro Antispam de Bitdefender. Antes de resolver este problema, asegúrese que no esta causado por una de las siguientes condiciones:

- Puede que esté desactivada la protección antispam. Para comprobar el estado de la protección antispam, haga clic en el icono de la barra

lateral izquierda de la interfaz de Bitdefender y, a continuación, haga clic en el enlace **VER MÓDULOS**. Haga clic en el icono de rueda dentada del panel **ANTISPAM** y, a continuación, mire en la parte superior de la ventana si el módulo está activado.

Si Antispam está desactivado, esto es lo que está causando el problema. Haga clic en el conmutador correspondiente para activar su protección antispam.

- La protección Antispam de Bitdefender está disponible solo para clientes de correo configurados para recibir mensajes de correo mediante el protocolo POP3. Esto significa lo siguiente:
  - Los mensajes recibidos mediante servicios de correo basados en web (como Yahoo, Gmail, Hotmail u otro) no se filtran como spam por Bitdefender.
  - Si su cliente de correo esta configurado para recibir mensajes de correo utilizando otro protocolo diferente a POP3 (por ejemplo, IMAP4), el filtro Antispam de Bitdefender no marcará estos como spam.

  > **Nota**
  >
  > POP3 es uno de los protocolos más extensos utilizados para descargar mensajes de correo de un servidor de correo. Si no sabe el protocolo que utiliza su cliente de correo para descargas los mensajes, pregunte a la persona que ha configurado su correo.

- Bitdefender Total Security no analiza el tráfico POP3 de Lotus Notes.

Una posible solución esta para reparar o reinstalar el producto. Sin embargo, debería contactar con Bitdefender para soporte, como se describe en la sección "*Pedir ayuda*" (p. 290).

El Autorrellenado de mi Wallet no funciona

Ha guardado sus credenciales online en su Gestor de contraseñas de Bitdefender y se ha dado cuenta de que el autorrelenado no funciona. Normalmente, este problema se produce cuando la extensión Wallet Bitdefender no está instalada en su navegador.

Para resolver esta situación, siga estos pasos:

- En **Internet Explorer:**

1. Abrir Internet Explorer.
2. Haga clic en Herramientas.
3. Haga clic en Barras de herramientas y extensiones.
4. Haga clic en Barras de herramientas y extensiones.
5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

- En **Mozilla Firefox:**
  1. Abra Mozilla Firefox.
  2. Haga clic en Herramientas.
  3. Haga clic en Complementos.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.
- En **Google Chrome:**
  1. Abra Google Chrome.
  2. Vaya al icono Menú.
  3. Haga clic en Configuración.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

Nota
El complemento se habilitará después de que reinicie su navegador.

Ahora compruebe si el autorrelenado de Wallet funciona con sus cuentas online.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 290).

La desinstalación de Bitdefender ha fallado

Si desea desinstalar su producto Bitdefender y observa que el proceso se cuelga o se bloquea el sistema, haga clic en **Cancelar** para cancelar la acción. Si esto no funciona, reinicie el sistema.

Cuando 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 Bitdefender de su sistema por completo:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
     - Archivos trasladados a la cuarentena
     - Wallets
     - Blindaje de Archivos
  4. Haga clic en **CONTINUAR**.
  5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
     - Archivos trasladados a la cuarentena
     - Wallets
     - Blindaje de Archivos
  5. Haga clic en **CONTINUAR**.
  6. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
   - Blindaje de Archivos
6. Haga clic en **CONTINUAR**.
7. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

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 resolver esto:

  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. 82).
  2. Desinstalar Bitdefender de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

d. Haga clic en **CONTINUAR**.

e. Espere a que el proceso de desinstalación se complete.

f. Reinicie su sistema en modo normal.

- En **Windows 8 y Windows 8.1**:

a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete.

g. Reinicie su sistema en modo normal.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets
- Blindaje de Archivos

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete.

h. Reinicie su sistema en modo normal.

3. Reinicie su producto Bitdefender.

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

  Para resolver esto:

  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. 82).
  2. Elimine las otras soluciones de seguridad de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       c. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.

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

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.

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

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.

3. Reinicie su sistema en modo normal y reinstale Bitdefender.

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

Para resolver esto:

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. 82).
2. Utilice la opción Restaurar sistema de Windows para restaurar el equipo a un punto anterior antes de la instalación del producto Bitdefender.
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. 290).

6.2. 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. 211)
- "¿Qué hacer cuando Bitdefender encuentra virus en su equipo?" (p. 213)
- "¿Cómo limpiar un virus en un archivo?" (p. 215)
- "¿Cómo limpio un virus en un archivo de correo?" (p. 216)
- "¿Qué hacer si sospecho que un archivo es peligroso?" (p. 217)
- "¿Qué son los archivos protegidos con contraseña del registro de análisis?" (p. 217)
- "¿Qué son los elementos omitidos en el registro de análisis?" (p. 218)
- "¿Qué son los archivos sobre-comprimidos en el registro de análisis?" (p. 218)
- "¿Por qué eliminó Bitdefender automáticamente un archivo infectado?" (p. 218)

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 "*Pedir ayuda*" (p. 290).

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 Total Security 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 interfaz de Bitdefender

Para entrar en el modo Rescate directamente desde Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Modo rescate**.

   Aparecerá una ventana de confirmación. Haga clic en **Sí** para reiniciar su equipo.
4. Una vez que reinicie su equipo, aparecerá un menú que le pedirá que seleccione un sistema operativo. Elija **Modo rescate Bitdefender** para arrancar en un entorno de Bitdefender desde el cual podrá limpiar la partición de Windows.
5. 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:

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 su sistema en modo Rescate:

1. Acceda al Modo Rescate, como se describe en “Iniciar el sistema en modo Rescate” (p. 211).
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 antivirus bajo demanda 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 se complete el análisis. 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** en el menú que aparece y después elija si desea reiniciar o apagar el equipo.

¿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 cada momento, actualice Bitdefender para asegurarse de que tiene las últimas firmas de virus y ejecute un Análisis del sistema para analizar el sistema.

Tan pronto como el análisis acabe, 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. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. Haga clic en el interruptor para desactivar el **Análisis en acceso**.
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. 80).
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 no lograse eliminar la infección:

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. 82).
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. 80).
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. 290).

¿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. Identifique el archivo comprimido que incluye el virus realizando un Análisis del sistema.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. En la ventana **Residente**, haga clic en el conmutador correspondiente para desactivar 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 del sistema para asegurarse de que no hay ninguna otra infección en el sistema.

Nota
Es importante saber que un virus almacenado en un archivo comprimido no es una amenaza inmediata para su sistema, ya que el virus debe descomprimirse y ejecutarse para que pueda 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. 290).

¿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. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. Haga clic en el interruptor para desactivar el **Análisis en acceso**.
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 Microsoft Outlook 2007: 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 agora.
   - En Microsoft Outlook 2010 / 2013: En el menú Archivo, haga clic en Info y luego en Configuración de cuenta (Añada o elimine cuentas, o cambie los ajustes de conexión existentes). Luego haga clic en Archivo de datos, seleccione los archivos de carpetas personales (.pst) que desea compactar, y haga clic en Configuración. Haga clic en Compactar agora.
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. 290).

¿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 asegurarse de que su sistema está protegido:

1. Ejecute un **Análisis del sistema** con Bitdefender. Para saber como se hace esto, por favor diríjase a "¿Cómo analizo mi sistema?" (p. 60).
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. 290).

¿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.

¿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.

¿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.

¿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.

ANTIVIRUS FOR MAC

7. INSTALACIÓN Y DESINSTALACIÓN

Este capítulo incluye los siguientes temas:

7.1. Requisitos del Sistema

Debe instalar Bitdefender Antivirus for Mac sólo en equipos Macintosh basados en Intel con versión OS X Mavericks (10.9.5), OS X Yosemite (10.10 o posterior), OS X El Capitan (10.11), OS X Sierra(10.12) instaladas.

Su Mac también debe cumplir con todos estos requisitos adicionales:

- Mínimo 1 Gb de Memoria RAM
- Mínimo 600 MB de espacio libre en disco

Se requiere de una conexión a Internet para registrar y actualizar Bitdefender Antivirus for Mac.

Cómo saber que versión de MAC OS X tiene y la información de hardware sobre su Mac

Haga clic en el icono Apple en la esquina izquierda superior de la ventana y elija **Acerca de este Mac**. En la ventana que aparece puede ver la versión del sistema operativo y otra información útil. Haga clic en **Más Info** para información detallada del hardware.

7.2. Instalando Bitdefender Antivirus for Mac

Puede instalar Bitdefender Antivirus for Mac desde:

- Bitdefender Central
- CD/DVD

7.2.1. Instalar desde Bitdefender Central

Desde Bitdefender Central puede descargar el kit de instalación. Una vez que el proceso de instalación se haya completado, se activa Bitdefender Antivirus for Mac.

Para descargar Bitdefender Antivirus for Mac desde Bitdefender Central, siga estos pasos:

1. Inicie sesión como administrador.
2. Diríjase a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta de Bitdefender utilizando su correo electrónico y contraseña.
4. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
5. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **OS X** para descargar su producto de Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
6. Ejecute el producto Bitdefender que ha descargado.
7. Siga los pasos de la instalación. Para obtener más información sobre el proceso, consulte "*Proceso de instalación*" (p. 224).

7.2.2. Instalar desde CD/DVD

1. Introduzca el CD/DVD de instalación en la unidad y ábralo. Utilice el acceso directo para descargar el instalador.
2. Siga los pasos de la instalación. Para obtener más información sobre el proceso, consulte "*Proceso de instalación*" (p. 224).
3. Inicie sesión en su cuenta Bitdefender Central:

   Nota
   Si ya tiene una suscripción activa a Bitdefender Antivirus for Mac, simplemente inicie sesión con su cuenta Bitdefender a la que esté asociada la suscripción y el producto se activará.

   Si su cuenta Bitdefender no tiene ninguna suscripción asociada, o si todavía no tiene una cuenta, proceda en consecuencia:

Ya tengo una cuenta de Bitdefender

Escriba la dirección de correo electrónico y la contraseña de su cuenta de Bitdefender y haga clic en **INICIAR SESIÓN**.

Si olvidó la contraseña de su cuenta o, sencillamente, desea cambiar la que ya estableció, haga clic en el enlace **Olvidé la contraseña**. Escriba su dirección de correo electrónico y, a continuación, haga clic en el botón **OLVIDÉ LA CONTRASEÑA**. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

Nota

Si ya tiene una cuenta de MyBitdefender, puede utilizarla para acceder a cuenta Bitdefender. Si ha olvidado su contraseña, primero tiene que ir a https://my.bitdefender.com para restablecerla. A continuación, utilice las credenciales actualizadas para iniciar sesión en cuenta Bitdefender.

Quiero crear una cuenta Bitdefender

Para crear correctamente una cuenta de Bitdefender, haga clic en el enlace **Crear una**. Escriba la información requerida en los campos correspondientes y, a continuación, haga clic en el botón **CREAR CUENTA**.

Lea las Condiciones del servicio de Bitdefender antes de seguir adelante.

Los datos que introduzca aquí serán confidenciales.

En este caso, el período de evaluación de treinta días se activará automáticamente. Antes de que expire el periodo de evaluación, active su suscripción siguiendo los pasos de "*Activar la suscripción*" (p. 250).

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 https://central.bitdefender.com.

Quiero iniciar la sesión con mi cuenta de Microsoft, Facebook o Google

Para iniciar sesión con su cuenta de Microsoft, Facebook o Google:

a. Seleccione el servicio que desee usar. Será redirigido a la página de inicio de sesión de ese servicio.

b. Siga las instrucciones proporcionadas por el servicio seleccionado para vincular su cuenta a Bitdefender.

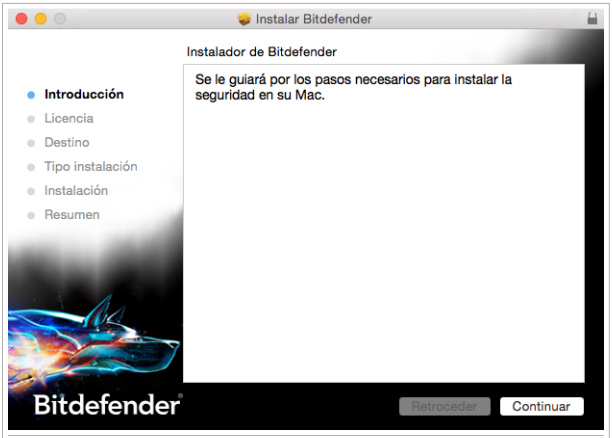
Nota
Bitdefender no tiene acceso a información confidencial, como la contraseña de la cuenta que utiliza para conectarse, o la información personal de sus amigos y contactos.

7.2.3. Proceso de instalación

Para instalar Bitdefender Antivirus for Mac:

1. Haga clic en el archivo descargado. Se iniciará un asistente que le guiará a través del proceso de instalación.
2. Siga el asistente de instalación.

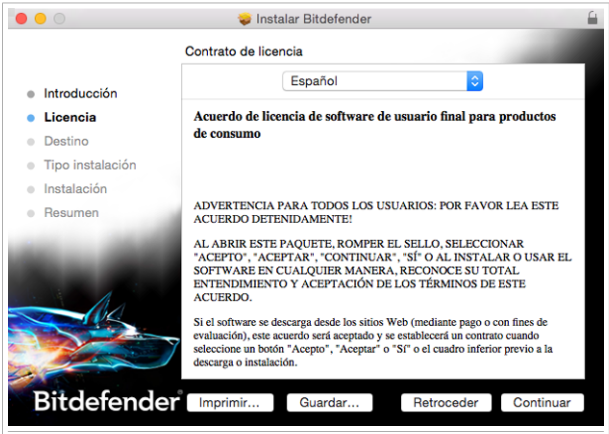
Paso 1 - Ventana de Bienvenida



Ventana de Bienvenida

Haga clic en **Continuar**.

Paso 2 - Lea los Términos del Contrato de Licencia



Leer el Acuerdo de Licencia

El Acuerdo de Licencia es un acuerdo legal entre usted y Bitdefender para el uso de Bitdefender Antivirus for Mac. Puede imprimir o guardar el Acuerdo de Licencia y puede ver estos más tarde.

Por favor, lea el Acuerdo de Licencia cuidadosamente. Para continuar instalando el software debe aceptar los términos del acuerdo de licencia del software. Haga clic en **Continuar** y, a continuación, haga clic en **Acepto**.

Importante

Si no está de acuerdo con estos términos, haga clic en **Continuar** y, a continuación, haga clic en **No acepto** para cancelar la instalación y salir del instalador.

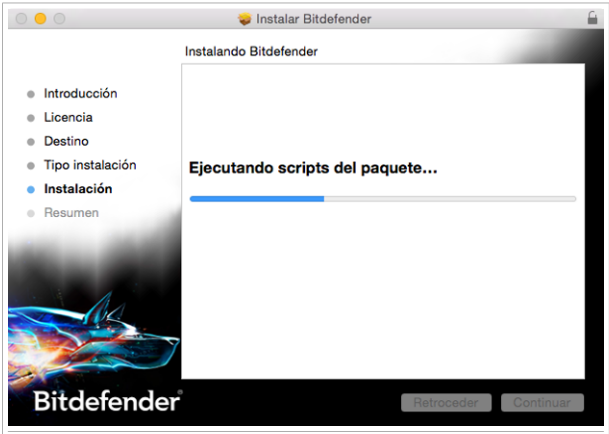
Paso 3 - Iniciar la instalación

Inicio de la Instalación

Bitdefender Antivirus for Mac se instalará en Macintosh HD/Library/Bitdefender. La ruta de instalación no se puede cambiar.

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

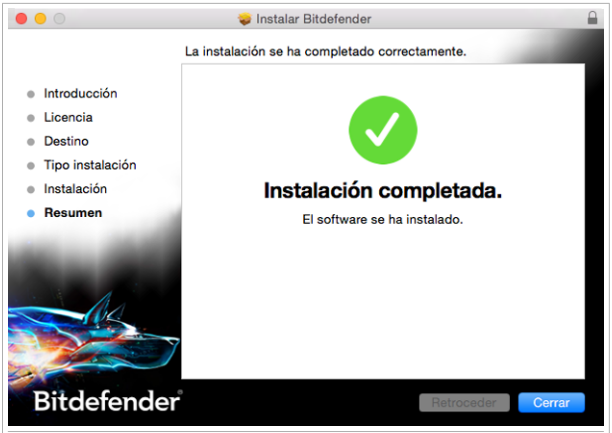
Paso 4 - Instalando Bitdefender Antivirus for Mac



Instalando Bitdefender Antivirus for Mac

Espere hasta que finalice la instalación y, a continuación, haga clic en **Continuar**.

Paso 5 - Finalizar



Finalizar

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

Ha finalizado el proceso de instalación.

En la primera instalación de Bitdefender Antivirus for Mac, aparece el asistente de Protección de Time Machine. Para más información, diríjase a "*Protección de Time Machine*" (p. 235).

7.3. Eliminando Bitdefender Antivirus for Mac

Al ser una aplicación compleja, Bitdefender Antivirus for Mac puede ser eliminando de forma normal, arrastrando el icono de la aplicación de la carpeta de Aplicaciones a la Papelera.

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** acceda a la carpeta de Aplicaciones y seleccione Utilidades.
2. Haga doble clic en la aplicación Desinstalador de Bitdefender para Mac para abrirlo.
3. Haga clic en el botón **Desinstalar** y espere a que finalice el proceso.
4. Haga clic en **Cerrar** para terminar.

> **Importante**
> Si hay un error, puede contactar con Atención al Cliente de Bitdefendercomo se describe en "*Pedir ayuda*" (p. 290).

8. INICIANDO

Este capítulo incluye los siguientes temas:

8.1. Acerca de Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac es un potente analizador antivirus que puede detectar y eliminar todo tipo de software malicioso ("malware"), incluyendo:

- adware
- virus
- spyware
- Caballos de Troya
- keyloggers
- gusanos

Esta aplicación detecta y elimina no solo malware de Mac, sino también malware de Windows, evitando por tanto que envíe accidentalmente archivos infectados a su familia, amigos y compañeros de trabajo que usen PCs.

8.2. Abrir Bitdefender Antivirus for Mac

Hay diferentes maneras de abrir Bitdefender Antivirus for Mac.

- Haga clic en el icono Bitdefender Antivirus for Macen el Launchpad.
- Haga clic en el icono en la barra de menús y seleccione **Abrir la ventana principal**.
- Abra una ventana del Finder, acceda a Aplicaciones y haga doble clic en el icono de Bitdefender Antivirus for Mac.

8.3. Ventana Aplicación Principal

En la ventana principal de la aplicación puede comprobar el estado de seguridad de su equipo, ejecutar análisis del sistema, proteger su navegación por la Web, o iniciar sesión en su cuenta Bitdefender.

Ventana Aplicación Principal

La opción **Autopilot** ubicada en la parte superior derecha de la ventana principal monitoriza continuamente las aplicaciones que se están ejecutando en el equipo, buscando acciones sintomáticas del malware, y evita que entre nuevo malware en su sistema.

Por razones de seguridad, se recomienda mantener Autopilot activado. Si desactiva Autopilot, no estará protegido automáticamente contra las amenazas de malware.

La barra de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y colores asociados. Si Bitdefender Antivirus for Mac no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone amarilla. Haga clic en el botón **Ver incidencias** para ver las incidencias que afectan a la seguridad de su sistema. Para información detalla de incidencias y cómo repararlas, diríjase a "*Reparar Incidencias*" (p. 237).

Bajo la barra de estado, hay disponibles tres botones de análisis para ayudarle a analizar su Mac:

- **Quick Scan**: busca malware en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los documentos,

descargas, descargas de correo electrónico y archivos temporales de cada usuario).

- **Análisis completo**: realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.
- **Análisis personalizado**: le ayuda a comprobar la existencia de malware en archivos, carpetas o volúmenes concretos.

Para más información, diríjase a "*Analizando Su Mac*" (p. 234).

Además de los botones de análisis, existen ciertas opciones adicionales disponibles:

- **Protección Web** - filtra todo el tráfico Web y bloquea cualquier contenido malicioso para proteger su navegación en la Web. Para más información, diríjase a "*Protección Web*" (p. 268).
- **Ir a cuenta Bitdefender**: haga clic en el enlace **Ir a su cuenta** de la parte inferior derecha de la interfaz principal para acceder a su cuenta Bitdefender. Para más información, diríjase a "*Bitdefender Central*" (p. 249).
- **Número de días restantes**: muestra el tiempo restante antes de que caduque su suscripción. Cuando se alcance la fecha de caducidad, haga clic en el enlace para acceder a una página Web desde donde podrá renovar su suscripción.
- **Comprar**: le lleva a la página Web de Bitdefender, donde puede ver las ofertas disponibles o adquirir una suscripción.
- **Comentarios** - abre una nueva ventana en su cliente de correo electrónico predeterminado mediante el cual puede contactar con nosotros.

8.4. Icono Aplicación Dock

El icono de Bitdefender Antivirus for Mac puede verse en el Dock en cuanto abre la aplicación. El icono del Dock le proporciona una manera fácil para analizar archivos y carpetas en busca de malware. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.

Icono del Dock

9. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Este capítulo incluye los siguientes temas:

9.1. Mejores Prácticas

Para mantener su sistema libre de malware y evitar la infección accidental de otros sistemas, siga estas recomendaciones:

- Mantenga activado **Autopilot** para permitir que Bitdefender Antivirus for Mac analice los archivos del sistema.
- Mantenga Bitdefender Antivirus for Mac actualizado con las últimas firmas de malware y actualizaciones de producto, al tiempo que tiene activado **Autopilot**.
- Compruebe y repare regularmente las incidencias reportadas por Bitdefender Antivirus for Mac. Para información detallada, diríjase a "*Reparar Incidencias*" (p. 237).
- Verifique el registro detallado de eventos relativos a la actividad de Bitdefender Antivirus for Mac en su equipo. Siempre que sucede algo relevante para la seguridad de su sistema o de sus datos, se añade un nuevo mensaje al historial de Bitdefender. Para más información, acceda a "*Historial*" (p. 246).
- También debería seguir estas recomendaciones:
  - Acostúmbrese a analizar los archivos que descargue de una fuente de almacenamiento externa (como por ejemplo una memoria USB o un CD), especialmente cuando desconoce el origen de los mismos.

- Si tiene un archivo DMG, móntelo y analice su contenido (los archivos del volumen/imagen montado).

La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&soltando sobre la ventana de Bitdefender Antivirus for Mac o al icono del Dock.

No se requiere otra acción o configuración. Sin embargo, si lo desea, puede ajustar la configuración de la aplicación y las preferencias para satisfacer mejor sus necesidades. Para más información, diríjase a "*Preferencias de Configuración*" (p. 243).

9.2. Analizando Su Mac

Además de la función **Autopilot**, que monitoriza continuamente las aplicaciones que se ejecutan en el equipo, busca síntomas de malware e impide que las nuevas amenazas de malware entren en su sistema, puede analizar su Mac o archivos concretos siempre que desee.

La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&soltando sobre la ventana de Bitdefender Antivirus for Mac o al icono del Dock. El asistente de análisis aparecerá y le guiará a través del proceso de análisis.

También puede iniciar un análisis de la siguiente manera:

1. Abrir Bitdefender Antivirus for Mac.
2. Haga clic en uno de los tres botones de análisis para iniciar el análisis deseado.
   - **Quick Scan**: busca malware en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los documentos, descargas, descargas de correo electrónico y archivos temporales de cada usuario).
   - **Análisis completo**: realiza una comprobación exhaustiva en busca de malware en todo el sistema. Todos los dispositivos montados se analizarán también.

     Nota

     Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén

llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición de vídeo).
Si lo prefiere, puede escoger no analizar volúmenes montados determinados añadiéndolos a la lista de Exclusiones en la ventana de Preferencias.

- **Análisis personalizado**: le ayuda a comprobar la existencia de malware en archivos, carpetas o volúmenes concretos.

9.3. Activar o desactivar Autopilot

Para activar o desactivar Autopilot puede hacer lo siguiente:

- Abra Bitdefender Antivirus for Mac y haga clic en el conmutador para activar o desactivar Autopilot.
- Haga clic en el icono en la barra de menús y seleccione **Desactivar Autopilot**.

Aviso

Le recomendamos que tenga desactivado Autopilot el menor tiempo posible. Si desactiva Autopilot, no estará protegido automáticamente contra las amenazas de malware.

9.4. Protección de Time Machine

La Protección de Time Machine de Bitdefender actúa como una capa adicional de seguridad para su unidad de copia de seguridad, incluyendo todos los archivos que haya decidido almacenar en ella, al bloquear el acceso desde cualquier fuente externa. En caso de que un ransomware cifrara los archivos que tiene almacenados en su unidad de Time Machine, podría recuperarlos sin tener que pagar el rescate solicitado.

Asistente de Protección de Time Machine

El asistente de Protección de Time Machine de Bitdefender aparecerá en cuanto instale Bitdefender Antivirus for Mac por primera vez en su Macintosh.

Tiene que configurar la aplicación del sistema de copia de seguridad de Time Machine antes de activar la protección de Bitdefender.

Si no tuviera Time Machine habilitado en su máquina:

1. Haga clic en la opción **Acceder a Time Machine**.

   Aparecerá la ventana **Time Machine** de Preferencias del sistema.

2. Active la característica y, a continuación, seleccione dónde desea guardar los archivos de copia de seguridad.

Si precisa más indicaciones sobre cómo activar la aplicación Time Machine en su sistema, haga clic en el enlace **Averigüe cómo configurar Time Machine** en el asistente.

Para activar la Protección de Time Machine de Bitdefender para sus copias de seguridad:

1. Haga clic en la opción **Activar protección**.

   Aparecerá una ventana de confirmación.

2. Haga clic en **Cerrar**.

Activación y desactivación de la Protección de Time Machine

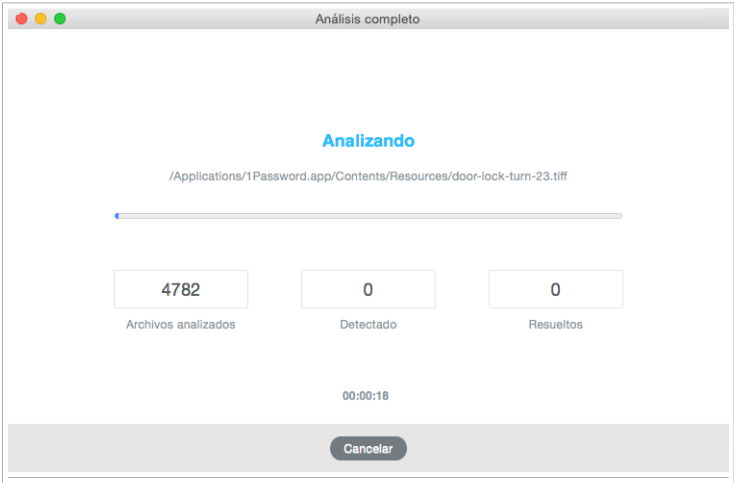
Para activar o desactivar la Protección de Time Machine:

1. Abrir Bitdefender Antivirus for Mac.

2. Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.
3. Seleccione la pestaña **Protección**.
4. Marque o deje sin marcar la casilla de verificación **Protección de Time Machine**.

9.5. Asistente del Análisis

Cuando inicie una análisis, aparecerá el asistente de Análisis de Bitdefender Antivirus for Mac.



Análisis en Progreso

Durante cada análisis se muestra Información en tiempo real acerca de las amenazas detectadas y resueltas.

Espere a que Bitdefender Antivirus for Mac finalice el análisis.

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

9.6. Reparar Incidencias

Bitdefender Antivirus for Mac automáticamente detecta y le informa sobre una serie de incidencias que pueden afectar a la seguridad de su sistema y

sus datos. De esta forma, puede evitar fácilmente y a tiempo riesgos para la seguridad.

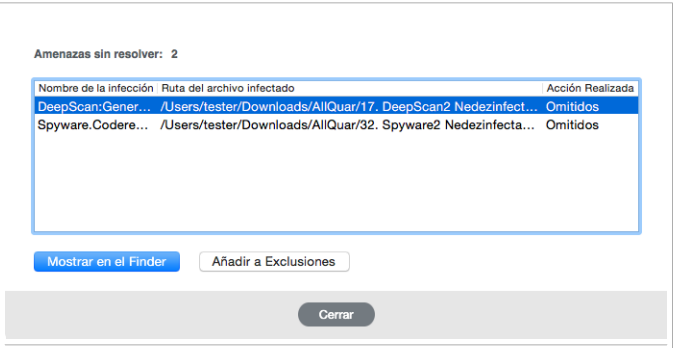
La reparación de incidencias indicadas por Bitdefender Antivirus for Mac es una manera rápida y sencilla de asegurarse una magnífica protección de su sistema y de sus datos.

Los problemas detectados incluyen:

- Las nuevas firmas de malware y actualizaciones de producto no se han descargado de nuestros servidores porque **Autopilot** está desactivado.
- Se han detectado amenazas no resueltas en su sistema.
- **Autopilot** está desactivado.

Para comprobar y reparar las incidencias detectadas:

1. Abrir Bitdefender Antivirus for Mac.
2. Si Bitdefender no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone amarilla.
3. Compruebe la descripción para más información.
4. Cuando se detecte un problema, haga clic en el botón **Ver incidencias** para obtener información acerca de lo que afecta a la seguridad de su sistema. En la ventana que aparece podrá adoptar las acciones oportunas.



Ventana de amenazas no solucionadas

La lista de amenazas no solucionadas se actualiza después de cada análisis del sistema.

Puede escoger adoptar las siguientes medidas respecto a las amenazas no solucionadas:

- Mostrar en el Finder. Lleve a cabo esta acción para eliminar manualmente las infecciones.
- Añadir a exclusiones. Esta acción no está disponible para malware encontrado dentro de archivos comprimidos.

9.7. Protección Web

Bitdefender Antivirus for Mac utiliza las extensiones TrafficLight para proteger completamente su navegación Web. Las extensiones TrafficLight interceptan, procesan y filtran todo el tráfico Web, bloqueando cualquier contenido malicioso.

Las extensiones funcionan y se integran con los siguientes navegadores: Mozilla Firefox, Google Chrome y Safari.

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web:

- Filtro de phishing avanzado - evita que acceda a sitios Web empleados para ataques de phishing.
- Filtro de malware - bloquea cualquier malware con el que entre en contacto mientras navega por Internet.
- Analizador de resultados de búsqueda - proporciona una advertencia anticipada sobre sitios Web peligrosos presentes en sus resultados de búsquedas.
- Filtro antifraude - proporciona protección contra sitios Web fraudulentos mientras navega por Internet.
- Notificación de seguimiento - detecta mecanismos de seguimiento en las páginas Web que visita para proteger su privacidad online.

Habilitación de extensiones TrafficLight

Para habilitar las extensiones TrafficLight, siga los pasos siguientes:

1. Abrir Bitdefender Antivirus for Mac.
2. Haga clic en **Solucionar ahora** para activar la protección Web.

3. Bitdefender Antivirus for Mac detectará qué navegador tiene instalado en su sistema. Para instalar la extensión Linkchecker en su navegador, haga clic en **Obtener extensión**.
4. Será redirigido a esta ubicación online:

   http://bitdefender.com/solutions/trafficlight.html
5. Seleccione **DESCARGA GRATUITA**.
6. Siga los pasos para instalar la extensión TrafficLight correspondiente a su navegador.

Calificación de páginas y alertas

Dependiendo de la clasificación que TrafficLight otorgue a la página Web que esté viendo, mostrará en su área uno de los iconos siguientes:

 Esta página es segura. Puede seguir trabajando.

 Esta página Web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.

 Debería abandonar la página Web inmediatamente. Como alternativa, puede escoger una de las opciones disponibles:

- Abandonar el sitio Web haciendo clic en **Llévame a un sitio seguro**.
- Dirigirse al sitio Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.

9.8. Actualizaciones

Cada día se encuentra e identifica nuevo software malintencionado. Por esta razón es muy importante mantener Bitdefender Antivirus for Mac actualizado con las últimas firmas de malware.

Mantenga activado **Autopilot** para que las firmas de malware y las actualizaciones de producto se descarguen automáticamente en su sistema. Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

La actualización de firmas de malware se realiza al instante, reemplazándose progresivamente los archivos a actualizar. De este modo, la actualización no afecta al funcionamiento del producto y, al mismo tiempo, se evita cualquier riesgo.

- Si Bitdefender Antivirus for Mac está actualizado, este puede detectar las últimas amenazas descubiertas y limpiar los archivos infectados.
- Si Bitdefender Antivirus for Mac no está actualizado, no podrá detectar y eliminarel último malware descubierto por los laboratorios de Bitdefender.

9.8.1. Solicitando una Actualización

Puede solicitar una actualización manualmente en cualquier momento.

Se requiere conexión a Internet con el fin de comprobar las actualizaciones disponibles y descargarlas.

Para solicitar una actualización manual:

1. Abrir Bitdefender Antivirus for Mac.
2. Haga clic en el botón **Acciones** en la barra de menús.
3. Elija **Base de datos de virus**.

Como alternativa, puede solicitar manualmente una actualización pulsando CMD + U.

Puede ver el progreso de actualización y archivos descargados.

9.8.2. Obteniendo Actualizaciones a través de un Servidor Proxy

Bitdefender Antivirus for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

9.8.3. Actualice a una nueva versión

De vez en cuando, lanzamos actualizaciones de producto para añadir nuevas características y mejoras o solucionar deficiencias del producto. Estas actualizaciones podrían requerir un reinicio del sistema para dar paso a la instalación de nuevos archivos. De forma predeterminada, si una actualización precisa un reinicio del equipo, Bitdefender Antivirus for Mac seguirá funcionando con los archivos anteriores hasta que se reinicie el

sistema. Así, el proceso de actualización no interferirá con el trabajo del usuario.

Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si no lee esta notificación, puede también hacer clic en **Reiniciar para actualizar** en la barra de menús o reiniciar manualmente el sistema.

10. PREFERENCIAS DE CONFIGURACIÓN

Este capítulo incluye los siguientes temas:

10.1. Preferencias de Acceso

Para abrir la ventana de Preferencias de Bitdefender Antivirus for Mac:

1. Abrir Bitdefender Antivirus for Mac.
2. Realice una de estas acciones:
   - Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.
   - Haga clic en el icono de la barra de menús y seleccione **Preferencias**.
   - Presione el comando coma(,).

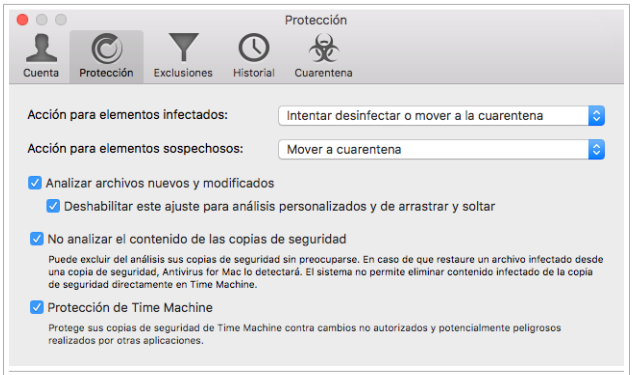
10.2. Información cuenta

La ventana de información de la cuenta le proporciona información acerca de su suscripción y de su cuenta Bitdefender.

Siempre que desee iniciar sesión con otra cuenta Bitdefender, haga clic en el botón **Cambiar cuenta**, introduzca su nueva dirección de correo electrónico y contraseña en la ventana de la aplicación cuenta Bitdefender y, a continuación, haga clic en **INICIAR SESIÓN**.

10.3. Preferencias de protección

La ventana de preferencias de protección le permite configurar el procedimiento general de análisis. Puede configurar las acciones a realizar en los archivos infectados y sospechosos detectados y otros ajustes generales.

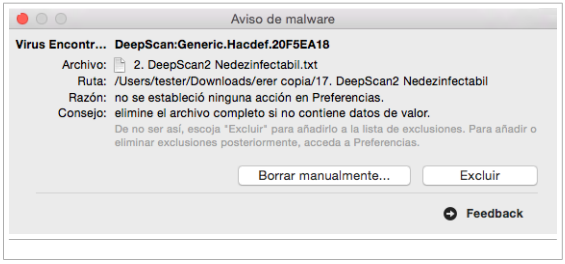


Preferencias de protección

- **Acción para elementos infectados.** Cuando detecta un virus u otro malware, Bitdefender Antivirus for Mac 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 desinfectarse se trasladan a la cuarentena para contener la infección.

  Aunque no se recomienda, puede establecer que la aplicación no haga nada con los archivos infectados. Los archivos detectados solo se mencionan en el registro.

  Autopilot asegura una buena protección contra el malware, con escaso impacto en el rendimiento del sistema. Si hay amenazas sin resolver, puede verlas y decidir qué hacer con ellas.



- **Acción para elementos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible.

De forma predeterminada, los archivos sospechosos se trasladan a la cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Si lo prefiere, puede escoger ignorar los archivos sospechosos. Los archivos detectados solo se mencionan en el registro.

- **Analizar archivos nuevos y modificados.** Seleccione esta casilla para que Bitdefender Antivirus for Mac analice sólo archivos que no han sido analizados antes o estos han sido modificados desde el último análisis.

  Puede elegir no aplicar esta opción de análisis arrastrar&soltar seleccionando la correspondiente casilla.

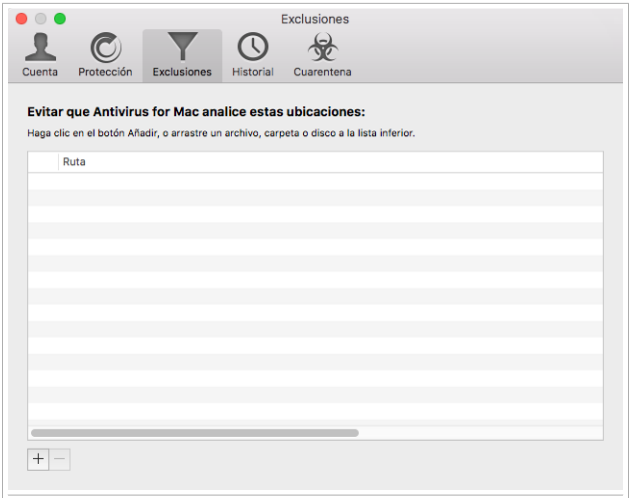
- **No analizar el contenido de las copias de seguridad.** Seleccione esta casilla de verificación para excluir del análisis los archivos de copia de seguridad. Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

- **Protección de Time Machine.** Marque esta casilla de verificación para proteger los archivos almacenados en Time Machine. En caso de que un ransomware cifrara los archivos que tiene almacenados en su unidad de Time Machine, podría recuperarlos sin tener que pagar el rescate solicitado.

10.4. Exclusiones del Análisis

Si así lo desea, puede hacer que Bitdefender Antivirus for Mac no analice ciertos archivos, carpetas o incluso un volumen entero. Por ejemplo, quizá querría excluir del análisis:

- Archivos que han sido identificados por error como infectados (conocidos como falsos positivos)
- Archivos que provocan errores de análisis
- Hacer copia de seguridad de los volúmenes



Exclusiones del Análisis

La lista de exclusiones contiene las rutas que han sido omitidas para el análisis.

Existen dos modos de establecer una exclusión de análisis:

- Arrastrar y soltar un archivo, carpeta o volumen sobre la lista de exclusiones.
- Haga clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de exclusiones. Luego, escoja el archivo, carpeta o volumen a excluir del análisis.

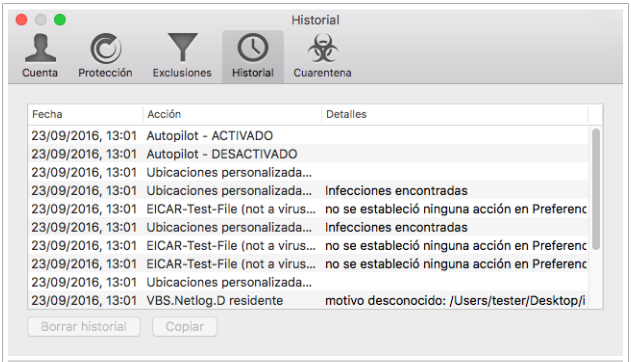
Para eliminar una exclusión de análisis, selecciónela en la lista y haga clic en el botón etiquetado con el signo menos (-), ubicado bajo la lista de exclusiones.

10.5. Historial

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC. Siempre que ocurra algo relevante concerniente a la seguridad de su sistema o de sus datos, se añadirá un nuevo mensaje al Historial de Bitdefender Antivirus for Mac, como si fuera un nuevo mensaje de correo electrónico que apareciese en su bandeja de entrada.

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 realizó correctamente, si se encontró malware en su equipo, si una aplicación no autorizada trató de acceder a su unidad de Time Machine, etc.

Se muestra información detallada acerca de la actividad del producto.



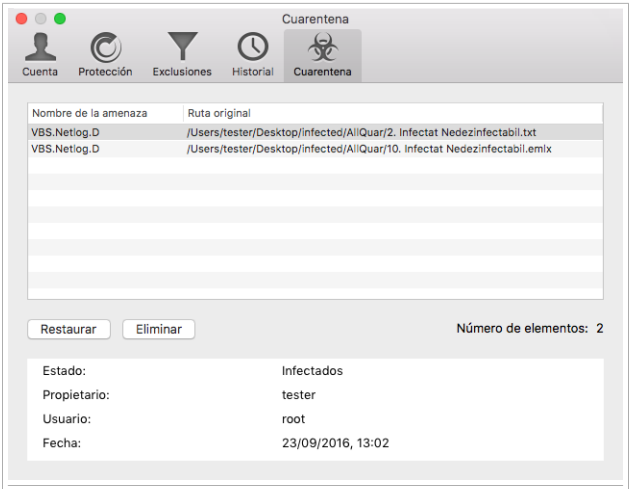
Historial

Cada vez que quiera eliminar el registro del historial, haga clic en el botón **Borrar historial**.

El botón **Copiar** le da la posibilidad de copiar esta información en el portapapeles.

10.6. Cuarentena

Bitdefender Antivirus for Mac le permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.



Archivos trasladados a la cuarentena

El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

11. BITDEFENDER CENTRAL

Este capítulo incluye los siguientes temas:

- "*Acerca de Bitdefender Central*" (p. 249)
- "*Mis suscripciones*" (p. 283)
- "*Mis dispositivos*" (p. 281)

11.1. Acerca de Bitdefender Central

Bitdefender Central es la plataforma Web en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet con solo acceder a https://central.bitdefender.com. Una vez que haya accedido a la misma, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos OS X, Windows y Android. Los productos disponibles para su descarga son:
  - Bitdefender Antivirus for Mac
  - La línea de productos de Windows de Bitdefender
  - Bitdefender Mobile Security
  - Asesor parental de Bitdefender
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

11.2. Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central. Dependiendo de la tarea que desee realizar, puede optar por cualquiera de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender Antivirus for Mac:
  1. Haga clic en el enlace **Ir a su cuenta** de la parte inferior derecha de la pantalla.
- Desde su navegador Web:

1. Abra un navegador Web en cualquier dispositivo con acceso a Internet.
2. Diríjase a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta con su correo electrónico y contraseña.

11.3. Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

11.3.1. Activar la suscripción

Una suscripción se puede activar durante el proceso de instalación mediante su cuenta de Bitdefender. Tras el proceso de activación, da comienzo la cuenta atrás de la validez de la suscripción.

Si ha comprado un código de activación a uno de nuestros resellers o lo ha recibido de regalo, puede añadir su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción mediante un código de activación, siga estos pasos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono ☰ ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Haga clic en **ENVIAR**.

La suscripción ya está activada.

Para comenzar la instalación del producto en sus dispositivos, consulte "*Instalar desde Bitdefender Central*" (p. 221).

11.3.2. Comprar suscripción

Puede adquirir una suscripción directamente desde su cuenta Bitdefender siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono ☰ ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.

3. Haga clic en el enlace **Comprar ahora**. Se le redirigirá a una página Web donde podrá realizar su compra.

En cuanto termine el proceso, la disponibilidad de la suscripción será visible en la esquina inferior derecha de la interfaz principal del producto.

11.4. Mis dispositivos

El área **Mis dispositivos** en su cuenta de Bitdefender le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de dispositivo muestran el nombre del mismo, el estado de protección y la disponibilidad restante de su suscripción.

11.4.1. Personalice su dispositivo

Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceda a Bitdefender Central.
2. En la ventana **Mis dispositivos**, haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Ajustes**.
3. Cambie el nombre del dispositivo al que desee y, a continuación, seleccione **Guardar**.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceda a Bitdefender Central.
2. En la ventana **Mis dispositivos**, haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Perfil**.
3. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes, establezca el sexo, la fecha de nacimiento e incluso añada una imagen al perfil.
4. Haga clic en **AÑADIR** para guardar el perfil.
5. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, haga clic en **ASIGNAR**.

11.4.2. Acciones remotas

Para actualizar Bitdefender de forma remota en un dispositivo, haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Actualizar**.

Para activar Autopilot de forma remota, haga clic en el icono ⋮ de la tarjeta del dispositivo deseada y, a continuación, seleccione **Ajustes**. Haga clic en el conmutador correspondiente para activar Autopilot.

Una vez que haga clic en una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de Control**. En esta ventana puede comprobar el estado de protección de sus productos Bitdefender y el número de días restantes de su suscripción. El estado de protección puede ser verde, cuando no hay ningún problema que afecte a su producto, o rojo cuando el dispositivo está en riesgo. Cuando existan problemas que afecten a su producto, haga clic en **Ver incidencias** para obtener más información.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis completo en sus dispositivos. Haga clic en el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible. Para más información sobre estos dos procesos de análisis, consulte "*Analizando Su Mac*" (p. 234).

12. PREGUNTAS FRECUENTES

¿Cómo puedo probar Bitdefender Antivirus for Mac antes de solicitar una suscripción?

Es un nuevo cliente de Bitdefender y le gustaría probar nuestro producto antes de comprarlo. El periodo de evaluación es de treinta días y puede seguir utilizando el producto instalado con solo adquirir una suscripción de Bitdefender. Para probar Bitdefender Antivirus for Mac, tiene que:

1. Crear una cuenta Bitdefender siguiendo estos pasos:
   - Diríjase a: https://central.bitdefender.com.
   - Escriba la información requerida en los campos correspondientes y, a continuación, haga clic en el botón **CREAR CUENTA**.

     Los datos que introduzca aquí serán confidenciales.
2. Descargue Bitdefender Antivirus for Mac de la siguiente manera:
   - En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
   - Escoja una de las dos opciones disponibles:
     - **DESCARGAR**

       Haga clic en el botón y guarde el archivo de instalación.
     - **En otro dispositivo**

       Seleccione **OS X** para descargar su producto de Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
   - Ejecute el producto Bitdefender que ha descargado.

Tengo un código de activación. ¿Cómo puedo añadir su validez a mi suscripción?

Si ha comprado un código de activación a uno de nuestros resellers o lo ha recibido de regalo, puede añadir su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción mediante un código de activación, siga estos pasos:

1. Acceda a Bitdefender Central.

2. Haga clic en el icono ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Haga clic otra vez en el botón **CÓDIGO DE ACTIVACIÓN**.

La extensión se puede ver ahora en su cuenta Bitdefender, y en su producto Bitdefender Antivirus for Mac instalado, en la parte inferior derecha de la pantalla.

El registro de análisis indica que todavía hay elementos sin resolver. ¿Cómo los elimino?

Los elementos sin resolver en el registro de análisis pueden ser:

- archivos de acceso restringido (xar, rar, etc.)

  Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y borrarlo manualmente. Asegúrese de vaciar la Papelera.

- buzones de correo de acceso restringido (Thunderbird, etc.)

  Solución: Utilice la aplicación para eliminar la entrada que contiene el archivo infectado.

- Contenido de las copias de seguridad

  Solución: active la opción **No analizar el contenido de las copias de seguridad** en Preferencias de protección o **Añadir a exclusiones** los archivos detectados.

  Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

> **Nota**
> Se entiende por archivos de acceso restringido aquellos que Bitdefender Antivirus for Mac solo puede abrir, pero no puede modificar.

¿Dónde puedo leer información detallada sobre la actividad del producto?

Bitdefender mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para acceder a esta información, abra la ventana de Preferencias de Bitdefender Antivirus for Mac:

1. Abrir Bitdefender Antivirus for Mac.

2. Realice una de estas acciones:
   - Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.
   - Haga clic en el icono de la barra de menús y seleccione **Preferencias**.
   - Presione el comando coma(,).
3. Seleccione la pestaña **Historial**.

   Se muestra información detallada acerca de la actividad del producto.

¿Puedo actualizar Bitdefender Antivirus for Mac a través de un servidor proxy?

Bitdefender Antivirus for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar a una conexión directa a Internet con el fin de obtener las actualizaciones de las firmas de malware.

¿Cómo puedo eliminar Bitdefender Antivirus for Mac?

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** acceda a la carpeta de Aplicaciones y seleccione Utilidades.
2. Haga doble clic en la aplicación Desinstalador de Bitdefender.
3. Haga clic en **Desinstalar** para continuar.
4. Espere a que termine el proceso y, a continuación, haga clic en **Cerrar** para finalizar.

> **Importante**
> Si hay un error, puede contactar con Atención al Cliente de Bitdefendercomo se describe en "*Pedir ayuda*" (p. 290).

¿Cómo elimino las extensiones TrafficLight de mi navegador?

- Para eliminar las extensiones TrafficLight de Mozilla Firefox, siga los pasos siguientes:
  1. Abra su navegador Mozilla Firefox.
  2. Vaya a **Herramientas** y seleccione **Complementos**.

3. Seleccione **Extensiones** en la columna izquierda.
4. Seleccione las extensiones y haga clic en **Eliminar**.
5. Reinicie el navegador para completar el proceso de eliminación.

- Para eliminar las extensiones TrafficLight de Google Chrome, siga los pasos siguientes:
  1. Abra su navegador Google Chrome.
  2. Haga clic en  en la barra de herramientas del navegador.
  3. Vaya a **Herramientas** y seleccione **Extensiones**.
  4. Seleccione las extensiones y haga clic en **Eliminar**.
  5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.
- Para eliminar las extensiones Bitdefender TrafficLight de Safari, siga los pasos siguientes:
  1. Abra su navegador Safari.
  2. Haga clic en  en la barra de herramientas del navegador y haga clic en **Preferencias**.
  3. Seleccione la pestaña **Extensiones** y localice en la lista la extensión **Bitdefender TrafficLight en Safari**.
  4. Seleccione la extensión y haga clic en **Desinstalar**.
  5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.

MOBILE SECURITY PARA ANDROID

13. FUNCIONES DE PROTECCIÓN

Bitdefender Mobile Security & Antivirus protege su dispositivo Android con las siguientes funciones:

- Analizador malware
- Asesor de privacidad
- Seguridad Web
- Antirrobo, incluyendo:
  - Localización remota
  - Bloqueo de dispositivo remoto
  - Borrado de dispositivo remoto
  - Alertas de dispositivo remotas
- Bloqueo de apps
- Informes
- Localizador

Puede usar el producto durante 14 días, sin cargo alguno. Tras expirar el período, ha de adquirir la versión completa para proteger su dispositivo móvil.

14. INICIANDO

Requisitos del Dispositivo

Bitdefender Mobile Security & Antivirus funciona en cualquier dispositivo que ejecute Android 3.0 y superior. Se necesita una conexión a Internet activa para el análisis malware en la nube.

Instalando Bitdefender Mobile Security & Antivirus

- **Desde Bitdefender Central**
  - Para Android
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. En la ventana **Mis dispositivos**, toque el icono +.
    4. Seleccione **Bitdefender Mobile Security** en la lista y, a continuación, toque **ACCEDER A GOOGLE PLAY**.
    5. En la pantalla de Google Play, toque **INSTALAR**.
  - En Windows, Mac OS X e iOS
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. En la ventana **MIS DISPOSITIVOS**, toque **INSTALAR Bitdefender**.
    4. Seleccione el enlace **En otro dispositivo**.
    5. Seleccione **Android**.
    6. Seleccione **Bitdefender Mobile Security** en la lista y, a continuación, toque **CONTINUAR**.
    7. Introduzca una dirección de correo electrónico en el campo correspondiente y toque **ENVIAR**.
    8. Acceda a su cuenta de correo electrónico desde su dispositivo Android y, a continuación, toque el botón **CONSEGUIRLO EN Google Play**.

       Se le redirigirá a la app **Google Play**.

9. En la pantalla de Google Play, toque **INSTALAR**.

- **Desde Google Play**

  Busque Bitdefender Mobile Security & Antivirus para encontrar e instalar la app.

  Como alternativa, escanee el código QR:

Inicie sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security & Antivirus debe vincular su dispositivo a una cuenta de Google o Bitdefender iniciando sesión en la cuenta desde la app. La primera vez que abra la app se le pedirá que registre una cuenta.

Si ha instalado Bitdefender Mobile Security & Antivirus desde su cuenta Bitdefender, la app intentará iniciar sesión automáticamente en esa cuenta.

Para vincular su dispositivo a una cuenta de Bitdefender:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque **USAR CUENTA DE CENTRAL** y, a continuación, escriba la dirección de correo electrónico y contraseña de su nueva cuenta de Bitdefender.

   Nota
   Si carece de cuenta, toque el botón correspondiente para crear una. Para iniciar sesión con una cuenta de Google, toque la opción **USAR ID DE GOOGLE**.

3. Toque **INICIAR SESIÓN**.

Activación de Bitdefender Mobile Security & Antivirus

Para que Bitdefender Mobile Security & Antivirus le proteja, debe activar su producto con una suscripción, la cual especifica cuánto tiempo puede utilizar el producto. En cuanto caduque, la aplicación dejará de realizar sus funciones y proteger su dispositivo.

Para activar Bitdefender Mobile Security & Antivirus:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. La app muestra información sobre el estado actual de la suscripción.

   Toque **Ya tengo una clave**.
3. Escriba un código de activación en el campo correspondiente y toque **ACTIVAR**.

Para ampliar una suscripción disponible:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Información de la cuenta** en la lista.
3. En la sección **Prolongar la suscripción**, escriba un código de activación y toque **ACTIVAR**.

   También puede ampliar su suscripción actual accediendo a las ofertas de la lista.

Panel de Control

Toque el icono Bitdefender Mobile Security & Antivirus en la carpeta de aplicaciones del dispositivo para abrir la interfaz de la aplicación.

El panel de control ofrece información sobre el estado de seguridad de su dispositivo y le permite administrar fácilmente todas las funciones de seguridad.

Cada vez que haya un proceso en curso o cuando una función requiera su atención, se mostrará en el panel de control una tarjeta con más información y las posibles acciones.

Puede acceder a las características de Bitdefender Mobile Security & Antivirus e ir fácilmente de una sección a otra con el botón **Menú** situado en la esquina superior izquierda de la pantalla:

Analizador malware
Le permite iniciar un análisis bajo demanda y activar o desactivar el análisis de almacenamiento. Para más información, por favor diríjase a"*Analizador malware*" (p. 263)

Asesor de privacidad
Le ofrece información sobre las apps Android instaladas en su dispositivo y sobre las acciones que éstas llevan a cabo en segundo plano. Para más información, por favor diríjase a"*Asesor de privacidad*" (p. 266)

Seguridad Web
Le permite activar y desactivar la característica de Seguridad Web. Para más información, por favor diríjase a"*Protección Web*" (p. 268)

Antirrobo
Le permite activar o desactivar el Antirrobo, así como configurar sus ajustes. Para más información, por favor diríjase a"*Características Antirrobo*" (p. 270)

Bloqueo de apps
Le permite proteger su aplicaciones instaladas mediante el establecimiento de un código de acceso PIN. Para más información, por favor diríjase a"*Bloqueo de apps*" (p. 275)

Informes
Mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con la actividad de su dispositivo. Para más información, por favor diríjase a"*Informes*" (p. 279)

Localizador
Se comunica con su smartwatch para ayudarle a encontrar su teléfono en caso de que lo extravíe u olvide dónde lo dejó. Para más información, por favor diríjase a"*Localizador*" (p. 280)

15. ANALIZADOR MALWARE

Bitdefender protege su dispositivo y sus datos frente a aplicaciones maliciosas utilizando el análisis en la instalación y el análisis bajo demanda.

Nota
Asegúrese de que su dispositivo móvil está conectado a Internet. Si su dispositivo no está conectado a Internet, no comenzará el proceso de análisis.

- **Análisis en la instalación**

  Siempre que instale una aplicación, Bitdefender Mobile Security & Antivirus la analizará automáticamente usando la tecnología en la nube.

  El tipo de análisis viene dado por la función Autopilot. Autopilot es un analizador inteligente que analizará todas las apps que trate de instalar, bloqueando los ataques de virus.

  Si se determina que la aplicación es peligrosa, aparecerá un alerta solicitándole su desinstalación. Toque **Desinstalar** para ir a la pantalla de desinstalación de la aplicación.

- **Análisis solicitado**

  Siempre que quiera asegurarse de que las aplicaciones instaladas en su dispositivo son seguras, puede iniciar un análisis bajo demanda.

  Para iniciar un análisis bajo demanda, simplemente toque el botón **INICIAR ANÁLISIS** de la tarjeta del Analizador de malware disponible en el panel de control.

  También puede realizar un análisis siguiendo estos pasos:

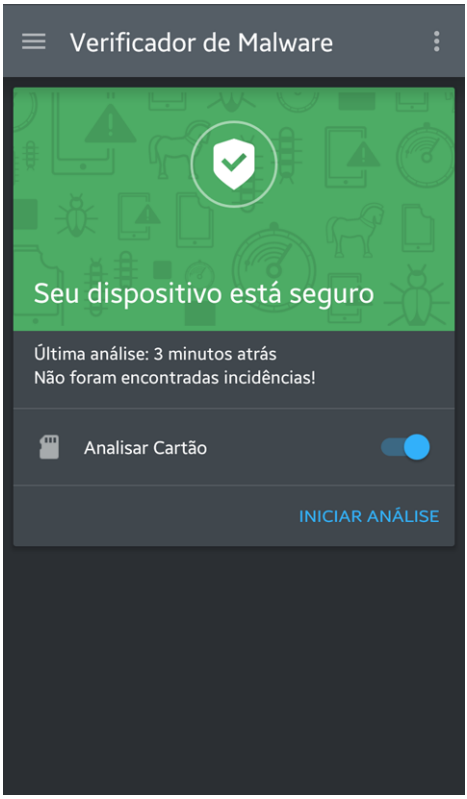
  1. Abrir Bitdefender Mobile Security & Antivirus.
  2. Toque el botón **Menú** y seleccione **Analizador de malware** en la lista.
  3. Toque **INICIAR ANÁLISIS**.

  Nota
  En Android 6 se requieren permisos adicionales para la característica Analizador de malware. Tras tocar el botón **INICIAR ANÁLISIS**, seleccione **Permitir** para lo siguiente:

  - ¿Permitir que **Antivirus** realice y gestione llamadas telefónicas?

- ¿Permitir que **Antivirus** acceda a las fotografías, vídeos y archivos en su dispositivo?

Se mostrará el progreso de análisis y puede detener el proceso en cualquier momento.



Análisis malware

Por defecto, Bitdefender Mobile Security & Antivirus analizará el almacenamiento interno de su dispositivo, incluyendo cualquier tarjeta SD que tenga montada. De esta forma, podrá detectarse cualquier aplicación peligrosa que pudiera estar en la tarjeta antes de que cause ningún daño.

Para habilitar o deshabilitar el ajuste de Analizar almacenamiento:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Analizador de malware** en la lista.
3. Toque el conmutador correspondiente.

También puede activar o desactivar el análisis de almacenamiento desde la zona de **Ajustes** con solo tocar el botón y, a continuación, el conmutador correspondiente.

Si se detecta cualquier aplicación maliciosa, se mostrará información sobre la misma y la podrá eliminar tocando el botón **DESINSTALAR**.

La tarjeta del Analizador de malware muestra el estado de su dispositivo. Cuando su dispositivo está a salvo, la tarjeta es de color verde. Cuando el dispositivo requiere un análisis, o hay alguna acción que requiera su atención, la tarjeta se vuelve roja.

16. ASESOR DE PRIVACIDAD

El Asesor de privacidad se basa en datos de auditoría en la nube para ofrecerle información permanentemente actualizada sobre sus apps Android.

La mayoría de las apps actúan de manera legítima, pero también las hay que pueden registrar su ubicación, acceder a su información personal y compartirla. El Asesor de privacidad le expone unos hechos, pero en última instancia es usted quien debe decidir si puede utilizar una app con seguridad o no.

Utilice el Asesor de privacidad para obtener más información sobre apps que:

- Acceden a su agenda de contactos o la envían a su nube.
- Pueden conocer su identidad real.
- Pueden ser negligentes a la hora de enviar sus contraseñas por Internet y poner sus cuentas en riesgo.
- Pueden utilizar y enviar su ID de dispositivo único para analizar lo que usted hace.
- Recogen datos de análisis para monitorizarle.
- Registran su ubicación.
- Muestran anuncios.
- puede costarle dinero

Toque el icono de filtro  para ver una lista con los indicios más importantes.

En esta lista hay la siguiente información:

- Qué apps son virus.
- Qué apps envían su identidad a extraños.
- Qué apps utilizan anuncios muy intrusivos.
- qué apps envían su información privada a extraños
- Qué apps pueden costarle dinero.
- Qué apps envían datos sin cifrar.
- Qué apps registran su ubicación.

- Qué apps tienen acceso a información sensible.

Puntuación de privacidad

Calculando una Puntuación de privacidad para cada usuario, el Asesor de privacidad le proporciona una idea precisa y personalizada de cuán vulnerable es usted, para que pueda evaluar y tomar las decisiones apropiadas respecto a todas las apps instaladas. Debe tener cuidado cuando su Puntuación de privacidad sea baja.

Si tiene dudas sobre los permisos requeridos por una aplicación determinada, intente encontrar más información sobre ella antes de decidir si seguir utilizándola o no.

17. SEGURIDAD WEB

Seguridad Web comprueba las páginas Web a las que accede con Google Chrome y con el navegador predeterminado de Android utilizando los servicios cloud de Bitdefender.

Si una URL apunta a un sitio Web conocido de phishing o fraudulento, o a contenido malicioso como spyware o virus, la página Web se bloquea temporalmente y se muestra una alerta.

Puede elegir ignorar la alerta y entrar en la página Web o volver a una página segura.

Nota

En Android 6 se requieren permisos adicionales para la característica Seguridad Web.
Dé permiso para registrarse como servicio de accesibilidad y toque **ACTIVAR** cuando se le solicite. Toque **Antivirus** y active el conmutador. A continuación, confirme que está de acuerdo con el permiso de acceso a su dispositivo.

Seguridad Web

18. CARACTERÍSTICAS ANTIRROBO

Bitdefender puede ayudarle a encontrar su dispositivo y evitar que sus datos personales caigan en malas manos.

Todo lo que necesita es activar el Antirrobo desde el dispositivo y, cuando sea necesario, acceder a **Bitdefender Central** desde cualquier navegador web en cualquier lugar.

Incluso si no tiene acceso a Internet, puede seguir protegiendo su dispositivo y sus datos enviando **comandos SMS** desde cualquier teléfono móvil a su smartphone mediante mensajes de texto ordinarios.

Bitdefender Mobile Security & Antivirus ofrece las siguientes opciones Antirrobo:

Localización remota

Vea la ubicación actual de su dispositivo en Google Maps. La ubicación se actualiza cada cinco segundos, por lo que puede seguirle la pista si está en movimiento.

La precisión de la ubicación depende de cómo pueda determinarla Bitdefender:

- Si está activado el GPS en el dispositivo, su ubicación puede señalarse con un par de metros de margen siempre que se encuentre en el alcance de los satélites GPS (es decir, no dentro de un edificio).
- Si el dispositivo está en interior, su localización puede determinarse con un margen de decenas de metros si la conexión Wi-Fi está activada y hay redes inalámbricas disponibles a su alcance.
- De lo contrario, la ubicación se determinará utilizando únicamente información de la red móvil, que ofrece una precisión de varios cientos de metros.

Mostrar IP

Muestra la última dirección IP del dispositivo seleccionado. Toque **MOSTRAR IP** para que se vea.

Borrado remoto

Borrar todos los datos personales del dispositivo extraviado.

Bloqueo remoto

Bloquee la pantalla de su dispositivo y establezca un número PIN para desbloquearla.

Enviar alerta al dispositivo (Scream)

Enviar de forma remota un mensaje para que se muestre en la pantalla del dispositivo o hacer que reproduzca un sonido fuerte por sus altavoces.

Si pierde su dispositivo, puede indicarle a quien lo encuentre la forma de devolvérselo mostrando un mensaje en la pantalla del dispositivo.

Si ha extraviado su dispositivo y hay probabilidad de que no se encuentre muy lejos (por ejemplo en algún lugar de la casa o la oficina), ¿qué mejor forma de encontrarlo que hacer que reproduzca un sonido a gran volumen? Se reproducirá el sonido incluso aunque el dispositivo se encuentre en modo silencioso.

Activación de Antirrobo

Para habilitar las características antirrobo, simplemente complete el proceso de configuración de la tarjeta Antirrobo disponible en el panel de control.

También puede activar el Antirrobo siguiendo estos pasos:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Antirrobo** en la lista.
3. Dará comienzo el siguiente procedimiento para ayudarle a activar esta característica:

   Nota

   En Android 6 se requieren permisos adicionales para la característica Antirrobo. Para activarla, siga los pasos indicados a continuación:

   - Toque **Activar Antirrobo** y, a continuación, toque **ACTIVAR**.
   - Dé permisos para lo siguiente:
     a. ¿Permitir que **Antivirus** envíe y vea los mensajes SMS?
     b. ¿Permitir que **Antivirus** acceda a la ubicación de este dispositivo?
     c. ¿Permitir que **Antivirus** acceda a sus contactos?

   a. **Conceder privilegios de administrador**

   Estos privilegios son esenciales para el funcionamiento del módulo Antirrobo y por tanto debe otorgarlos para poder continuar.

   b. **Establecer PIN de la aplicación**

Para asegurarse de que cualquier cambio efectuado en los ajustes de Antirrobo cuenta con su autorización, debe establecer un PIN. Cada vez que se intenten modificar los ajustes de Antirrobo, será necesario introducir el PIN para que se apliquen los cambios.

Nota
El Bloqueo de apps utiliza el mismo código PIN para proteger las aplicaciones que tiene instaladas.

c. **Establezca el número de confianza para el Antirrobo**

Cuando se inserta una tarjeta SIM diferente en su dispositivo, Bitdefender Mobile Security & Antivirus envía automáticamente un mensaje de texto al número de confianza informándole del nuevo número de teléfono.

Así podrá enviar comandos SMS a su teléfono incluso aunque cambien la tarjeta SIM y, por tanto, el número.

El número de confianza puede ser el de alguien que usted conozca, o el de otro teléfono que utilice. Puede teclear el número o seleccionar uno de la lista de contactos.

Importante
Este paso no es obligatorio, pero se recomienda que establezca el número de confianza durante la configuración inicial. El comando Wipe funciona solo cuando se envía desde el número de confianza predefinido.

Una vez que se activa Antirrobo, puede activar o desactivar independientemente las opciones de control vía SMS y vía Web desde la pantalla de Antirrobo tocando los botones correspondientes.

Utilización de las funciones de Antirrobo desde Bitdefender Central (Control Web)

Nota
Todas las características de Antirrobo necesitan que esté activa la opción **Datos en segundo plano** en los ajustes de Uso de datos de su dispositivo.

Para acceder a las características de Antirrobo desde su cuenta de Bitdefender:

1. Acceda a Bitdefender Central.
2. En la ventana **MIS DISPOSITIVOS**, seleccione la tarjeta de dicho dispositivo.
3. Seleccione la pestaña **Antirrobo**.
4. En el campo inferior de la ventana, toque el icono ⋯ y, a continuación, toque el botón correspondiente a la característica que desee utilizar:

   Localizar - muestra la ubicación de su dispositivo en Google Maps.

   Alerta - escriba un mensaje para mostrarlo en la pantalla de su dispositivo y/o haga que su dispositivo reproduzca una alarma sonora.

   Bloquear - bloquee su dispositivo y establezca un código PIN para desbloquearlo.

   Borrar - elimina toda la información de su dispositivo.

   Importante
   Después de borrar un dispositivo, todas las características de Anti-Theft dejan de funcionar.

   Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.

Utilización de las funciones de Antirrobo mediante comandos SMS (Control SMS)

Una vez que se habilitan los comandos SMS, puede enviar los siguientes comandos a su smartphone por SMS desde cualquier otro teléfono móvil:

- **locate** - envía un mensaje que muestra la ubicación del dispositivo al teléfono móvil desde el cual se ha enviado el comando. Este mensaje contiene un enlace a Google Maps que puede abrirse en el navegador del teléfono móvil.
- **scream** - reproduce un sonido con el volumen alto en el altavoz del dispositivo.
- **lock** - bloquea la pantalla del dispositivo con el PIN de Bitdefender Mobile Security & Antivirus.
- **wipe** - elimina toda la información de su dispositivo.

Importante
El comando Wipe funciona solo cuando se envía desde el número de confianza predefinido.

- **callme** - marca el número de teléfono desde el cual se ha enviado el comando, activando el altavoz. Así podrá escuchar discretamente a la persona que tenga su teléfono.
- **help** - envía un mensaje que muestra todos los comandos disponibles al teléfono móvil desde el cual se ha enviado el comando.

Todos los comandos SMS deben enviarse con el siguiente formato:

bd-<PIN> <command>

Nota
Los corchetes angulares indican variables y no deben incluirse en el comando.

Por ejemplo, si ha establecido el PIN de seguridad a 123456 y desea recibir un mensaje con la ubicación de su teléfono móvil, envíe el siguiente mensaje de texto a su número de teléfono:

bd-123456 locate

19. BLOQUEO DE APPS

Las aplicaciones instaladas, como las de correo electrónico, fotos o mensajes, pueden contener datos de carácter personal que le gustaría mantener en privado restringiendo selectivamente el acceso a ellos.

El Bloqueo de apps le ayuda a bloquear el acceso no deseado a sus aplicaciones mediante el establecimiento de un código de acceso PIN de seguridad. El código PIN que establezca debe tener un mínimo de cuatro caracteres, pero no más de ocho, y se le requerirá cada vez que quiera acceder a las aplicaciones restringidas seleccionadas.

Activación del Bloqueo de apps

Para restringir el acceso a las aplicaciones seleccionadas, configure el Bloqueo de apps en la tarjeta que se muestra en el panel de control después de activar el Antirrobo.

También puede activar el Bloqueo de apps siguiendo estos pasos:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Bloqueo de apps** en la lista.
3. Permita el acceso de Bitdefender al uso de datos tocando **ACTIVAR** y, a continuación, active el conmutador correspondiente.

   Nota
   En Android 6 se requieren permisos adicionales para la característica Hacer foto.
   Para activarla, permita que **Antivirus** tome fotos y grabe vídeo.

4. Vuelva a la app y toque **ESTABLECER PIN** para configurar el código de acceso.

   Nota
   Este paso solo está disponible si no ha configurado previamente el PIN de Antirrobo.

5. Seleccione las aplicaciones que desee proteger.

Este código será necesario siempre que quiera acceder a cualquiera de las aplicaciones restringidas.

Nota
El Antirrobo utiliza el mismo código PIN para ayudarle a localizar su dispositivo.

Bloqueo de apps

Opciones de Bloqueo de Apps

Toque el botón en el menú del Bloqueo de apps y, a continuación, seleccione **Ajustes** para acceder a la configuración avanzada del Bloqueo de apps.

En la **Configuración** del Bloqueo de apps puede hacer lo siguiente:

- Activar Hacer foto cuando se realicen tres intentos de desbloqueo incorrectos.
- Configurar el Bloqueo de apps para que espere treinta segundos antes de solicitar de nuevo el código PIN que estableció.
- Notificaciones de bloqueo de apps recién instaladas.
- Activar el Desbloqueo inteligente para redes Wi-Fi de confianza.
- Activar el Desbloqueo inteligente para la red Wi-Fi actual.
- Cambie su código PIN.

Hacer foto

Con Hacer foto de Bitdefender puede poner en una situación comprometida a sus amigos o familiares. De esta manera educará su curiosidad para que no traten de ver sus archivos personales o las aplicaciones que utiliza.

El funcionamiento de esta característica es muy sencillo: cada vez que se introduce tres veces seguidas de forma incorrecta el código PIN que estableció para proteger sus apps, se toma una foto usando la cámara frontal. Dicha foto se guarda junto con el motivo y la hora, y podrá verla cuando abra Bitdefender Mobile Security & Antivirus y acceda a la función de Bloqueo de apps.

Nota
Esta característica solo está disponible en teléfonos que posean una cámara frontal.

Para configurar la característica Hacer foto:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Bloqueo de apps** en la lista.
3. Toque el botón en el menú del Bloqueo de apps y, a continuación, seleccione **Ajustes**.
4. Active el conmutador **Hacer foto cuando se realicen tres intentos de desbloqueo incorrectos**.

Las fotos que se tomen cuando se introduzca un PIN incorrecto se mostrarán en el menú de Bloqueo de apps y se pueden ver a pantalla completa.

Como alternativa, se pueden ver en su cuenta de Bitdefender:

1. Diríjase a: https://central.bitdefender.com.
2. Inicie sesión en su cuenta.
3. Seleccione el dispositivo en la ventana MIS DISPOSITIVOS y, a continuación, acceda a la pestaña Antirrobo.

   Se muestran las fotos.

Solo se guardan las últimas tres fotos.

Desbloqueo inteligente

Una forma fácil de evitar que el Bloqueo de apps le pida introducir el código PIN para las apps protegidas cada vez que accede a ellas es activar el Desbloqueo inteligente.

Con el Desbloqueo inteligente puede determinar que las redes Wi-Fi que utiliza normalmente son de confianza, de forma que cuando se conecte a ellas, el Bloqueo de apps se deshabilitará para las apps protegidas.

Para activar el Desbloqueo inteligente:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Bloqueo de apps** en la lista.
3. Toque el botón  en el menú del Bloqueo de apps y, a continuación, seleccione **Ajustes**.
4. Active el conmutador **Desbloqueo inteligente para redes Wi-Fi de confianza**.

   Para determinar que la conexión Wi-Fi que está utilizando actualmente es de confianza, active el conmutador **Confiar en la red Wi-Fi actual**.

> **Nota**
> Este ajuste solo está disponible si el Desbloqueo inteligente está activado.

Si cambia de opinión, desactive la característica y las redes Wi-Fi que haya establecido como redes de confianza dejarán de ser tratadas como tal.

20. INFORMES

La característica Informes mantiene un registro detallado de los eventos relacionados con las actividades de análisis en su dispositivo.

Siempre que sucede algo relevante para la seguridad de su dispositivo, se añade un nuevo mensaje a los Informes.

Para acceder a la sección Informes:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Informes** en la lista.

Aquí podrá ver información detallada sobre la actividad de las características de su Bitdefender. En la sección Visor de sucesos tiene a su disposición todos los eventos acaecidos en su dispositivo.

En esta sección se mostrará un nuevo consejo cada semana, así que asegúrese de revisarla con cierta frecuencia para obtener el máximo partido de la app.

Todos los domingos se genera el informe de la semana en curso. Recibirá una notificación informándole al respecto cuando esté disponible.

21. LOCALIZADOR

Con Bitdefender WearON podrá encontrar fácilmente su smartphone si se lo dejó en la oficina, en una sala de conferencias o debajo de un cojín en el sofá. Puede encontrar el dispositivo incluso si está puesto el modo silencioso.

Mantenga esta característica habilitada para asegurarse de que siempre tiene su smartphone a mano.

Nota
Esta característica funciona con Android 4.3 y Android Wear.

Activación de WearON

Para utilizar WearON, solo tiene que conectar su smartwatch a la aplicación Bitdefender Mobile Security & Antivirus y activar la característica con el siguiente comando de voz:

Start:<Where is my phone>

Bitdefender WearON tiene dos comandos:

1. **Alerta de teléfono**

   Con la característica de Alerta de teléfono puede encontrar rápidamente su smartphone cuando se aleje demasiado de él.

   Si lleva puesto su smartwatch, éste detectará automáticamente la aplicación en su teléfono y vibrará cuando se aleje más de diez metros de su dispositivo.

   Para activar esta característica, abra Bitdefender Mobile Security & Antivirus, toque **Ajustes globales** en el menú y seleccione el conmutador correspondiente en la sección WearON.

2. **Scream**

   Encontrar su teléfono nunca fue tan fácil. Cuando se olvide de dónde dejó su teléfono, toque el comando Scream de su reloj para hacer que suene su teléfono.

22. BITDEFENDER CENTRAL

Bitdefender Central es la plataforma Web en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet con solo acceder a https://central.bitdefender.com. Una vez que haya accedido a la misma, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos OS X, Windows y Android. Los productos disponibles para su descarga son:
  - Bitdefender Mobile Security & Antivirus
  - Bitdefender Antivirus for Mac
  - La línea de productos de Windows de Bitdefender
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

Acceso a su cuenta de Bitdefender

Para acceder a su cuenta Bitdefender, simplemente:

1. Abra un navegador Web en cualquier dispositivo con acceso a Internet.
2. Diríjase a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta con su dirección de correo electrónico y contraseña.

Mis dispositivos

El área **Mis dispositivos** en su cuenta Bitdefender le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de dispositivo muestran el nombre del mismo, el estado de protección y la disponibilidad restante de su suscripción.

Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceda a Bitdefender Central.

2. En la ventana **Mis dispositivos**, toque en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Ajustes**.
3. Cambie el nombre del dispositivo en el campo correspondiente y, a continuación, seleccione **Guardar**.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceda a Bitdefender Central.
2. En la ventana **Mis dispositivos**, toque en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Perfil**.
3. Toque en **Añadir propietario** y, a continuación, rellene los campos correspondientes, establezca el sexo, la fecha de nacimiento e incluso añada una imagen al perfil.
4. Toque **AÑADIR** para guardar el perfil.
5. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, toque **ASIGNAR**.

Para tener acceso a más acciones remotas e información acerca de su producto Bitdefender en un dispositivo concreto, seleccione la tarjeta de dicho dispositivo.

Una vez que seleccione una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de Control**. En esta ventana puede comprobar el estado de protección de sus productos Bitdefender y el número de días restantes de su suscripción. El estado de protección puede ser verde, cuando no hay ningún problema que afecte a su producto, o rojo cuando el dispositivo está en riesgo. Cuando existan problemas que afecten a su producto, toque **Ver incidencias** para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis en su dispositivo. Toque en el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.

- **Antirrobo**. Si no se acuerda de dónde ha puesto su dispositivo, con la función Antirrobo puede localizarlo y llevar a cabo acciones remotas. Toque **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora. Para más información sobre esta característica, consulte "*Características Antirrobo*" (p. 270).

Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceda a Bitdefender Central.
2. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis suscripciones**.

Aquí tiene información sobre la disponibilidad de las suscripciones que posee y el número de dispositivos que utilizan cada una de ellas.

Puede añadir un nuevo dispositivo a una suscripción o renovarlo seleccionando una tarjeta de suscripción.

Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Mobile Security & Antivirus como se indica en "Instalando Bitdefender Mobile Security & Antivirus" (p. 259):

Renovar suscripción

Si le quedan menos de treinta días a su suscripción y usted rechazó la renovación automática, puede renovarla manualmente siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis suscripciones**.
3. Seleccione la tarjeta de suscripción deseada.

4. Toque **RENOVAR** para continuar.

Se abrirá una página Web en su navegador de Internet, donde puede renovar su suscripción de Bitdefender.

23. PREGUNTAS FRECUENTES

¿Por qué necesita Bitdefender Mobile Security & Antivirus una conexión a Internet? La aplicación necesita comunicarse con los servidores de Bitdefender para determinar el estado de seguridad de las aplicaciones que analiza y de las páginas Web que visita, y también para recibir comandos de su cuenta Bitdefender cuando utiliza las características de Antirrobo.

¿Para qué necesita Bitdefender Mobile Security & Antivirus cada permiso?

- Acceso a Internet -> usado para la comunicación cloud.
- Leer identidad y estado del teléfono -> se usa para detectar si el dispositivo está conectado a Internet y extraer determinada información del dispositivo necesaria para crear un ID único cuando se comunica con Bitdefender cloud.
- Leer y guardar favoritos del navegador -> el módulo Seguridad Web elimina sitios peligrosos de su historial de navegación.
- Leer datos de registro -> Bitdefender Mobile Security & Antivirus detecta signos de actividad malware desde los registros de Android.
- Leer / escribir SMS, contactos, datos de cuenta y almacenamiento externo -> requerido para la función de borrador remoto.
- Localizar -> requerido para la localización remota.
- Cámara -> necesaria para Hacer foto.
- Almacenamiento -> se utiliza para permitir que el Analizador de malware compruebe la tarjeta SD.

¿Dónde puedo leer información detallada sobre la actividad de la aplicación?

Bitdefender Mobile Security & Antivirus mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para acceder a esta información, abra Bitdefender Mobile Security & Antivirus y toque el botón **Menú**. A continuación, seleccione **Informes** en la lista.

He olvidado el código PIN que establecí para proteger mi aplicación. ¿Qué hago?

1. Acceda a Bitdefender Central.

2. En la ventana **Mis dispositivos**, seleccione el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Ajustes**.
3. Obtenga el código PIN del campo **PIN de aplicación**.

¿Cómo repercutirá Bitdefender Mobile Security & Antivirus en el rendimiento y en la autonomía de la batería de mi dispositivo?

Conseguimos un impacto mínimo. La aplicación solo se ejecuta cuando es esencial: después de que instale una aplicación, cuando utilice la interfaz de la aplicación o cuando quiera un control de seguridad. Bitdefender Mobile Security & Antivirus no se ejecuta en segundo plano cuando llama a sus amigos, escribe sus mensajes o juega una partida.

¿De qué me informa el Asesor de privacidad sobre las aplicaciones que instalo?

El Asesor de privacidad le informa sobre lo que cada aplicación puede hacer en su dispositivo. Le indica si una aplicación puede acceder a sus datos privados, enviar mensajes, conectarse a Internet o ejecutar cualquier otra función que pueda suponer un riesgo para su seguridad.

¿Puedo eliminar una aplicación que considere una amenaza para mi privacidad?

Puede eliminar manualmente una aplicación mediante el Asesor de privacidad. Para ello, toque la app deseada y, a continuación, el botón **DESINSTALAR APP**. Confirme su elección y espere a que complete el proceso de desinstalación.

¿Cómo puedo desactivar las notificaciones del Asesor de privacidad?

Si desea dejar de recibir notificaciones del Asesor de privacidad:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Ajustes** en la lista.
3. En la sección **Asesor de privacidad**, toque el conmutador correspondiente.

¿En qué idiomas está disponible Bitdefender Mobile Security & Antivirus?

Bitdefender Mobile Security & Antivirus está disponible actualmente en los siguientes idiomas:

- Inglés
- Francés
- Alemán

- Italiano
- Rumano
- Español
- Brasileño
- Portugués
- Polaco
- Coreano
- Vietnamita
- Griego
- Holandés

Se añadirán otros idiomas en futuras versiones. Para cambiar el idioma de la interfaz de Bitdefender Mobile Security & Antivirus, vaya a los ajustes **Idioma y texto** de su dispositivo y configure el dispositivo con el idioma que desee utilizar.

¿Puedo cambiar la cuenta Bitdefender asociada a mi dispositivo?

Sí, puede cambiar fácilmente la cuenta de Bitdefender vinculada a su dispositivo siguiendo los pasos que se indican a continuación:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Información de la cuenta** en la lista.
3. Toque **CERRAR SESIÓN** y, a continuación, confirme su elección.
4. Toque **USAR CUENTA DE CENTRAL** y, a continuación, escriba la dirección de correo electrónico y contraseña de su nueva cuenta de Bitdefender.

¿Qué es el administrador de dispositivos?

El Administrador de dispositivos es una función de Android que da a Bitdefender Mobile Security & Antivirus los permisos que necesita para ejecutar determinadas tareas de forma remota. Sin estos privilegios, el bloqueo remoto no funcionaría y el borrado del dispositivo no podría completarse para eliminar sus datos. Si desea desinstalar la app, asegúrese de revocar estos privilegios antes de tratar de desinstalarla desde **Ajustes > Ubicación & Seguridad > Seleccionar administradores de dispositivo**.

¿Para qué sirve el número de confianza?

Si su teléfono cae en manos de alguien que no tenga la intención de devolverlo a su legítimo dueño, cabe esperar que cambie rápidamente la tarjeta SIM. Siempre que Bitdefender Mobile Security & Antivirus detecte que se ha cambiado la tarjeta SIM de su teléfono, enviará automáticamente

un mensaje de texto al número que ha establecido informando del nuevo número de teléfono. Así podrá enviar comandos SMS a su teléfono incluso aunque cambien la tarjeta SIM y, por tanto, el número. Este puede ser el número de alguien que usted conozca y en el que confíe, o el de otro teléfono que utilice.

¿Puedo cambiar el número de confianza después de haberlo establecido?

Para establecer un número de confianza diferente:

1. Abrir Bitdefender Mobile Security & Antivirus.
2. Toque el botón **Menú** y seleccione **Ajustes** en la lista.
3. En la sección **Antirrobo**, toque **Número de confianza**.

   Se le pedirá que indique el PIN para poder cambiar el número de confianza.

¿Cuánto me va a costar enviar los comandos SMS?

Los comandos SMS se envían como cualquier otro mensaje de texto y, por tanto, su operador se los cobrará como tales. Bitdefender no realiza ningún cargo adicional.

Cómo arreglar el error "No Google Token" que aparece cuando se inicia sesión en Bitdefender Mobile Security & Antivirus.

Este error ocurre cuando el dispositivo no está asociado con una cuenta de Google, o el dispositivo está asociado con una cuenta pero un problema temporal evita que se conecte a Google. Pruebe una de las siguientes soluciones:

- Vaya a los Ajustes de Android > Aplicaciones > Administrar aplicaciones > Bitdefender Mobile Security & Antivirus y toque **Borrar datos**. Luego intente iniciar sesión nuevamente.
- Asegúrese de que su dispositivo está asociado a una cuenta de Google.

  Para comprobar esto, diríjase a Ajustes > cuentas & sincronización y mire si existe una cuenta de Google bajo **Administrar cuentas**. Añada su cuenta si no aparece ninguna, reinicie su dispositivo e intente iniciar sesión en Bitdefender Mobile Security & Antivirus.
- Reinicie su dispositivo, luego inicie sesión nuevamente.

CONTACTO

24. PEDIR AYUDA

Bitdefender proporciona a sus clientes un nivel sin igual de soporte rápido y preciso. 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. Al mismo tiempo, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

La sección "*Resolución de incidencias comunes*" (p. 186) le proporciona la información necesaria sobre las incidencias más frecuentes a las que se pueda enfrentar cuando utiliza este producto.

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

Si no halla respuesta a sus dudas en los recursos proporcionados, acceda a http://www.bitdefender.es/support/contact-us.html y póngase en contacto con nuestros representantes de soporte.

También puede consultar nuestro "*Recursos online*" (p. 291) para obtener asesoramiento o información adicional sobre todos los productos Bitdefender.

25. 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/support/consumer.html

- Foro de Soporte de Bitdefender:

  http://forum.bitdefender.com

- El portal de seguridad informática HOTforSecurity:

  http://www.hotforsecurity.com

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

25.1. 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/support/consumer.html.

25.2. 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.

25.3. Portal HOTforSecurity

El portal HOTforSecurity es una preciada fuente de información de seguridad informática. Aquí puede saber las varias amenazas a las que está expuesto su pc cuando está conectado a Internet (malware, phishing, spam, cibercriminales).

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 HOTforSecurity es http://www.hotforsecurity.com.

26. INFORMACIÓN DE CONTACTO

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 10 años ha establecido una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectaciones de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

26.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Centro de soporte:http://www.bitdefender.es/support/consumer.html
Documentación: documentation@bitdefender.com
Distribuidores Locales:http://www.bitdefender.es/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

26.2. 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/partners/partner-locator.html.
2. Elija su país y ciudad mediante las opciones correspondientes.
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.

26.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están lista para responder a cualquier pregunta sobre sus áreas de operación, tanto comerciales como de asuntos generales. Sus direcciones y contactos están listados a continuación.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Tel (oficina&comercial): 1-954-776-6262
Comercial: sales@bitdefender.com
Soporte Técnico: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Alemania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Oficina: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Comercial: vertrieb@bitdefender.de
Soporte Técnico: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

España

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Teléfono: +34 902 19 07 65
Comercial: comercial@bitdefender.es
Soporte Técnico: http://www.bitdefender.es/support/consumer.html
Página Web: http://www.bitdefender.es

Rumania

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Teléfono comercial: +40 21 2063470
Correo comercial: sales@bitdefender.ro

Soporte Técnico: http://www.bitdefender.ro/support/consumer.html
Página Web: http://www.bitdefender.ro

Emiratos Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Teléfono comercial: 00971-4-4588935 / 00971-4-4589186
Correo comercial: mena-sales@bitdefender.com
Soporte Técnico: http://www.bitdefender.com/support/consumer.html
Página Web: http://www.bitdefender.com

Glosario

ActiveX

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

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

Actualizar

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 de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan 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 problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Amenaza persistente avanzada

Una amenaza persistente avanzada (Advanced Persistent Threat, APT) explota vulnerabilidades de los sistemas para robar información importante que se entrega a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el objetivo primordial de este malware.

El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo, para poder monitorizar y recopilar información importante sin dañar las máquinas objetivo. El método empleado para inyectar el virus en la red es un archivo PDF o un documento de Office que parezca inofensivo, para que cualquier usuario decida ejecutarlo.

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 conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

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

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

Cliente de mail

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

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio determinado. Un código de activación permite la activación de una suscripción válida durante un cierto período de tiempo y para determinado número de dispositivos, y también puede utilizarse para ampliar una suscripción con la condición de que se genere para el mismo producto o servicio.

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.

Descargar

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

E-mail

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

Elementos en 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

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web. los navegadores más populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Extensión de un archivo

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

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho 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 añadir a otros programas.

Heurístico

Un método basado en reglas para identificar nuevos virus. Este método de análisis no se basa en firmas de virus específicas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de un virus existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

Honeypot (sistema trampa)

Un sistema informático que sirve como señuelo para atraer a los piratas informáticos con el fin de estudiar cómo actúan e identificar los métodos delictivos que utilizan para recabar información del sistema. Las empresas y grandes corporaciones están más interesadas ??en implementar y utilizar estos sistemas trampa para mejorar su estado general de seguridad.

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.

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

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 con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

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.

Photon

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto de la protección antivirus en el rendimiento. Monitorizando en segundo plano la actividad de su PC, crea patrones de uso que ayudan a optimizar los procesos de arranque y de análisis.

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.

Ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Cryptolocker, CryptoWall y TeslaWall son solo algunas de las variantes que secuestran los sistemas personales de los usuarios.

La infección puede propagarse al acceder a spam, descargar archivos adjuntos, o instalar aplicaciones, evitando que el usuario se percate de lo que está sucediendo en su sistema. Los usuarios habituales y empresas son el objetivo de los hackers de ransomware.

Red Privada Virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su intercepción por parte de los fisgones. Una muestra de seguridad es la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Rootkit

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

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

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

Ruta

Las rutas exactas de un archivo en un equipo. Esta suma de información 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 los grupos de noticias. Generalmente conocido como correo no solicita.

Spyware

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

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

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

TCP/IP

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

Troyano

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

El término viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar 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 hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

Virus de macro

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

Estas aplicaciones permiten introducir un macro en un documento y también que el 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.